ORAL ARGUMENT NOT YET SCHEDULED

No. 16-1135, consolidated with No. 16-1139

IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT

COMPETITIVE ENTERPRISE INSTITUTE, et al.,
Petitioners,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY, et al.,
Respondents.

ON PETITION FOR REVIEW OF FINAL RULE OF TRANSPORTATION SECURITY ADMINISTRATION

JOINT APPENDIX
VOLUME I OF II (JA 1 – JA 415)

BENJAMIN C. MIZNER
Principal Deputy Assistant Attoney General
CHANNING D. PHILLIPS
United States Attorney
MARK B. STERN
SHARON SWINGLE
(202) 353-2689
Attorneys, Appellate Staff
Civil Division, Room 7250
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
JERAMIE SCOTT
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioner
Electronic Privacy Information Center

SAM KAZMAN
HANS BADER
COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street NW, 7th Floor
Washington, DC 20005
(202) 331-2278
Counsel for Petitioner
Competitive Enterprise Institute

December 15, 2016

TABLE OF CONTENTS

Page

VOLUME I

VOLUME II

THIS PAGE INTENTIONALLY LEFT BLANK

FEDERAL REGISTER

Vol. 81 Thursday,

No. 42 March 3, 2016

Part II

Department of Homeland Security

Transportation Security Administration

49 CFR Part 1540

Passenger Screening Using Advanced Imaging Technology; Final Rule

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1540

[Docket No. TSA–2013–0004]

RIN 1652–AA67

Passenger Screening Using Advanced Imaging Technology

AGENCY: Transportation Security Administration, DHS.

ACTION: Final rule.

SUMMARY: The Transportation Security Administration (TSA) is amending its civil aviation security regulations to specify that TSA may use advanced imaging technology (AIT) to screen individuals at security screening checkpoints. This rule is issued to comply with a decision of the U.S. Court of Appeals for the District of Columbia Circuit, which ordered TSA to engage in notice-and-comment rulemaking on the use of AIT for passenger screening.

DATES: Effective May 2, 2016.

FOR FURTHER INFORMATION CONTACT: Chawanna Carrington, Acting Passenger Screening Program Portfolio Section Lead-Checkpoint Solutions and Integration Division, Office of Security Capabilities—Transportation Security Administration, *OSCCSI-PSP@tsa.dhs.gov,* 571–227–2958 (phone), 571–227–1931 (fax).

SUPPLEMENTARY INFORMATION:

Availability of Rulemaking Document

You can get an electronic copy using the Internet by—

(1) Searching the electronic Federal Docket Management System (FDMS) Web page at *http://www.regulations.gov;* or

(2) Accessing the Government Printing Office's Web page at *http://www.gpo.gov/fdsys/browse/collection.action?collectionCode=FR* to view the daily published **Federal Register** edition; or accessing the ''Search the **Federal Register** by Citation'' in the ''Related Resources'' column on the left, if you need to do a Simple or Advanced search for information, such as a type of document that crosses multiple agencies or dates.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Small Entity Inquiries

The Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996 requires TSA to comply with small entity requests for information and advice about compliance with statutes and regulations within TSA's jurisdiction. Any small entity that has a question regarding this document may contact the person listed in the **FOR FURTHER INFORMATION CONTACT** section. Persons can obtain further information regarding SBREFA on the Small Business Administration's Web page at *https://www.sba.gov/category/advocacy-navigation-structure/regulatory-policy/regulatory-flexibility-act/sbrefa.*

Abbreviations and Terms Used in This Document

AIT Advanced Imaging Technology
ANSI American National Standards Institute
APA Administrative Procedure Act
ATR Automatic Target Recognition
ATSA Aviation and Transportation Security Act
CAPPS Computer-Assisted Passenger Prescreening System
CDRH Center for Devices and Radiological Health
CFR Code of Federal Regulations
DHS Department of Homeland Security
DOJ Department of Justice
DNA Deoxyribonucleic acid
EAJA Equal Access to Justice Act
E.O. Executive Order
ETD Explosives Trace Detection Devices
FAA Federal Aviation Administration
FDA Food and Drug Administration
FR **Federal Register**
GAO Government Accountability Office
HPS Health Physics Society
ICAO International Civil Aviation Organization
IEEE International Electronic and Electrical Engineers
IRFA Initial Regulatory Flexibility Analysis
LCCE Life Cycle Cost Estimate
NEPA National Environmental Policy Act of 1969
NPRM Notice of Proposed Rulemaking
OCRL/OTE Office of Civil Rights and Liberties, Ombudsman and Traveler Engagement
OMB Office of Management and Budget
OSC Office of Security Capabilities
PIA Privacy Impact Assessment
PMIS Performance Management Information System
PMO Program Management Office
PRA Paperwork Reduction Act
RFA Regulatory Flexibility Act of 1996
RIA Regulatory Impact Analysis
SAM Screener Allocation Model
SOP Standard Operating Procedure
SSI Sensitive Security Information
THz Terahertz
TSA Transportation Security Administration
TSL Transportation Security Laboratory
TSO Transportation Security Officer
UMRA Unfunded Mandates Reform Act
U.S.C. United States Code
WTMD Walk Through Metal Detector

Table of Contents

I. Background

A. Summary of the Final Rule

Congress has charged the Transportation Security Administration (TSA), a component of the U.S.

Department of Homeland Security (DHS), with responsibility for civil aviation security, 49 U.S.C. 114(d), including combatting the threat posed by al Qaeda and other terrorists. The Administrator of TSA must ''assess current and potential threats to the domestic air transportation system'' and take ''necessary actions to improve domestic air transportation security,'' including by providing for ''the screening of all passengers and property'' before boarding an aircraft to ensure that no passenger is ''carrying unlawfully a dangerous weapon, explosive, or other destructive substance.'' *See* 49 U.S.C. 44904(a) and (e); 44901(a); 44902(a)(1).

By Federal regulation, ''[n]o individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft. . . .'' 49 CFR 1540.107(a). The final rule amends this regulation to specify that the screening and inspection of a person may include the use of advanced imaging technology (AIT).

Congress has directed 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.'' 49 U.S.C. 44925(a).[1] In June 2008, the Senate Appropriations Committee encouraged TSA to expand the use of AIT.[2] TSA began deploying AIT in 2008 after laboratory and operational testing.

The AIT currently deployed by TSA is a millimeter wave imaging technology that can detect metallic and non-metallic objects on an individual's body or concealed in his clothing without physical contact. The technology bounces electromagnetic waves off the body to detect anomalies. If an anomaly is detected, a pat-down of the area where the anomaly is located is usually performed to determine if a threat is present.

AIT addresses a critical weakness in aviation security regarding the inability of walk-through metal detectors (WTMDs) to screen for non-metallic explosives and other non-metallic threat items. AIT provides detection capability for weapons, explosives, and other objects concealed under a person's clothing that may not trigger a metal detector. TSA has determined that use of AIT is the most effective technology currently available to detect both metallic and non-metallic threat items concealed on passengers, such as the non-metallic explosive used by the so-called ''Christmas Day bomber'' in 2009 in his attempt to blow up an American passenger aircraft.

AIT is an essential component of TSA's risk-based security approach. This approach relies on a comprehensive security system including state-of-the-art technologies (such as AIT), a highly-trained frontline workforce, intelligence analysis and information sharing, behavior detection, explosives detection canine teams, Federal Air Marshals (FAMS), and regulatory enforcement.

In 2012, Congress enacted the FAA Modernization and Reform Act of 2012, Public Law 112–95, which required TSA to ensure that all AIT used to screen passengers must be equipped with and employ automatic target recognition (ATR) software. 49 U.S.C. 44901(l). That software eliminates passenger-specific (*i.e.,* individual) images and instead indicates the location of potential threats on a generic outline. Since May 2013, all AIT units deployed by TSA have been equipped with ATR capability. The final rule adopts the statutory definitions of AIT and ATR, and requires that any AIT equipment used to screen passengers be equipped with and employs ATR software.

There are approximately 793 AIT machines deployed at nearly 157 airports nationwide. AIT screening is safe for all passengers and the technology meets all national health and safety standards. Passengers generally may decline AIT screening and opt instead for a pat-down.

B. Purpose of the Final Rule

The final rule is adopted to comply with a ruling of the United States Court of Appeals for the District of Columbia Circuit. In *Electronic Privacy Information Center (EPIC)* v. *U.S. Department of Homeland Security,* 653 F.3d 1 (D.C. Cir. 2011), the court directed TSA to conduct notice-and-comment rulemaking on the use of AIT to screen passengers. TSA published a notice of proposed rulemaking (NPRM) on March 26, 2013, to obtain public comment on its proposal to revise civil aviation security regulations to codify that TSA may use AIT for passenger screening. 78 FR 18287. The final rule defines AIT, states that AIT may be used to screen passengers, and requires that AIT be equipped with and employ the use of ATR software.

C. Costs and Benefits

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. As the AIT unit life cycle is 10 years from deployment to disposal, the period of analysis for estimating the cost of the rule is 10 years. TSA has revised the NPRM Regulatory Impact Analysis (RIA) assumption of an 8-year life cycle for AIT units to 10 years based on a recent life cycle cost estimate (LCCE) report.[3] AIT deployment began in 2008 and TSA, therefore, includes costs that have already been borne by TSA, the traveling public, the screening systems industry, and airports. Consequently, this RIA takes into account costs that have already occurred—in years 2008–2014—in addition to the projected costs in years 2015[4]–2017. By reporting the costs that have already occurred and estimating future costs in this manner, TSA accounts for the full life cycle of AIT machines.

TSA estimates the total cost of the rule from 2008–2017 to be $2,146.31 million (undiscounted). TSA incurs over 98 percent of all costs.

AIT generates benefits by reducing security risks because it is capable of detecting both metallic and non-metallic weapons and explosives.[5] Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the WTMD. TSA also considered the added benefit of deterrence—the effect of would-be

---

[1] *See also* Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack'' (Jan. 7, 2010), available at *http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack* (charging DHS with aggressively pursuing enhanced screening technology in order to prevent further such attempts while at the same time protecting passenger privacy).

[2] S. Rep. No. 110–396, at 60 (2008).

[3] TSA's Office of Security Capabilities (OSC), ''Life Cycle Cost Estimate for Passenger Screening Program,'' March 10, 2014. This is a TSA acquisition sensitive report based on OSC technology assessments.

[4] The 2015 cost estimates used historical data when available. Please see the RIA for the complete description of the 2015 cost estimates.

[5] Metal detectors and AITs are both designed to detect metallic threats on passengers, but do so in different ways. Metal detectors rely on the inductance that is generated by the metal, while AIT relies on the metal's reflectivity properties to indicate an anomaly. AIT detection capabilities exceed that of metal detectors because AIT can detect metallic and non-metallic weapons, non-metallic bulk explosives, and non-metallic liquid explosives.

attackers becoming discouraged because of increased security measures—from the use of AIT. Morral and Jackson (2009) stated, ''Deterrence is also a major factor in the cost-effectiveness of many security programs. For instance, even if a radiation-detection system at ports never actually encounters weapon material, if it deters would-be attackers from trying to smuggle such material into the country, it could easily be cost-effective even if associated program costs are very high.'' [6] Given the demonstrated ability of AIT to detect concealed metallic and non-metallic objects, it is reasonable to assume that AIT acts as a deterrent to attacks involving the smuggling of a metallic or non-metallic weapon or explosive on board a commercial airplane. As an essential component in TSA's comprehensive security system because it can detect both non-metallic and metallic threats concealed under a person's clothing, AIT plays a vital role in decreasing the vulnerability of civil aviation to a terrorist attack.

To describe further the security benefits from AIT, TSA performed a break-even analysis to compare the potential direct costs of an averted terrorist attack to the net cost of AIT. Agencies use a break-even analysis when quantification of benefits is not possible. According to OMB Circular No. A–4, ''Regulatory Analysis,'' such an analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the nonquantified costs need to be) before the rule would yield zero net benefits?'' [7] Based upon the results from the break-even analysis, TSA estimates that AIT will need to prevent an attack between once every 5.25 years to once every 23.5 years—depending on the size of the aircraft—for the direct cost of an averted attack to equal the annualized cost of AIT. The break-even analysis does not include the difficult to quantify indirect costs of an attack or the macroeconomic impacts that could occur due to a major attack. See Section III of this preamble for more detailed results of the economic analyses.

D. Changes From the NPRM

In the NPRM, TSA proposed to amend 49 CFR 1540.107 by adding a new paragraph to specify that the screening and inspection of an individual prior to entering a sterile area of an airport or boarding an aircraft may include the use of AIT. TSA defined AIT as ''screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.'' TSA received many comments stating that the definition was too broad. Commenters also expressed confusion and uncertainty regarding the use of the word ''anomalies.'' Some commenters suggested privacy safeguards be included in the final rule.

In response to those comments, TSA changed the definition in the final rule. TSA is adopting the definition of AIT created by Congress in the FAA Modernization and Reform Act of 2012.[8] That legislation, codified at 49 U.S.C. 44901(l), defines AIT as ''a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body; and may include devices using backscatter x-rays or millimeter waves and devices referred to as 'whole-body imaging technology' or 'body scanning machines'.'' Further, in response to privacy concerns, TSA is adopting the statutory language that requires any AIT used for passenger screening to be equipped with and employ ATR software and comply with such other requirements TSA determines are necessary to address privacy considerations. Finally, consistent with the statute, TSA is defining ATR as, ''software installed on an advanced imaging technology device that produces a generic image of the individual being screened that is the same as the images produced for all other screened individuals.''

In response to public comments, TSA also revised the RIA published with the NPRM to include a break-even analysis and pertinent data that has become available since the publication of the NPRM, including an updated AIT deployment schedule. TSA's major changes to the RIA from the NPRM are:

- Revising the airport listings to include 460 airports instead of 448. The updated airport list includes new, previous, and former airports that operated AIT units and are regulated under 49 CFR part 1542.
- Updating the AIT life cycle and period of analysis from 8 to 10 years based on a recent LCCE report from the TSA Office of Security Capabilities (OSC). Using the information from this report, TSA also revised its previous assumption about the share of Passenger Screening Program expenditures spent on AIT technology.
- Revising the number of AIT units to be deployed from 821 to 793 throughout the period of analysis (2008–2017) based on new data.
- Revising the total wait time for a passenger that opts-out of AIT screening from 80 to 150 seconds to include passenger time spent waiting for a same gender Transportation Security Officer (TSO) to perform the pat-down.
- Revising the calculation of utilities costs to incorporate new data on the hours of AIT operation from the TSA's Performance Management Information System (PMIS) database.
- Refining the calculation of personnel costs by using information on specific labor hours dedicated to AIT operation in response to new data on hours of AIT operation.
- Revising the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs.
- Including a break-even analysis to answer the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?''
- Revising language within the RIA and final rule to state that passengers ''may generally opt-out of AIT screening'' to reflect current DHS policy.[9]

Table 1 presents a summary of the effects of these changes. In the table, NPRM and final rule costs have been annualized due to the different periods of analysis.

---

[6] Andrew R. Morral, Brian A. Jackson, ''Understanding the Role of Deterrence in Counterterrorism Security,'' 2009, Rand Homeland Security Program, *http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf*.

[7] *http://www.whitehouse.gov/omb/circulars_a004_a-4/*.

[8] Public Law 112–95 (126 Stat. 11, Feb. 14, 2012).

[9] *See* Privacy Impact Assessment Update for TSA Advanced Imaging Technology (DHS/TSA/PIA–032(d)) December 18, 2015, *https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf*.

TABLE 1—CHANGES IN AIT ESTIMATES FROM THE NPRM TO THE FINAL RULE

[Annualized at a 7% discount rate in 2014 dollars]

Variables	NPRM and FR comparison			Description of changes
	NPRM	Final rule	Difference	
Annualized Industry Costs ($millions)				
Airport Utilities Cost	$0.19	$0.15	−$0.04	This estimate decreased due to incorporation of newly available historical data on AIT hours of operation from the TSA's PMIS database.
Backscatter AIT Removal	0.21	0.18	−0.03	Total cost in constant dollars remained the same, but annualized cost decreased because of the different periods of analysis between NPRM and final rule.
Annualized Passenger Costs ($millions)				
Opportunity Costs (Delay Costs).	2.08	2.60	0.52	This estimate increased because the estimated duration of a pat-down increased from 80 to 150 seconds to include passenger wait time to be handed off to a same gender TSO.
Annualized TSA Costs ($millions)				
Personnel	216.40	117.17	−99.22	TSA refined this estimate to account for labor hours dedicated to AIT operation. TSA used AIT operational hours recorded in PMIS as a basis for this estimate.
Training	5.81	27.68	21.87	TSA revised the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs.
Equipment	70.62	56.53	−14.08	TSA revised its cost estimates in 2014–2017 to reflect the most recent LCCE document by OSC. TSA also revised some assumptions for cost estimates from 2008–2013 based on the recent LCCE.
TSA Utilities Cost	0.25	0.26	0.01	This change reflects the revised estimate on AIT operation time and an increase of airport enrollment in TSAs utilities reimbursement program.
Total Costs	[10] 295.56	204.57	−90.99	The total cost decreased from the NPRM, primarily from the reduction in personnel costs.
Benefits				
Break-Even Analysis	Prevent 1 attack per 5.25 to 23.52 years considering only the major direct costs of an averted attack.			Per public comment, TSA has included a break-even analysis in the RIA.

II. Public Comments on the NPRM and TSA Responses

A. Summary

TSA published the NPRM on March 26, 2013, and requested comments be submitted by June 24, 2013. Private citizens, industry associations, advocacy groups, and non-profit organizations submitted comments in docket TSA 2013–0004. The discussion below groups the submissions by the primary issues raised in the public comments.

B. Support for AIT

Comments: A number of submissions included a statement of general support for the continued use of AIT without offering additional, substantive rationale. Commenters also expressed approval for AIT for a variety of reasons. Several individual commenters stated they have medical conditions (*e.g.,* metallic implants, metallic artificial joints, and prostheses) which cause them to alarm the WTMD, and they prefer the ease and quickness of AIT to the pat-down procedure, which would be required to resolve an alarm of the WTMD. Several other commenters noted that the need to ensure the safety of airline passengers and other American targets against terrorist threats outweighs possible privacy concerns associated with AIT. In supporting AIT use, many commenters referenced the terrorist attacks on September 11, 2001. Individual commenters also stated they did not have any concerns related to the use of AIT. In response to other public comments opposed to AIT, several individual commenters questioned the significance of the alleged impact of AIT on privacy or safety. Several individual commenters also expressed a preference for AIT over a pat-down.

TSA Response: TSA agrees with these commenters that AIT provides the most effective and least intrusive means currently available to detect both metallic and non-metallic threats concealed under a person's clothing.

C. Opposition to AIT

Comments: Many submissions included statements of opposition to the continued use of AIT. Of these, individual commenters expressed concerns pertaining to efficacy, privacy,

[10] There was a calculation error in the NPRM's presentation of annualized costs. TSA has resolved this error and presented the correct annualized amounts in Table 1. The error in annualized cost did not affect any other cost estimates in the NPRM, including the estimated total cost of the rule and the estimated itemized costs presented in the NPRM.

health, cost, and civil liberties. TSA addresses each of these topics in subsequent comment responses in this preamble. Some individual commenters also expressed criticism of TSA and its staff. Some comments included statements requesting the elimination of AIT.

Other commenters made statements regarding the impact of AIT screening on their travel choices. Many of these commenters indicated they no longer travel by air because of the use of AIT. Some said they limit their airline travel as much as possible because of AIT screening. An individual commenter cited a news article that highlights increasing ridership of Amtrak over airline travel. Several other individual commenters noted that international travelers no longer want to visit the United States because of AIT screening. According to another individual commenter, the AIT scanners have created an ''adversarial tension'' between TSOs and travelers that is detrimental to security.

A few commenters discussed TSA's statement in the NPRM that the public generally approves of the AIT scanners. For example, an individual commenter stated this claim was not supported by data regarding the public's approval. Other commenters suggested that TSA should not assume the lack of complaints about AIT to be support for the use of AIT. For example, a privacy advocacy organization stated that TSA has not taken into consideration the number of passengers who choose AIT over a pat-down because it is faster and potentially less invasive of personal privacy, not because they support the use of AIT. Another individual commenter, however, acknowledged that National ABC and CBS news polls indicated that the majority of poll participants favored full body scanners at airports.

TSA Response: The information TSA receives from intelligence-gathering agencies confirms that civil aviation remains a favored target for extremists and terror organizations. AIT is an essential tool to address that threat by helping TSA to detect both metallic and nonmetallic explosives and other dangerous items concealed under clothing. AIT screening generally is optional and passengers are advised that they may choose to undergo a pat-down instead of AIT.

TSA takes the issues raised in the comments regarding the screening experience seriously and has instituted changes in its policies to address these concerns. New risk-based policies have transformed the agency from one that screens every passenger in the same manner to one that employs a more effective, risk-based, intelligence-driven approach. Adopting a risk-based approach permits much-needed flexibility to adjust to changing travel patterns and shifting threats.

For example, beginning in 2011, after analyzing intelligence reports, TSA instituted new screening procedures for passengers under the age of 12 and those ages 75 and older to expedite screening and reduce the need for a pat-down to resolve alarms.[11] TSA also instituted TSA Pre✓™ (a known and trusted traveler program) based on the rationale that most passengers do not pose a risk to aviation security.[12] This program increases passenger throughput at the security checkpoint and improves the screening experience of frequent, trusted travelers.[13] In addition, TSA Pre✓™ reduces the amount of time TSOs devote to screening low-risk travelers, thereby increasing the resources available to deter or detect the next attack. TSA is working to expand the population of passengers eligible for the program, the number of participating air carriers, and the airports where it is available. In December 2013, TSA launched its TSA Pre✓™ application program that allows U.S. citizens and lawful permanent residents to apply for TSA Pre✓™. As of February 2015, TSA Pre✓™ is available at 120 airports and eleven airlines participate in the program. Millions of passengers have undergone expedited screening through the program. Finally, TSA has instituted a new protocol at certain airports that allow passengers who are not registered in TSA Pre✓™ to undergo a real-time threat assessment at the airport so that they may be randomly selected for expedited screening. TSA will always incorporate random and unpredictable security measures throughout the airport, and no individual is guaranteed expedited screening. TSA encourages all potential passengers to learn about the TSA Pre✓™ program by going to its Web site at *www.tsa.gov.*

As explained in the NPRM, in order to address privacy concerns and meet the statutory requirement to install and employ ATR software on all AIT units, TSA removed all backscatter AIT machines from screening checkpoints, and only millimeter wave AIT machines equipped with ATR are used to screen passengers. The ATR displays a generic outline on which boxes appear where an anomaly is detected. The outline is displayed on the AIT machine so that the passenger and the TSO are able to see the boxes. No specific image of an individual is created.

TSA disagrees with statements that use of AIT has had a material impact on U.S. air travel and the comments did not contain data in support. TSA was unable to find empirical evidence that air travel is reduced due to AIT. TSA notes that based on PMIS data collected from 2009, the first full year of data collection, through 2013, the last full year of data available at the time TSA began drafting this final rule, approximately one percent of passengers have selected a pat-down over AIT screening.[14] TSA agrees with a commenter that independent polling on AIT acceptance shows strong public support for and understanding of the need for AIT.[15]

D. TSA Authority To Use AIT

Comments: Many individual commenters stated that TSA has overstepped its authority by deploying AIT and that the agency itself should be eliminated or that AIT should be eliminated as a screening technology. Additionally, many individual commenters stated that responsibility for airport security and the costs should be returned to either the owners of airports or the airlines.

A non-profit organization referenced 49 U.S.C. 44903(b)(2)(A) and 49 U.S.C. 44903(b)(2)(B) to support its statement that the proposed rule is inconsistent with statutory requirements to protect passengers and the public interest in promoting air transportation. The organization stated that TSA is not authorized ''to sexually assault passengers'' under current statutes or regulations. An individual commenter stated that TSA, as a Federal agency, has no jurisdiction over public airports, which the commenter stated are mostly on state land. Another individual commenter alleged that the

[11] These individuals currently can receive some form of expedited screening, are permitted to leave their shoes, light jackets, and headwear on for screening, and are screened primarily by the Walk-Through Metal Detector (WTMD). *See https://www.tsa.gov/travel/special-procedures, https://www.tsa.gov/travel/special-procedures/traveling-children.*

[12] *https://www.tsa.gov/tsa-precheck.*

[13] *https://www.tsa.gov/tsa-precheck. See also Ruskai* v. *Pistole,* 775 F.3d 61, 64 (1st Cir. 2014) (''Additionally, TSA has opted to impose more limited screening burdens on passengers whom it confirms are part of TSA's PreCheck program. As described in the briefing, PreCheck offers passenger members 'expedited screening in designated lanes if they have been cleared for such screening based on certain background checks conducted prior to their arrival at the airport,' and a more limited pat-down in the event that the passenger alarms a WTMD.'').

[14] PMIS is a database used to track checkpoint operations. The database contains information on AIT use.

[15] 78 FR 18296 at footnote 62.

Administrator of TSA acted illegally implementing AIT and stated he should be removed from office and charged accordingly.

TSA Response: TSA has the statutory authority to deploy AIT. The Administrator of TSA has overall responsibility for civil aviation security, and Congress has conferred on the Administrator authority to carry out that responsibility.[16] Federal law requires that the Administrator ''assess threats to transportation,'' and ''develop policies, strategies, and plans for dealing with threats to transportation security.''[17]

Prior to the terrorist attacks of September 11, 2001, and the enactment of the Aviation and Transportation Security Act (ATSA),[18] air carriers were required to conduct the screening of passengers and property and did so in accordance with regulations issued by the Federal Aviation Administration (FAA) and security programs approved by the FAA.[19] The security programs were sensitive security information (SSI) and were not shared with the public.[20] The ATSA transferred that responsibility to TSA, as codified at 49 U.S.C. 44901(a), and required the TSA Administrator to provide for the screening of all passengers and property that will be carried aboard a passenger aircraft. Federal law also requires the TSA Administrator to prescribe regulations to require air carriers to refuse to transport a passenger or the property of a passenger who does not consent to a search, and to protect passengers and property on an aircraft against an act of criminal violence or aircraft piracy.[21] As commenters noted, when prescribing certain regulations, the Administrator is required to consider whether the regulation is consistent with protecting passengers and the public interest in promoting air transportation.[22] Air transportation security is essential to ensure the freedom of movement for people and commerce. As the U.S. Court of Appeals for the First Circuit wrote in *Ruskai,* ''[p]lanes blown out of the sky in Russia and attempted bombings on U.S. airliners in recent years have warned TSA that its screening procedures must be capable of detecting both metallic and nonmetallic threats.''[23] TSA has determined that AIT is the best method currently available to screen passengers for both metallic and nonmetallic threats concealed under clothing.

As explained in the NPRM, Congress has directed that TSA prioritize the development and deployment of new technologies to detect all types of terrorist weapons at airport screening checkpoints, including the submission of a strategic plan to promote the optimal utilization and deployment of a range of detection technologies, including, ''backscatter x-ray scanners.''[24] TSA has complied with this statute and with the subsequent statutory requirement that all AIT units used for passenger screening be equipped with ATR software, which eliminates passenger-specific images and only produces a generic outline.[25] Since May 16, 2013, all AIT units deployed by TSA have been equipped with ATR software; AIT units that could not accommodate ATR software have been removed from the airports.

E. Congressional Directive To Deploy AIT

Comments: Some commenters addressed the 2004 congressional directive discussed in the NPRM regarding the development and deployment of new screening equipment. An individual commenter noted that this congressional direction specifically included the investment in and deployment of AIT. Other commenters, however, stated that TSA's implementation of AIT is inconsistent with congressional direction. Specifically, a privacy advocacy group stated that TSA's deployment of AIT is inconsistent with a qualifier in the congressional directive—that the agency develop equipment to detect threats that terrorists would likely try to smuggle aboard an air carrier aircraft.[26] The commenter stated that TSA has demonstrated an overly broad interpretation of the congressional authorization and that, although the agency repeatedly cites AIT's abilities to identify weapons, the NPRM does not establish how such weapons are likely to be smuggled aboard planes by terrorists. The commenter further stated that TSA must analyze and evaluate AIT and alternatives regarding the ability to detect weapons and explosives likely to be used by terrorists, and demonstrate that AIT best achieves that goal with concrete evidence. The commenter stated that the analysis on which TSA currently relies fails to do either satisfactorily.

One individual commenter stated that a congressional directive is insufficient to supplant TSA's duty to make a reasoned decision regarding the use of AIT. An individual commenter expressed concern that TSA did not act in accordance with the congressional direction because the agency acted without either public input or independent testing, and pursued a technology the commenter stated was purchased as part of a ''corrupt deal.'' Another individual commenter stated that Congress authorized TSA to procure and deploy AIT only as a secondary screening tool at security checkpoints—not as a primary means of screening. Other individual commenters stated that even if Congress has authorized the proposed deployment of AIT, the proposed use of AIT is not necessarily legal or the appropriate course of action, and TSA was not performing the agency's own due diligence in trying to restrain the executive and legislative branches subsequent to congressional direction.

TSA Response: TSA is in compliance with Federal law, as well as congressional directives to pursue the development of new, advanced detection technology.[27] AIT addresses a critical vulnerability in aviation security. While WTMD and hand-held metal detectors are unable to screen for nonmetallic items, AIT can detect non-metallic explosives and other non-metallic threats, such as plastic firearms and knives. Explosives Trace Detection Devices (ETD) screen for nonmetallic explosives, but the process is too slow to perform on the same number of passengers as are currently screened by AIT. Congress clearly recognized this issue when it directed TSA 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.''[28] There is no requirement in the statute or in any of the congressional reports to limit the use of AIT to secondary screening.

AIT provides greater detection capability for weapons, explosives, and other threats concealed on a passenger's body that may not trigger a metal

[16] 49 U.S.C. 114(d).

[17] 49 U.S.C. 114(f).

[18] Public Law 107–71 (115 Stat. 597, Nov. 19, 2001).

[19] 14 CFR part 108, 66 FR 37330 (July 17, 2001). The FAA Administrator prescribed regulations requiring air carriers to screen all passengers and property before boarding.

[20] *See* 14 CFR 191.7(a) (2001).

[21] 49 U.S.C. 44902(a) and 44903(b).

[22] 49 U.S.C. 44903(b)(1),(2), and (3).

[23] *Ruskai* v. *Pistole,* 775 F.3d, 61, 63 (1st Cir. 2014).

[24] 49 U.S.C. 44925(a) and (b). ''Detection Equipment at Airport Screening Checkpoints,'' Report to Congress, Aug. 9, 2005. *See also* 78 FR 18292.

[25] 49 U.S.C. 44901(l).

[26] 49 U.S.C. 44925(a).

[27] *See* 49 U.S.C. 44925(a) and 44901(l).

[28] 49 U.S.C. 44925(a).

detector. Concealed threat items, including nonmetallic explosives, pose a substantial threat to aviation security. As the former TSA Administrator explained in an August 2013 speech to the Airports Council International/North America, ''With respect to the evolving security challenges we all face today, one of the principal concerns we have is the continued migration to more nonmetallic threats such as liquid and plastic explosives.'' [29] As explained in the NPRM, on December 25, 2009, a bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in Umar Farouk Abdulmutallab's attempt to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear. 78 FR 18291. More recently, in the spring of 2012, AQAP developed another concealed, nonmetallic explosive that had a new level of redundancy in the event the primary system failed. Fortunately, this plot was thwarted.[30] Additionally, open source information shows that terrorists currently plan to conduct attacks against the United States. Terrorists test the limits of TSA's ability to detect nonmetallic explosives concealed under clothing; the destruction of passenger aircraft remains a terrorist priority.

F. Compliance With the Administrative Procedure Act

Comments: Some commenters addressed concerns related to the Administrative Procedure Act (APA). Generally, commenters stated that TSA has not complied with the APA's procedural requirements. Non-profit organizations, a privacy advocacy group, and individual commenters stated that TSA did not comply with APA requirements prior to initial deployment of AIT. A privacy advocacy group stated that the agency received two petitions signed by numerous civil liberties organizations to institute a rulemaking proceeding, yet failed to initiate such a proceeding. A few individual commenters stated that if TSA had initially complied with rulemaking procedures, the public likely would have rejected the proposed action, and TSA would not have been able to deploy the technology. A privacy advocacy group and an individual commenter raised further concerns regarding the money spent on the deployment of AIT despite the lack of opportunity for public comment.

Commenters stated that the proposed rule and justification provided in the NPRM would not meet the arbitrary and capricious standard applied to agency actions under the APA. A privacy advocacy group stated that factors regarding effectiveness, alternatives, and health risks were not considered and the term ''anomaly'' was not adequately explained.

Commenters also stated that the proposed regulatory language effectively failed to provide the public with adequate notice and denied the public the opportunity to provide meaningful comment because the rule is too broad and vague, and descriptive information on the program was omitted.

An individual commenter wrote that noncompliance with APA requirements indicated TSA acts as it chooses without accountability. Another individual commenter requested TSA to commit to complying with APA requirements in the future. A non-profit organization requested that TSA hold public hearings in the future before imposing new procedures and policies, but specified that the agency should retain the authority to declare emergency regulations and procedures without public hearings or a comment period. Further, an individual commenter suggested that TSA withdraw the proposed rule and issue an advance notice of proposed rulemaking to allow TSA to gather missing information in order to receive comments that are more meaningful. An advocacy group and an individual commenter stated that TSA only issued a NPRM because it was court-ordered. Other commenters wrote that TSA had the option to request public input prior to implementing and deploying AIT scanners.

TSA Response: As discussed above, TSA deployed AIT consistent with its statutory authority and as directed by Congress. TSA issued the NPRM consistent with the opinion of the U.S. Court of Appeals for the DC Circuit in *EPIC* v. *DHS,* 653 F.3d 1 (D.C. Cir. 2011). In that case, TSA contended it had properly processed letters it received from EPIC and other groups regarding the initiation of a rulemaking proceeding. TSA also described how the deployment of AIT was consistent with statutory exceptions to the notice-and-comment requirements of the APA. The court did not agree. ''None of the exceptions urged by the TSA justifies its failure to give notice of and receive comments upon such a rule.'' [31] The court explained that,

> [d]espite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon his or her personal privacy in a way a magnetometer does not. Therefore, regardless whether this is a 'new substantive burden,'. . . the change substantively affects the public to a degree sufficient to implicate the policy interests animating notice-and-comment rulemaking.[32]

A subsequent decision by the same court, however, indicates that TSA's decision not to engage in rulemaking prior to deploying AIT was not unreasonable. Following the court's APA ruling, EPIC petitioned the court to recover attorney's fees under the Equal Access to Justice Act (EAJA). 28 U.S.C. 2412(d). The EAJA allows attorney's fees to be recovered unless the position of the government ''was substantially justified or . . . special circumstances make an award unjust.'' [33] In denying EPIC's request to recover attorney's fees, the court stated, ''[t]he TSA's position regarding the only issue on which EPIC prevailed—whether the agency improperly bypassed notice and comment in adopting the new screening technology—was substantially justified.'' [34]

Federal regulation stipulates that no individual may enter the sterile area of an airport or board an aircraft without submitting to the screening and inspection of his or her person and accessible property ''in accordance with the procedures being applied to control access to that area or aircraft. . . .'' 49 CFR 1540.107(a). This requirement was originally promulgated by the FAA through notice and comment rulemaking and then transferred to TSA by ATSA.[35]

Although TSA acknowledges that it did not engage in notice and comment rulemaking related to the deployment of AIT specifically prior to its use, TSA does not agree with statements by commenters that there was no public notice of TSA's use of AIT. Prior to the deployment of AIT, TSA conducted years of testing on the safety, effectiveness, and efficiency of the

[29] John S. Pistole, TSA Administrator, address at the Airports Council International–North America (Aug. 14, 2013). Text available at *https://www.tsa.gov/news/speeches/airports-council-international-%E2%80%93-north-america-tsa-administrator-john-s-pistole-0.*

[30] *Id.* Note that these examples occurred on flights originating outside of the United States. Therefore, TSA's AIT would not have been in place to detect the devices.

[31] *EPIC,* 653 F.3d at 11.

[32] *Id.* at 6.

[33] 28 U.S.C. 2412(d)(1)(A).

[34] *EPIC* v. *DHS,* No. 10–1157 (Order filed Feb. 15, 2012).

[35] *See* 62 FR 41730, 63 FR 19691, and 66 FR 37330, 37360. The ATSA transferred that authority from FAA to TSA in 2001. On February 22, 2002, the TSA and FAA published a final rule titled ''Civil Aviation Security Rules,'' 67 FR 8340, transferring the regulations at 14 CFR parts 107, 108, 109 and 191 to 49 CFR parts 1540, 1542, 1544, 1548, and 1520, and §§ 129.25 and 129.26 to part 1546.

technology.[36] Contrary to the assertion of a commenter regarding the purchase of AIT equipment, the AIT equipment was obtained in accordance with all government procurement requirements, which includes the public solicitation of bids.[37] TSA also considered alternatives to AIT and these are discussed in the NPRM and the RIA. In 2007, TSA initiated the first pilot test of AIT in the secondary screening position. In January 2008, TSA published a Privacy Impact Assessment (PIA), which encompassed AIT screening of all passengers, both as a primary and secondary form of passenger screening.[38] The PIA provided notice to the public regarding TSA's use of the technology. It stated that TSA published extensive information on the technology on its Web site beginning in February 2007 and conducted outreach with national press and with privacy advocacy groups to explain the evaluation of the technology. The PIA explained that informational brochures were made available to the public at each pilot site showing the image that the technology created. The cover page of each PIA includes a point of contact for the public to reach out to with questions or concerns. In 2009, TSA began to test AIT as the primary screening equipment. In 2010, TSA submitted a Report to Congress on privacy protections and deployment of AIT.[39] TSA also published information on its Web site to inform passengers of AIT procedures at the checkpoint at *www.tsa.gov.* The public may provide comments or concerns regarding AIT by contacting the TSA Contact Center.[40]

As directed by the court, TSA issued the NPRM and invited public comment on its proposed regulation regarding the use of AIT for primary screening of passengers. The NPRM invited public comment on a variety of issues related to the use of AIT, including the threat to aviation security, types of AIT equipment, privacy safeguards, safety, AIT procedures and items discovered using AIT. TSA received thousands of comments on these issues. In response to comments and to avoid confusion, TSA has altered the regulatory text in the final rule. TSA has determined not to define AIT using the term ''anomaly''; instead, TSA has adopted the statutory definition of AIT, *i.e.,* a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body. In addition, TSA has clarified the final rule by adopting the statutory provision to deploy AIT equipped with ATR software. Thus, AIT equipment must produce a generic image of the individual being screened that is the same as the images produced for all other screened individuals. These changes are in response to the concerns of commenters regarding the breadth of the regulatory text, and significantly mitigate any privacy concerns associated with the use of AIT as a primary screening method. Accordingly, and consistent with TSA's obligation to complete this rulemaking and TSA's discretion to prioritize its rulemaking resources, TSA does not intend to issue a supplemental NPRM or hold public hearings on this matter. TSA addresses issues regarding effectiveness and safety in subsequent responses.

G. Adherence to the Court Decision in EPIC v. DHS

Comments: Commenters also discussed the court's decision in *EPIC* v. *DHS.* Several individual commenters specifically supported EPIC's position that AIT scanners are invasive of individual privacy. Another individual commenter opposed the court's decision to allow TSA to continue use of AIT. A privacy advocacy group wrote that the NPRM incorrectly stated the holding of the case. A privacy advocacy group and many individual commenters pointed out the length of time that elapsed between the court decision and the issuance of the NPRM. A privacy advocacy group stated that it filed three mandamus petitions during the elapsed 2-year period. An advocacy group stated that the constitutional issue raised by EPIC was not ripe for decision because the court did not have a rulemaking record before it and speculated that the court might invalidate its holding regarding the Fourth Amendment in a future judicial review of this rulemaking.

TSA Response: TSA is in compliance with the court's directive to engage in notice-and-comment rulemaking on the use of AIT to screen passengers. TSA notes that all of EPIC's other constitutional and statutory challenges to the use of AIT, including its Fourth Amendment claims, were rejected by the court. The court also rejected EPIC's petition for rehearing (including the Fourth Amendment ruling), as well as three subsequent petitions that EPIC filed demanding immediate issuance of the NPRM. TSA notes that the court issued its decision before TSA instituted ATR software on all of the millimeter wave AIT units and removed all of the backscatter units from service. The ATR software does not produce an individual image of a passenger that must be reviewed by a TSO, but instead reveals a generic outline that is visible to the passenger as well as the TSO. In a recent case decided after these changes in AIT equipment were implemented, the U.S. Court of Appeals for the First Circuit held that a constitutional challenge to AIT body scanners that depict revealing images of bodies and pat-downs procedures for passengers who opted out of screening using AIT became moot following the installation of ATR software on all millimeter wave units and the removal of backscatter machines.[41]

H. Fourth Amendment Issues

Comments: Commenters also addressed concerns related to the Fourth Amendment. The vast majority of these commenters stated that use of AIT constitutes a violation of Fourth Amendment rights. Individual commenters stated that AIT fails to meet the standard of a constitutionally permissible search. Specifically, some individual commenters stated that TSA could not conduct such searches without a warrant. Individual commenters also stated that neither the purchase of an airline ticket nor a desire to travel is sufficient to give TSA ''probable cause'' to conduct a search.

Others stated that AIT is impermissible under Federal case law. Several individual commenters cited the holding in *U.S.* v. *Davis,* in which the U.S. Court of Appeals for the Ninth Circuit held that administrative searches must be ''no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to

[36] *See, e.g.,* ''Detection Equipment at Airport Screening Checkpoints,'' Report to Congress, Aug. 9, 2005. The report describes TSA's ongoing research and development program to develop technologies to increase its ability to detect explosives on passengers, including body imaging systems, *i.e.,* backscatter x-ray.

[37] *See* The TSA is seeking sources for Imaging Technology systems, Solicitation No. HSTS04–08–R–CT2056, *https://www.fbo.gov/index?s=opportunity&mode=form&id=be7cd5b087bd3d28ce6bee81f7644141&tab=core&_cview=1.*

[38] ''Privacy Impact Assessment for TSA Whole Body Imaging,'' Jan. 2, 2008. Updates to the initial AIT PIA were conducted on Oct. 17, 2008, Jul. 23, 2009, and Jan. 25, 2011. See *http://www.dhs.gov/publication/dhstsapia-032-advanced-imaging-technology.* All TSA PIA reports are available at *http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.*

[39] ''Advanced Imaging Technologies: Passenger Privacy Protections,'' Fiscal Year 2010 Report to Congress, Feb. 25, 2010.

[40] *https://www.tsa.gov/contact.*

[41] *Redfern* v. *Napolitano,* 727 F.3d 77, 83–85 (1st Cir. 2013).

fly.''[42] Several individual commenters stated that the AIT screening process fails to meet this standard because elements of the scan and the opt-out alternative are too intrusive, and the scope of the scan is not tailored narrowly enough to exclusively identify weapons, explosives, and incendiaries (*e.g.,* AIT is able to identify items such as adult diapers and women's sanitary products, which commenters stated are outside the scope of threats TSA is trying to identify). Individual commenters recommended alternative search methods that they thought were less invasive and better suited to meet TSA's need, such as x-raying suitcases, using WTMD, and only using AIT as a secondary means of screening.

Other court cases cited in the comments to support claims that AIT violates the Fourth Amendment include: *U.S.* v. *Pulido-Baquerizo,* 800 F.2d 899 (9th Cir. 1986), *U.S.* v. *Skipwith* 482 F.2d. 1272 (5th Cir. 1973), *U.S.* v. *Hartwell,* 436 F.3d 174 (3d Cir. 2006), *Camara* v. *Municipal Court,* 387 U.S. 523 (1967), *Missouri* v. *McNeely,* 133 S.Ct. 1552 (2013), *Katz* v. *U.S.,* 389 U.S. 347 (1967). An individual commenter also cited a court decision pertaining to virtual strip searches, *Reynolds* v. *City of Anchorage,* 379 F.3d 358 (6th Cir. 2004) to support opposition to AIT.

An individual commenter observed that, even though AIT use was not found to be in violation of the Fourth Amendment in *EPIC* v. *DHS,* the subsequent issuance of an NPRM, which does not specify the degree to which AIT will be used to promote the government's interest, may result in TSA's failure to meet the balancing test applied to Fourth Amendment rights cases.

TSA Response: The court in *EPIC* held that the use of AIT as a primary screening method at an airport security checkpoint does not violate the Fourth Amendment.[43] This decision is consistent with decisions by the U.S. Supreme Court and the Federal circuits that have upheld airport security screening as a valid administrative search that does not require a warrant, probable cause, reasonable suspicion, or the consent of the passenger.[44] More than 30 years ago, the U.S. Court of Appeals for the Third Circuit recognized that the government ''unquestionably has the most compelling reasons,'' including ''the safety of hundreds of lives and millions of dollars' worth of private property for subjecting airline passengers to a search for weapons and explosives.'' *Singleton* v. *Comm'r of Internal Revenue,* 606 F.2d 50, 52 (3d Cir. 1979). ''[T]he events of September 11, 2001, only emphasize the heightened need to conduct searches at this nation's international airports,'' *U.S.* v. *Yang,* 286 F.3d 940, 944 n.1 (7th Cir. 2002). In a recent opinion issued by the U.S. Court of Appeals for the Eleventh Circuit, the Court concluded that AIT ''is a reasonable administrative search under the Fourth Amendment.''[45]

Like other exceptions created by courts for searches that do not require a warrant, the administrative search within the airport context reflects the careful balancing of the public's privacy interests against the compelling goal of protecting the traveling public. As explained by the D.C. Circuit in *EPIC,* because the primary goal of airport screening is ''not to determine whether any passenger has committed a crime but rather to protect the public from a terrorist attack,'' airport screening is permissible under the Fourth Amendment without individualized suspicion so long as the government's interest in conducting screening outweighs the degree of intrusion on an individual's privacy.[46] The court made clear that this standard does not require the government to use the least intrusive search method possible.[47] In fact, the U.S. Supreme Court has held that the scope of the administrative search must be ''reasonably related to [its] objectives'' and ''not excessively intrusive.''[48] In *EPIC,* the court found that the—

> balance clearly favors the Government here. The need to search airline passengers 'to ensure public safety can be particularly acute,' and, crucially, an AIT scanner, unlike a magnetometer, is capable of detecting, and therefore of deterring, attempts to carry aboard airplanes explosives in liquid or powder form. On the other side of the balance, we must acknowledge the steps TSA has already taken to protect passenger privacy, in particular distorting the image created using AIT and deleting it as soon as the passenger has been cleared.[49] [Citations omitted]

With the addition of ATR software and the elimination of any individual image, the balance tips even more in favor of the government. Courts have also held that, ''absent a search, there is no effective means of detecting which airline passengers are reasonably likely to hijack an airplane.''[50]

Commenters' claims and citations to support the position that the least intrusive search method must be adopted are contrary to U.S. Supreme Court precedent in *Quon,* as well as the *EPIC* decision. In fact, the court in *EPIC* specifically rejected the argument that *U.S.* v. *Hartwell,* cited in many of the comments, stands for the proposition that AIT scanners must be minimally intrusive to be consistent with the Fourth Amendment.[51] Moreover, especially following the universal deployment of ATR software, TSA believes that the use of AIT as a primary screening method is not intrusive. The scan and the results require just a few seconds. Passengers are not subjected to any physical intrusion. The only potential for invasiveness occurs when AIT alarms, thereby requiring additional screening to verify whether a threat item is present.[52] Passengers are instructed through TSA's Web site and cautioned before they enter the AIT unit to remove all items from their pockets to prevent an alarm.

TSA is not required to use any of the alternatives to AIT mentioned in the comments to achieve the legal requirements of a valid search. For example, all baggage, whether checked or carry-on, is already screened as required under 49 U.S.C. 44901. Limiting an airport search to baggage, however, would not address the threat that a person could conceal an explosive on his or her person. The government has latitude under the Fourth Amendment to choose among

---

[42] 482 F.2d 893, 913 (9th Cir. 1973).

[43] *EPIC,* 653 F.3d at 10.

[44] *Chandler* v. *Miller,* 520 U.S. 305, 323 (1997) (''We reiterate, too, that where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as 'reasonable'–for example, searches now routine at airports''), *Nat'l Treasury Emps. Union* v. *Von Raab,* 489 U.S. 656, 675 n.3 (1989) (''The point [of valid suspicionless searches] is well illustrated also by the Federal Government's practice of requiring the search of all passengers seeking to board commercial airlines . . . without any basis for suspecting any particular passenger of an untoward motive.''), *U.S.* v. *Aukai,* 497 F.3d 955, 960 (9th Cir. 2007) (en banc) (''The constitutionality of an airport screening search, however, does not depend on consent.'').

[45] *Corbett* v. *TSA,* 767 F.3d 1171, 1180 (11th Cir. 2014) (''The scanners at airport checkpoints are a reasonable administrative search because the governmental interest in preventing terrorism outweighs the degree of intrusion on . . . privacy and the scanners advance that public interest.'').

[46] *EPIC,* 653 F.3d at 10.

[47] *Id.* at 10–11.

[48] *City of Ontario* v. *Quon,* 560 U.S. 746, 761 (2010) (internal quotation marks omitted).

[49] *EPIC,* 653 F.3d at 10.

[50] *See Singleton* v. *Comm'r of Internal Revenue,* 606 F.2d 50, 52 (3d Cir. 1979). *See also U.S.* v. *Marquez,* 410 F.3d 612, 616 (9th Cir. 2005) (''Little can be done to balk the malefactor after weapons or explosives are successfully smuggled aboard, and as yet there is no foolproof method of confining the search to the few who are potential hijackers.'' (quoting *Davis,* 482 F.2 at 910)).

[51] *EPIC,* 653 F.3d at 10–11.

[52] In other limited circumstances, based on the particular item of clothing, TSA may require additional screening even if the AIT does not alarm.

reasonable alternatives for conducting an administrative search.[53] AIT is the only technology that will find both metallic and non-metallic items, and will find both explosives and non-explosives items. The WTMD only finds metallic items, thus does not find such threats as explosive devices made without metal, or other non-metallic items. The ETD will find only explosives, not metallic items (such as firearms) or non-metallic items that are not explosives (such as ceramic knives); the same is true for explosives detection canines. Pat-down screening is useful for finding both metallic and non-metallic items, and will find both explosives and non-explosives items, however, that method is slower than AIT and many persons consider pat downs to be more intrusive than AIT.

The other cases cited in the comments, particularly those relating to whether consent is required for airport screening, are inapplicable. Both *U.S.* v. *Davis,* 482 F.2d 893 (9th Cir. 1973) and *U.S.* v. *Pulido-Baquerizo,* 800 F.2d 899 (9th Cir. 1986) regarding whether a passenger must consent to a search, have been superseded by the decision of the U.S. Court of Appeals for the Ninth Circuit in *U.S.* v. *Aukai.*[54] In *Aukai,* the court confirmed that airport screening searches are constitutionally reasonable administrative searches and clarified that the reasonableness of such searches does not depend, in whole or in part, upon the consent of the passenger being searched.[55] *U.S.* v. *Skipwith,* 482 F.2d 1272 (5th Cir. 1973), deals with a law enforcement search based on suspicion, which is not required for the administrative search performed by TSA. Neither *Camara* v. *Municipal Court,* 387 U.S. 523 (1967), *Missouri* v. *McNeely,* 133 S. Ct. 1552 (2012), nor *Katz* v. *U.S.,* 389 U.S. 347 (1967) involves the administrative search conducted by TSA at airport security checkpoints, which courts have consistently found is justified by the compelling government interest in protecting the traveling public.[56]

Finally, the reference to strip search cases by a commenter is not applicable to AIT given the privacy restrictions TSA used when it first deployed AIT and even more so now that all AIT units are equipped with ATR software and do not display an individual image. In addition, the AIT units do not have the ability to store, print, or transmit any images. As noted previously, a TSO does not usually touch a passenger's body unless the AIT alarms. With ATR, there is no individual image of a traveler; the generic outlines produced are so innocuous that they are displayed publicly at the airport.

I. Other Legal Issues

Comments: Commenters raised other legal issues in opposing AIT. Several individual commenters, a non-profit organization, and several advocacy groups stated that AIT scanning and/or opt-out process violates rights guaranteed by the First, Second, Fifth, Sixth, Eighth, Ninth, Tenth, and Fourteenth Amendments, respectively. Commenters did not generally provide further substantive legal arguments in support of these constitutional claims. An advocacy group, however, cited a Supreme Court case, *Aptheker* v. *Sec'y of State,* 378 U.S. 500, 505 (1964), which held that if a law ''too broadly and indiscriminately restricts the right to travel'' it ''thereby abridges the liberty guaranteed by the Fifth Amendment.'' The commenter further stated that the court considered relevant ''that Congress has within its power 'less drastic' means of achieving the congressional objective of safeguarding our national security.'' An individual commenter cited *U.S.* v. *Guest,* 383 U.S. 745 (1966) and *Shapiro* v. *Thompson,* 394 U.S. 618 (1969) in opposing the use of AIT. Another advocacy group cited 49 U.S.C. 40101, 40103, and the International Covenant on Civil and Political Rights, a treaty that the U.S. has ratified, as further reinforcing the right to travel. The commenter remarked that the NPRM does not recognize that travel by air and, specifically, by common carrier, is a right and that TSA must evaluate its proposed actions within that context. Similarly, an individual commenter stated that TSA's use of AIT involves limitations on constitutional rights and, therefore, strict scrutiny should be the judicial review standard applied. Another individual commenter stated that implementation of AIT scanners assumes travelers' guilt, which is in violation of the principle of the presumption of innocence.

One individual commenter stated that it is outside of TSA's mission to identify and confiscate items that are not a threat (*e.g.,* illegal drugs) and that such ''mission creep'' is an inappropriate use of Federal funds and distracts TSA staff from their actual mission. Other individual commenters stated that AIT and pat-downs violate laws prohibiting sexual molestation. A non-profit organization suggested that TSA review and modify its policies to ensure that they do not conflict with existing state law procedures protecting children from physical and sexual assault or with existing child protective services legislation.

TSA Response: As to the claims of violations of the Constitution, as explained in the response to the previous grouping of comments, in recognition of the importance of the safety concerns at issue, courts have regularly upheld airport screening procedures against constitutional challenges. Thus, it is well settled as a matter of law that an airport screening search conducted to protect the safety of air travelers is a legitimate exercise of government authority and does not impinge on any of the constitutional amendments listed in the comments. Passengers are on notice that their persons and their property are subject to search prior to entering the sterile area of the airport or boarding an aircraft. Federal law requires ''the screening of all passengers and property'' before boarding an aircraft to ensure no passenger is ''carrying unlawfully a dangerous weapon, explosive, or other destructive substance.'' 49 U.S.C. 44901(a) and 44902(a). Federal law also requires commercial air carriers to prevent anyone from boarding who does not submit to security screening. 49 U.S.C. 44902(a).

The use of AIT to conduct passenger screening does not implicate any constitutional rights in the manner described in the comments. Passengers are not restricted regarding their speech or right to assemble so long as they do not interfere with screening.[57]

[53] *Quon,* 560 U.S. at 764 (''Even assuming there were ways that [the government] could have performed the search that would have been less intrusive, it does not follow that the search conducted was unreasonable.'').

[54] *U.S.* v. *Aukai,* 497 F.3d 955 (9th Cir. 2007) (en banc).

[55] *Aukai,* 497 F.3d at 957.

[56] *See generally Marquez,* 410 F.3d 612,618 (''It is hard to overestimate the need to search air travelers for weapons and explosives'') and *Singleton,* 606 F.2d 50, 52 (''the government unquestionably has the most compelling reasons . . . for subjecting airline passengers to a search for weapons or explosives that could be used to hijack an airplane.''). The facts in *Camara* involved the attempted search of a home without a warrant. The Supreme Court found that the government was not able to articulate a special need or legitimate public interest to justify dispensing with the requirement to obtain a warrant. In *McNeely,* a blood test of a person suspected of driving while intoxicated was obtained without a warrant. In *Katz,* the Supreme Court held that electronically listening to and recording an individual's conversation at a public telephone booth without a warrant violated the Fourth Amendment.

[57] Interference with screening is prohibited by 49 CFR 1540.109. TSA defines interference in part as that which ''might distract or inhibit a screener from effectively performing his or her duties,'' to include verbal abuse of screeners by passengers or air crew, but not good-faith questions from individuals seeking to understand the screening of

Continued

Passengers may transport unloaded firearms in checked baggage in a locked, hard-sided container, thus, there is no infringement of Second Amendment rights. 49 CFR 1540.111. In general, the Fifth, Sixth, and Eighth Amendments have to do with the rights of persons accused of a crime and have no relevance to airport security screening conducted by TSA. Federal law requires that screening be conducted on all passengers and property prior to boarding an aircraft, and rights reserved for citizens or the states, discussed in the Ninth and Tenth Amendments respectively, are not impacted by airport screening. Comments invoking the Fourteenth Amendment generally did so without specifying which clause of the Amendment is at issue the or how it was implicated by AIT, or invoked it in connection with non-AIT aspects of TSA screening.

Federal courts have long held that airport screening searches do not violate a traveler's right to travel.[58] ''Air passengers choose to fly, and screening procedures . . . have existed in every airport in the country since at least 1974.'' [59] The holding in *Aptheker,* cited by a commenter, pertained to whether Section 6 of the Subversive Activities Control Act of 1950, which restricted members of Communist organizations in obtaining or using a passport, was constitutional. It has no application to the use of AIT to conduct airport screening, which does not restrict a person's right to travel, the ability to obtain a passport, or the ability to obtain documentation necessary to enter a country legally. Further, the Ninth Circuit Court of Appeals has held that TSA's regulation requiring passengers to present identification prior to entering a sterile area or boarding an aircraft, 49 CFR 1540.107(b), does not violate any Constitutional rights.[60]

As to the comment regarding the confiscation of items that are not a security threat such as illegal drugs, the purpose of TSA screening is to prevent weapons, explosives, and other items that could pose a security threat (prohibited items) from being carried into the sterile area of the airport or onboard an aircraft in order to ensure the freedom of movement for people and commerce. 49 CFR 1540.111. TSA's mission has not changed. TSOs do not search for other illegal items. When searching for prohibited items, however, it is not unusual for TSOs to uncover items that may be evidence of criminal activity. When that happens, the TSO turns such matters over to law enforcement officers to resolve, consistent with applicable criminal statutes. TSOs do not take possession of such items. In addition, once an anomaly is detected by AIT, or a metal object is detected by a WTMD, or either screening system misalarms, additional screening must take place to determine whether there is an item, and if so, if the item detected is a threat to aviation security. As the court in *Hartwell* noted, ''Even assuming that the sole purpose of the checkpoint was to search only for weapons or explosives, the fruits of the search need not be suppressed so long as the search itself was permissible. . . . Since the object in Hartwell's pocket could have been a small knife or bit of plastic explosives, the TSA agents were justified in examining it.'' [61]

TSA's pat-down procedures are designed to ensure that any touching of the body by a TSO is minimally intrusive while effectively screening for prohibited items. A TSO does not touch a passenger's body unless necessary to resolve an AIT alarm, or unless the passenger has opted for a pat-down, and the procedures are largely similar to those employed to resolve WTMD alarms. Touching of the body to perform this essential security function is fully within the scope of TSA's authority, and TSA's procedures are consistent with civil and criminal state laws. Sexual molestation or inappropriate touching of a passenger by an employee is strictly prohibited and TSA has procedures in place to investigate any allegations of such conduct thoroughly. TSA takes all allegations of misconduct seriously.

Passengers who believe they have experienced unprofessional conduct at a security checkpoint may request to speak to a supervisor at the checkpoint or write to the TSA Contact Center at *TSA-ContactCenter@dhs.gov.* Passengers who believe they have been subject to discriminatory treatment at the checkpoint may file a complaint with TSA's Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement (OCRL/OTE) at *TSA–CRL@tsa.dhs.gov, or submit an online complaint at https://www.tsa.gov/contact-center/form/complaints.*[62] The Office of Inspection, in addition to OCRL/OTE and management, may investigate misconduct allegations. Travelers may also file discrimination complaints concerns with the DHS Office for Civil Rights and Civil Liberties (CRCL) via CRCL's Web site at *http://www.dhs.gov/complaints.* In addition, as discussed further below, TSA has amended its screening procedures to modify the pat-down used when necessary to screen children age 12 and under and adults age 75 and older and has reduced the instances where such passengers would be subject to a pat-down.

J. Evolving Threats to Security

Comments: Commenters also addressed the evolving threats to aviation security discussed by TSA in the NPRM. Some commenters stated that TSA's screening efforts are not linked to the decrease in aircraft-related terror attempts since September 11, 2001. For example, individual commenters and a non-profit organization stated that the threat attempts listed in the NPRM were thwarted by intelligence efforts, not TSA screening. Other individual commenters, however, supported TSA's efforts to deploy tools like AIT scanners to detect and deter future attacks. Individual commenters credited secured cockpits and stricter policies for cockpit access with preventing terrorist attacks on commercial airlines since September 11, 2001. Furthermore, a few individual commenters suggested that in addition to enhanced cockpit security, passengers' awareness and willingness to fight back deters terrorists from targeting planes.

Several commenters discussed the evolving threat from nonmetallic explosives. A few individual commenters suggested that TSA's response to the increased threat of nonmetallic explosives is not sustainable because terrorists will find other ways to hide devices. A few individual commenters disagreed with TSA's focus on nonmetallic threats, because these types of weapons have been used for several decades.

---

their persons or property. *See* 67 FR 8340, 8344 (Feb. 22, 2002). Interference with screening might also include passenger activity that requires a screener to ''turn away from his or her normal duties to deal with the disruptive individual,'' or might ''discourage the screener from being as thorough as required.'' *See id.;* 49 CFR 1540.109; *Rendon* v. *TSA,* 424 F.3d 475 (6th Cir. 2005) (constitutional rights not infringed when penalty was imposed on traveler who became loud and belligerent after he set off metal detector alarm which required screener to shut down his line and call over his supervisor).

[58] *U.S.* v. *Davis,* 482 F.2d 893 (9th Cir. 1973).

[59] *Hartwell,* 436 F.3d at 174.

[60] *Gilmore* v. *Gonzales,* 435 F.3d 1125, 1136–1137 (9th Cir. 2006) (''We reject Gilmore's right to travel argument because the Constitution does not guarantee the right to travel by any particular form of transportation . . . . Gilmore does not possess a fundamental right to travel by airplane even though it is the most convenient mode of travel for him.'').

[61] *Hartwell,* 436 F.3d at 181 n.13. *See also Marquez,* 410 F.3d at 617 (''The screening at issue here is not unreasonable simply because it revealed that Marquez was carrying cocaine rather than C–4 explosives.'').

[62] More information on TSA Civil Rights is available at *https://www.tsa.gov/travel/passenger-support/civil-rights.*

A few individual commenters suggested that the long lines at checkpoints, which the commenters stated are caused by TSA screening, are more attractive targets to terrorists than airplanes. Lastly, several individual commenters stated there is no evidence indicating that terrorist threats similar in magnitude to September 11, 2001, are increasing.

TSA Response: TSA agrees that the threat to aviation security by terrorists continues to evolve as terrorists test current security measures to uncover vulnerabilities to exploit. Terrorist groups remain focused on attacking commercial aviation. The primary threat from these groups is from explosive devices, as we have seen in incidents originating abroad, such as the non-metallic bomb used by the Christmas Day bomber in 2009, the toner cartridge printer bombs from Yemen placed on two cargo aircraft destined for Chicago in 2011, and the improved ''next generation'' underwear bomb also from Yemen, recovered by a foreign intelligence service in April 2012. The incidents abroad inform us of terrorists' intentions and capabilities, and are lessons that TSA must learn from to prevent terrorists from attempting such an act here. These examples show that terrorists continue to attack aviation, are capable of constructing non-metallic explosive devices, and continue to develop new ways to do so. Open source information indicates that terrorists continue to intend violence against aviation within the United States. TSA does not agree that intelligence reporting alone is responsible for thwarting terrorist threats. TSA agrees that improvements in intelligence gathering and sharing such information, along with other layers of security, including as mentioned in the comments, hardened cockpit doors and assistance from passengers, contribute greatly to aviation security. The combination of security layers, both seen and unseen, provides the best opportunity to detect and deter a terrorist attack.

TSA also agrees that security procedures and equipment must continue to evolve as the threat evolves. As discussed above, AIT is the most effective technology currently available to detect both metallic and nonmetallic threats, both explosive and non-explosive, concealed under passenger clothing, TSA continues to research and test new equipment and procedures to stay ahead of evolving threats.

TSA agrees that long lines at the checkpoints could pose a security risk and has taken steps to address long lines by monitoring throughput. However, TSA remains focused on the fundamentals of security, and strives to strike a balance between security effectiveness and line efficiency. Passengers can obtain information before they leave for the airport on what items are prohibited; acceptable ID; rules for liquids, gels and aerosols; and traveling with children. Guidance for travelers with disabilities, medical conditions or medical devices, tips for dressing and packing, and information on traveling with food and gifts is provided. In addition, as noted in the NPRM, the Web site contains instructions on AIT screening procedures. 78 FR 18296. Preparing in advance for security screening and following the instructions of the TSOs are the most effective ways to reduce lines at the checkpoint.

K. TSA's Layers of Security

Comments: Commenters addressed the TSA layers of security discussed in the NPRM. A privacy advocacy group suggested that the layered approach discussed by TSA is not supported by data and, therefore, does not justify the need for AIT. The commenter also recommended that TSA revise the layered approach so weaknesses in security can be identified. Furthermore, a few commenters suggested that TSA focus on other security methods, such as profiling, interviewing, and ''Pre-check'' screening programs to identify dangerous individuals. An individual stated that the efficacy of AIT screening has not been scientifically proven. The commenter further suggested that since there are other approaches used by TSA to identify potential threats, AIT would be most useful as a secondary screening method instead of as the primary screening method. A professional association, however, stated that because of the advanced methodologies of adversaries, technologies like AIT scanners are needed to secure air travel. The commenter suggested that techniques involving human intervention, such as Screening Passengers by Observation Techniques, the Behavioral Detection Officer program, and passenger screening canines would also be useful. Many commenters mentioned their support for the use of racial profiling tactics instead of AIT, and argued that such measures would be more efficient and effective.

An advocacy group alleged that TSA's ''trusted traveler program'' approach would weaken security because it can eliminate entire classes of passengers from AIT screening. The commenter recommended that TSA consider other, less invasive and cost-effective screening procedures that would allow TSA to implement AIT as a secondary, rather than a primary, screening tool. Furthermore, the commenter suggested that TSA enhance layers of security by testing canine bomb detection, face recognition, and explosives residue machines, in an effort to reduce the need for AIT scanning.

TSA Response: TSA believes that a comprehensive security system is the most effective means to address potential terrorist threats, since no single security measure may be sufficient by itself. TSA also agrees that ETD, behavior detection and passenger screening canine are valuable tools to address terrorist threats, and TSA uses these at airports.

TSA does not agree with commenters that using AIT, as a secondary screening method, would be as effective as currently deployed. Limiting its use to resolve alarms of the WTMD, which can only detect metallic threats, would severely restrict our ability to prevent adversaries from smuggling non-metallic weapons and explosives on board an aircraft.

As discussed above, AIT is the best technology currently available to detect both metallic and nonmetallic threats, and explosives as well as non-explosives. TSA has tested the effectiveness of the technology, and the equipment must meet TSA detection standards to be deployed in an airport. In addition, testing is conducted by the DHS Transportation Security Laboratory (TSL). The TSL Independent Test and Evaluation group provides certification and qualification tests and laboratory assessments on explosive detection capability. TSA procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of items concealed under a person's clothing. While the detection requirements of AIT are classified, the procurement specifications state that any approved system must be sensitive enough to detect smaller items.

Regarding the comments recommending racial profiling, transportation security screening is regulated by the Constitution, federal law, and applicable DHS and component policies setting forth the appropriate limits on use of race, ethnicity, and other characteristics. In addition, racial profiling is not an effective security measure and can easily be defeated. It is premised on the erroneous assumption that any particular individual of one race or ethnicity is more likely to engage in misconduct than any particular individual of another race or ethnicity. In addition to being ineffective, profiling violates DHS policies and ultimately undermines the public trust. TSA disagrees with the commenter who wrote that TSA's trusted traveler program would weaken security. The TSA Pre✓™ program is based on the premise that most passengers do not pose a risk to aviation security. This program will permit those passengers who voluntarily provide information for a security risk assessment to undergo expedited screening and allow TSOs to devote more time to screening unknown passengers.

L. Effectiveness of AIT Screening

Comments: Many commenters made general statements that AIT scanners are not effective in addressing security threats. An individual commenter stated that because TSA has not released data regarding the effectiveness of AIT scanners and the number of prohibited items detected by AIT, the NPRM would not be taken seriously. Some commenters, including a privacy advocacy organization and a community organization, stated that TSA has not provided enough information about what AIT can detect. The commenter stated that the agency has not made a distinction between an ''anomaly'' and a ''threat.'' Commenters also stated that the use of AIT scanners makes air travel more vulnerable to terrorism.

Many submissions discussed the efficacy of AIT to detect anomalies concealed under the clothing of a passenger. Some commenters stated that AIT scanners are not effective because they cannot detect items that are concealed under fake skin, under skin folds, or under shoes, implanted bombs, and objects hidden inside of a person. A few individuals stated that objects are not detected if concealed on the side of the body. A commenter stated that a passenger was able to bring an empty metal box concealed under clothing through AIT units without detection. The commenter believed that the metal box was not detected because the rate at which the AIT beams reflect off the metal is the same rate at which beams reflect the background. The commenter stated that if an object like the metal box were placed at the side of a body, the object beam reflection would look no different from the blackened background. According to another individual commenter, a peer-reviewed publication in the Journal of Homeland Security stated that explosives with low ''Z'' like plastics look like flesh to the scanner because flesh is also low ''Z.'' A few individual commenters referred to a video posted by a blogger that the commenters stated portrayed a man who was able to conceal objects (both metal and nonmetal) from an AIT scanner by sewing the objects into the lining of his shirt.

Some commenters discussed the ability of AIT to detect plastic, powder, and liquid explosives. One individual commenter stated that a 2007 government audit found that agents were able to pass through security checkpoints with explosives and bomb parts. Commenters stated that the explosives used by the ''underwear bomber'' and ''shoe bomber'' would not be detected by AIT. A commenter stated that a 2010 Government Accountability Office (GAO) report indicated that it remains unclear whether the AIT would have detected the weapon used in the December 2009 Christmas Day bomber incident based on the preliminary information GAO had received. An advocacy group also expressed concern that AIT scanners cannot detect pentaerythritol tetranitrate (the powder explosive the group states was used by the Christmas Day bomber), and claimed that this chemical continues to be used in other domestic and international terror attempts. An individual commenter alleged AIT could not detect explosives molded into specific shapes. Another individual commenter stated that since there are claims that AIT cannot detect powder explosives, AIT scanners are not fulfilling the statutory provision at 49 U.S.C. 44925 which TSA has used as justification for deploying AIT.

An individual commenter suggested that, although the AIT scanners can adequately detect metal in firearms and concealed knives, security screening should also be able to detect explosives with negligible false negative rates and low false positive rates. The commenter recommended that a reasonable detection limit would be no lower than 20 percent of the amount of the explosive needed to bring an airplane down. The commenter suggested that systems that detect significant quantities of explosives or detonators should be used for screening baggage and items concealed under clothing.

A few individuals expressed concern that because AIT on its own cannot differentiate between threatening objects and non-threatening objects, passengers carrying non-threatening objects are subject to more intrusive, secondary searches including pat-downs. A community organization stated that travelers of the Sikh religion are often subject to secondary searches even when the AIT scanner did not identify any anomalies. Similarly, an individual commenter stated that, although AIT scanners can detect anomalies, often times a pat-down could not resolve whether the anomaly is a threat. An individual commenter, however, remarked that continued use of AIT would reduce the number of pat-downs as well as enhance detection of nonmetallic weapons, because AIT is effective in detecting threats. The commenter suggested that AIT checkpoints be re-designed to minimize the level of intrusion and embarrassment associated with scanned images.

Many commenters wrote that AIT scanners are no more effective at addressing security threats than other, less invasive screening methods. A few individual commenters and advocacy groups suggested that the NPRM has not adequately justified the ability of AIT to reduce significantly the threat of terror attacks on aircraft compared to alternative screening practices. Some individual commenters stated that the WTMD is more effective at detecting metallic items than AIT. A few of these individual commenters remarked that WTMD is as effective as AIT overall, but they preferred WTMD because it is less invasive than AIT. An advocacy group suggested that a cost-benefit analysis of AIT would certainly justify the scanners if they were effective in deterring terrorism compared to screening alternatives. An individual commenter also stated there is not enough evidence of increased threats using nonmetallic objects to justify the need for body scanners. The commenter explained that prior to AIT, nonmetallic objects were addressed by less-invasive means including WTMDs, bomb-sniffing dogs, Federal Air Marshals, and explosives detection machines. The commenter also stated that nonmetallic weapons that are small enough to conceal on the body do not pose a threat. One individual commenter, however, discussed examples where the use of the AIT scanner was instrumental in identifying weapons concealed under clothing. The commenter stated that there is no alternative technology that can assist in detecting explosives and other harmful objects that can be used to harm travelers.

Many commenters, including a non-profit organization, an advocacy group, and individual commenters, made general statements that AIT scanners are ineffective because of reported high false positive rates. An individual commenter stated that travelers might be more accepting of the invasiveness of AIT scanners if TSA revealed data regarding the effectiveness of the technology (*i.e.,* false positives and false positive rates). Several commenters, including a non-profit organization and a community organization, stated that the false detection of non-threatening objects leads to pat-downs where passengers are subjected to unnecessary, invasive screening. An individual referenced incidents which, the commenter stated, caused passengers embarrassment when their medical device raised a false positive. An individual commenter argued that the high rate of false positives causes security checkpoint lines to move slowly, which subsequently requires TSA to use WTMDs to relieve the backup. A few individuals expressed concern regarding a false sense of security created for TSA officers and passengers by the large volume of false alarms caused by AIT scanners. The commenters concluded that this false sense of security weakens security. Similarly, an individual commenter remarked that the process of responding to false positives (searching for non-threatening objects) takes TSA's focus off identifying actual threats.

An individual commenter stated that AIT scanners are not effective in identifying a passenger with a threatening weapon because passengers can travel from airports or terminals that do not use AIT scanners. The commenter stated that passengers could also avoid detection by placing a weapon on a companion passenger under 12 years of age or on a pet. The commenter also stated that AIT scanners are ineffective at making air travel safer because the long lines make passengers more vulnerable to terror attacks. An individual commenter, however, wrote that the AIT scanners are more effective as a deterrent to terrorists than random pat-downs or profiling because of the expectation that the AIT will scan all passengers entering the sterile area.

TSA Response: TSA cannot fully address the specific detection capabilities of AIT in the final rule, because much of the information is classified. As explained in the NPRM, AIT is able to detect both metallic and nonmetallic items concealed under an individual's clothing. The NPRM describes some of the items concealed under clothing that have been detected by AIT. 78 FR 18297. AIT equipment must meet detection specifications and overall performance standards established by TSA. The AIT machines are tested regularly to ensure that the detection capabilities and performance standards are maintained. After years of testing and operational experience at the airport, TSA maintains that AIT provides the best opportunity currently available to detect both metallic and nonmetallic threats concealed under a person's clothing. TSA procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of items concealed under a person's clothing. While the detection requirements of AIT are classified, the procurement specifications require that any approved system be sensitive enough to detect smaller items. Prior to deployment, the machines are tested in the laboratory and in the field to certify that the detection standards are met. In addition, the DHS Transportation Security Laboratory (TSL) also tests the equipment to verify detection capability. After deployment, testing continues as TSA regularly conducts both overt and covert detection tests. In addition, AIT detection capability has been tested by DHS and the GAO.

The millimeter wave AIT equipment currently deployed at airports to screen passengers uses ATR software that enables the AIT automatically to identify irregularities on passengers using imaging analysis techniques based on contour, pattern, and shape. The AIT is designed to detect irregularities concealed under clothing; therefore, commenters are correct that it may detect items that do not pose a threat. Commenters also are correct that in order to determine whether AIT has alarmed on a threat item, a TSO will conduct further screening at the location where the AIT has indicated that there is an anomaly, thereby eliminating the need to pat-down the entire body. Generally, a passenger is only touched if an anomaly is indicated by AIT, and only the part of the body where the machine has indicated an anomaly is located is touched during the pat-down. At times, ETD or other forms of additional screening may be employed to resolve an alarm and to clear a passenger for entry into the sterile area after AIT screening. Passengers are advised to avoid wearing clothing with large metal embellishments and large metal jewelry and to remove all items in their pockets to reduce the possibility that the AIT will alarm on innocuous items.

TSA is aware of the audits conducted by the GAO on the effectiveness of screening measures. However, AIT was not in use at the checkpoint when the GAO tested security procedures described in the 2007 report cited by a commenter.[63] The 2010 report cited by a commenter did not contain any recommendations regarding the use of AIT, but did state that a cost/benefit analysis would be beneficial.[64] The RIA includes an extensive analysis of the costs of AIT and a qualitative discussion of its benefits. In addition, the RIA discusses the alternatives to AIT considered by TSA.

TSA disagrees with the comments alleging that because there is no direct evidence that AIT has prevented a terrorist attack on its own, the technology is not effective. As the Supreme Court pointed out in rejecting a similar argument in *Von Raab,* the validity of a screening program does not turn on ''whether significant numbers of putative air pirates are actually discovered by the searches conducted under the program.'' Given the government's interest ''in deterring highly hazardous conduct,'' the Supreme Court emphasized, ''a low incidence of such conduct, far from impugning the validity of the scheme . . . is more logically viewed as a hallmark of success.'' 489 U.S. at 675 n.3.[65] In *Corbett,* the Court of Appeals upheld the use of AIT and found that ''the scanners effectively reduce the risk of air terrorism . . . the Fourth Amendment does not require that a suspicionless search be fool-proof or yield exacting results.''[66]

Further, the fact that AIT, or any single security measure, may not be completely foolproof does not mean that it is ineffective and should not be used at all. A discussion of the alternatives to AIT considered by TSA is included in the RIA. TSA has always maintained that AIT is the best technology currently available to detect the threat of nonmetallic and other dangerous items and that a comprehensive security system is the best means to detect and deter terrorist attacks as no single layer by itself, including AIT, may be sufficient. Accordingly, TSA agrees with commenters that other security measures, including those mentioned in the comments such as canine, Federal Air Marshalls, and explosive detection systems, should also be deployed to increase the chance that a threat will be detected. TSA does in fact employ all of those measures. However, TSA does not

[63] U.S. Government Accountability Office, ''Aviation Security Vulnerabilities Exposed Through covert Testing of TSA's Passenger Screening Process,'' GAO–08–48T (Nov. 15, 2007).

[64] U.S. Government Accountability Office, ''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–10–484T (Mar. 17, 2010).

[65] *See also MacWade* v. *Kelly,* 460 F.3d 260, 274 (2d Cir. 2006) (holding that the deterrent effect of an anti-terrorism screening program in the New York subway system ''need not be reduced to a quotient'' to satisfy 4th Amendment balancing.'') and *Cassidy* v. *Chertoff,* 471 F.3d 67, 83 (2d Cir. 2006) (government is not required to ''adduce a specific threat'' to ferry system before engaging in suspicionless searches).

[66] *Corbett,* 767 F.3d at 1181.

agree that any of those measures should replace AIT because AIT provides stand-alone value as well.

In response to a comment regarding the redesign of the checkpoint to minimize embarrassment of passengers during the screening process, TSA points out that since May 2013, TSA has only deployed AIT with ATR software at the airport. ATR eliminates the individual image and produces a generic outline that is visible to the passenger and the TSO. In addition, TSA offers passengers who must undergo a pat-down the opportunity to have the pat-down conducted in a private screening location that is not visible to the traveling public.

Currently there are approximately 793AIT machines located at almost 157 airports nationwide. Given limited resources, TSA uses a risk-based approach to deploy AIT and continues to assess and test ''next generation'' AIT systems, which TSA anticipates will improve anomaly detection capability, decrease processing time, and better suit the physical constraints of airport checkpoints.

M. Screening Measures Used in Other Countries

Comments: Commenters discussed screening measures used in foreign countries. The majority of these comments recommended that TSA consider implementing a screening system similar to the one used by Israel. In addition to individual commenters, a privacy advocacy group stated that in 2011 the European Union (EU) issued a ruling banning the use of backscatter body scanners in all airports; that Italy discontinued its use of millimeter wave scanners because they were found to be slow and ineffective; and that Germany and Ireland discontinued use of AIT because of concerns regarding efficacy. A few individual commenters stated that the AIT scanners were removed from other countries because of health and safety concerns.

TSA Response: AIT is used in airports and mass transit systems in many countries, including in Canada, the Netherlands, Australia, Nigeria, and the United Kingdom.[67] TSA works directly with foreign governments and through the International Civil Aviation Organization (ICAO) to share information on AIT as well as other security measures.[68] TSA continues to believe that AIT provides the most effective technology currently available to detect metallic and nonmetallic threats. As was explained in the NPRM and discussed below, AIT has been tested for safety by both TSA and independent entities. The results confirm that AIT is safe for individuals being screened, equipment operators, and bystanders. *See* 78 FR 18294–18296.

TSA is aware that the European Commission adopted a legal framework on security scanners.[69] That framework states that the use of security scanners is optional, and that only security scanners which do not use ionizing radiation can be deployed and used for passenger screening. It also specifies that the scanners shall not store, retain, copy, print, or retrieve images. However, the Commission also found that ''[s]ecurity scanners are an effective method of screening passengers as they are capable of detecting both metallic and non-metallic items carried on a person. The scanner technology is developing rapidly and has the potential to significantly reduce the need for manual searches (''pat downs'') applied to passengers, crews and airport staff.'' [70]

N. Laboratory and Operational Testing of AIT Equipment

Comments: Some submissions discussed testing of AIT scanners for operational effectiveness. Several commenters stated that no testing has been conducted by independent parties, or they expressed concern that TSA did not publicly release the results of AIT equipment testing. A few individual commenters objected to having TSA test the scanners on the traveling public. An individual commenter suggested that validation tests should include evidence of attempts to defeat a screening technique and recommended that if the results indicate that AIT is less effective for screening than other devices, TSA should discontinue use of AIT in favor of technology that the results favor.

An individual commenter stated the need for long-term studies, including potential effects of the AIT equipment if it were to malfunction, become ''out of spec,'' or suffer from poor maintenance.

TSA Response: The FAA began testing AIT when it was responsible for passenger screening at airports prior to the creation of TSA. TSA continued laboratory testing of AIT as the threat from nonmetallic substances increased. To better assess the application of AIT to the airport environment, TSA conducted limited field trials of different types of AIT equipment at several airports. Throughout 2007 and 2008, AIT was piloted in the secondary position for these trials. In 2009, in response to the Christmas Day bomber, TSA began to evaluate using AIT in the primary screening position since there are no other currently deployed technologies in the primary screening position that can detect nonmetallic threats concealed under a passenger's clothing. When conducting tests both in the laboratory and in the field, TSA evaluated the equipment for safety, detection capability, operational efficiency, and passenger impact. Because of the successful results observed during testing and the need to address the threat from nonmetallic explosives concealed under clothing, TSA decided to procure AIT units for use in the primary position at airport checkpoints.

All of the AIT units are regularly inspected by the manufacturer to ensure that they operate effectively and meet TSA specifications. In addition, the units are tested each day prior to use at the checkpoint. If the equipment does not meet operational specifications, it cannot be used.

The GAO released a report, ''Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems,'' in March 2014 describing the types of tests TSA conducts on AIT.[71] As explained in the report, TSA conducts the following five tests to evaluate the performance of AIT equipment: (1) Qualification testing in a laboratory setting at the TSA Systems Integration Facility to evaluate the technology's capabilities against TSA's procurement specification and detection standard to include testing of false alarm rates; (2) Operational testing at airports to evaluate system effectiveness and suitability for the airport environment; (3) Covert testing to identify vulnerabilities in the technology, operator use, and TSO compliance with procedures; (4) Performance Assessments to test TSO compliance with Standard Operating Procedures (SOPs); and (5) Checkpoint drills to assess TSO compliance with SOPs and ability to resolve anomalies

[67] *http://science.howstuffworks.com/millimeter-wave-scanner4.htm*; *http://cnsnews.com/news/article/us-paid-full-body-scanners-nigeria-s-four-international-airports-2007.*

[68] ICAO recognizes that AIT may be used as a primary screening measure for passengers. ICAO ''Aviation Security Manual,'' Doc 8973/8 Restricted (2011).

[69] European Commission, Press Release, ''Aviation Security: Commission Adopts New Rules on the Use of Security Scanners at European Airports,'' Brussels, Belgium (Nov. 14, 2011). The countries referenced by several commenters (Germany, Ireland, and Italy) are members of the European Union.

[70] *Id.*

[71] U.S. Government Accountability Office Report to Congressional Requesters, ''Advanced Imaging Technology: TSA Needs Additional Information before Procuring Next-Generation Systems,'' GAO–14–357, March 2014.

identified by AIT.[72] Qualification testing is conducted when a technology is first considered for deployment and for subsequent upgrades to the technology. The TSL also conducts certification testing on detection capability. In addition to these tests, the actual units are subjected to a factory acceptance test at the manufacturer's facility and a site acceptance test at the airport. TSA also tests the units for radiation exposure as described in the NPRM and in response to additional comments described below. Covert testing is also conducted by the Inspector General of DHS and GAO.[73] TSA studies the results of laboratory and covert tests closely, and modifies procedures as appropriate. TSA believes that the testing described above adequately supports the use of AIT as a primary screening mechanism.

O. Radiation Exposure

Comments: The effects of radiation associated with AIT use was also addressed by commenters. A professional association stated its belief that AIT emissions present a negligible health risk to passengers, airline crewmembers, airport employees, and TSA staff. Numerous commenters, however, expressed concern regarding exposure to radiation. Some of these commenters suggested that no dose of radiation is safe. Many individual commenters and an advocacy group expressed concern about the radiation from backscatter scanners, which they stated could lead to the development of cancer. Many individuals also warned that exposure to millimeter wave radiation could hold the potential for long-term health effects and that additional studies are needed. Some commenters concluded that, even if the current x-ray scanners were removed, the proposed rule would not prevent their reintroduction should software become available to address privacy issues.

Several commenters, including a privacy advocacy organization, a non-profit organization, and individual commenters, cautioned that TSA screeners could be at risk and should be provided with dosimeters to ensure that their exposure is within acceptable limits. An individual commenter stated that, although TSA claimed that the radiation scan only affects the surface of the skin, skin cancer is the largest incidence of cancer in the world, and it is caused by radiation exposure on the skin. Another commenter stated that eyes are particularly susceptible to radiation. A few individuals suggested that imaging technology using radiation should not be used at all since alternatives exist. Other commenters stated that the question that needs to be asked with respect to the safety of AIT scanning is not whether the increase in deaths is below some arbitrary value, but whether the lives saved through avoiding a terrorist attack are greater than the lives lost through an increased incidence of cancer or other diseases arising from the use of AIT scanners. Lastly, a few individuals mentioned that because of their exposure to radiation for medical treatment, they are not comfortable getting further, unnecessary exposure from AIT scanners.

TSA Response: In compliance with the statutory requirement that all AIT machines used for screening be equipped with and employ ATR software, TSA removed the general-use backscatter AIT units from the checkpoint.[74] TSA notes that it is adopting the statutory requirement mandating the use of ATR software on AIT used to conduct screening in the regulatory text.

Contrary to assertions by some commenters and as discussed in the NPRM, general-use backscatter units were independently evaluated and found to be within national standards for acceptable radiation exposure by the Food and Drug Administration (FDA)'s Center for Devices and Radiological Health (CDRH), the National Institute of Standards and Technology, the Johns Hopkins University Applied Physics Laboratory and the U.S. Army Public Health Command.[75] A report issued by the DHS Office of Inspector General in 2012 confirms that prior to the deployment of general-use backscatter units, TSA conducted four radiation safety assessments and the results of each study concluded that the level of radiation emitted was below ANSI's acceptable limits.[76]

In addition, in June 2013, the American Association of Physicists in Medicine released the results of an independent study of the general-use backscatter units previously used by TSA for screening passengers.[77] The study measured exposures across multiple scanners in both the factory and in real-time use at airports, including organ doses. This study also found that radiation doses were below the ionizing radiation limits set by the American National Standards Institute and Health Physics Society (ANSI/HPS) and were safe for employees and passengers, including children, pregnant women, frequent flyers and individuals with medical implants.

In the NPRM, TSA noted that DHS had requested the National Academies of Sciences, Engineering, and Medicine to review previous studies as well as current processes to estimate radiation exposure resulting from the general-use backscatter equipment. That study was released in October 2015 and confirms that radiation doses did not exceed the ANSI/HPS standard.[78]

As explained in the NPRM, the ANSI/HPS standard takes into consideration individuals who may be more susceptible to radiation health effects, such as pregnant women, children, and persons who receive radiation treatments, as well as the general exposure to ionizing radiation present in the environment. 78 FR 18295. In fact, the radiation emissions from the general-use backscatter equipment were so low that they were below the environmental radiation emissions that individuals are exposed to every day, and individuals would have to be screened more than 200 times a year to exceed the negligible individual dose, which is still below the ANSI/HPS standard.[79] 78 FR 18296.

[72] The report also contained recommendations to improve TSO performance on AIT and resource effectiveness, and to ensure that next generation AIT units meet mission needs. TSA generally concurred in the recommendations and noted that it will review its screening assessment programs, monitor, update and report efforts to capture operational data on screening, improve its assessment of overall effectiveness of next-generation AIT and complete a more comprehensive technology roadmap.

[73] The Inspector General of DHS recently conducted covert testing of TSA aviation security screening and the Secretary has directed TSA to undertake a number of steps to enhance security capabilities and techniques. *See, e.g.,* Statement by Secretary Jeh C. Johnson On Inspector General Findings on TSA Security Screening, Press Release, Jun. 1, 2015. TSA's response to the Inspector General's findings and the changes TSA has implemented to address those findings were discussed in the testimony of TSA Administrator, Peter V. Neffenger, before the Senate Committee on Appropriations, Subcommittee on Homeland Security on Sep. 29, 2015. *See https://www.tsa.gov/news/testimony/2015/09/29/testimony-tsa-efforts-address-oig-findings.*

[74] 49 U.S.C. 44901(l).

[75] 78 FR 18295. *See also https://www.tsa.gov/FOIA.*

[76] Department of Homeland Security, Office of Inspector General, ''Transportation Security Administration's Use of Backscatter Units,'' OIG–12–38, Feb. 2012 at p. 5.

[77] ''Radiation Dose from Airport Scanners,'' American Association of Physicists in Medicine, AAPM Report No. 217 (2013). Available at *http://www.aapm.org/pubs/reports.*

[78] National Academies of Sciences, Engineering, and Medicine. Airport Passenger Screening Using Backscatter X-Ray Machines: Compliance with Standards (2015), available at *http://www.nap.edu/21710.*

[79] TSA disagrees with the comments that attempted to link AIT to skin cancer, for the reasons explained in this preamble. TSA notes that according to the Stanford Medicine Cancer Institute, ultraviolet radiation from the sun is the

Continued

As explained in the NPRM, the millimeter wave equipment uses non-ionizing radio frequency energy. 78 FR 18294–18295. The millimeter wave equipment used by TSA must comply with the 2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™—2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494–522, published April 1998. The equipment also is consistent with Federal Communications Commission and Health Canada Safety Code regulations. 78 FR 18295. The FDA confirmed that millimeter wave security systems that comply with the IEEE Std.C95.1™—2005 cause no known health effects.[80] TSA has posted a compilation of emission safety reports of the millimeter wave technology system.[81]

TSA implemented safety protocols to ensure that AIT is safe for passengers and the TSA workforce. When backscatter machines were still in use, each individual AIT machine was tested once a year to verify that radiation emitted fell within the national safety standards. Regular testing is also conducted on checkpoint machines that use x-ray technology, such as baggage scanners. This testing is performed by the manufacturers or maintenance providers in accordance with their TSA contracts. Because of the regular testing of TSA equipment, there is no need for operators to wear dosimeters to measure radiation emissions. In the event that a radiation test was to reveal that the emission was above the standard, the machine would be immediately taken out of service and TSA would conduct a system-wide review.

P. Other Health and Safety Issues

Comments: Commenters also mentioned other safety and health concerns related to AIT. Numerous individual commenters generally stated that they consider the safety of the AIT scanners to be uncertain and that they are concerned that AIT is harmful to their health. Some individuals suggested that the machines amount to a medical examination performed by someone who is not a trained medical professional. A few individual commenters expressed concern about the maintenance and calibration of the scanners. According to another individual commenter, the AIT scanners and pat-downs are a physical and psychological attack on an individual, and the passenger must restrain himself or herself from natural instincts to move away from harmful physical contact to ensure their privacy and to avoid health risks.

TSA Response: All AIT units are tested for safety, detection capability, operational efficiency, and impact on passengers prior to deployment. The millimeter wave units currently in use at the airports do not use ionizing radiation. Federal law requires that all AIT units be equipped with ATR software, which does not produce an individual image, only a generic outline that is visible on the machine. TSA permits passengers generally to opt out of AIT screening and receive a thorough pat-down instead. TSA has also instituted the TSA Pre✓™ program, which allows known and trusted travelers an opportunity to undergo expedited screening, which sometimes includes screening by WTMD. This program increases throughput (among other changes) and improves the screening experience of frequent, trusted travelers. Of course, in order to maintain comparable security, no passenger is guaranteed expedited screening, and program participants may be required to undergo regular screening on a random basis.

Q. Backscatter Technology

Comments: Some submissions specifically addressed backscatter technology. Many individual commenters opposed the use of backscatter technology because of the alleged health impact. According to several commenters, x-ray radiation is cumulative, and the effects over a lifetime are not well known. A few individual commenters added that the people who may be most at risk are TSA personnel working near the scanners and frequent flyers, who are already exposed to radiation from high altitude flying. In addition, another individual commenter suggested that, even if the risk to one individual is small, when the machines are used on hundreds of millions of people, the probability that some set of individuals acquire cancer is significant.

One commenter warned that ionizing radiation might cause deoxyribonucleic acid (DNA) damage that leads to carcinogenesis and that a model used by the health physics community would predict the probability of a fatal cancer about the same as the probability of being killed by a terrorist in an airplane. However, the commenter expressed the belief that the real danger is very high local radiation exposures if the mechanical scanning mechanism and associated systems for shutting off the x-ray beam fail. Another individual disputed TSA's statement that independent tests had been conducted on backscatter technology, and the commenter stated that subsequent information showed that the tests were flawed, their results were misused, or they were not conducted by truly independent entities.

A few commenters, including an individual commenter and a privacy advocacy group, remarked on the ineffectiveness of backscatter machines. One of them suggested that the x-ray beam might not be able to distinguish between explosives and tissue when an explosive package is shaped to fit in with natural body contours. An individual commenter stated that even though TSA is removing backscatter scanners from airports, until the process is complete, they would continue to be used at some airports. Another individual recommended that TSA investigate the bad management decision that led to a waste of tax dollars on what the commenter described as an obviously unacceptable technology. Another commenter suggested that backscatter technology was adopted because of lobbying by politically connected individuals with a financial interest in the machines. A few commenters discussed TSA's selection to use Rapiscan as the vendor for AIT scanners. According to some individual commenters, the choice of using Rapiscan as the vendor is inappropriate because a former DHS Secretary was reported to have lobbied for Rapiscan and AIT prior to his departure from the agency.

TSA Response: As discussed above, the general-use backscatter AIT equipment deployed by TSA was tested for safety, detection capability, operational efficiency, and passenger impact before deployment.[82] Independent testing confirmed that the x-ray emissions from the general-use backscatter units were so low as to

main cause of skin cancer. *http://stanfordhealthcare.org/medical-conditions/cancer/skin-cancer/causes-skin-cancer/ultraviolet-radiation.html.* There is no evidence that AIT is related to the incidence of skin cancer.

[80] FDA, ''Products for Security Screening of People,'' available at *http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm.*

[81] *https://www.tsa.gov/FOIA.*

[82] All general-use backscatter AIT units were removed from screening checkpoints as of May 16, 2013, to comply with the statutory requirement that any AIT used to screen passengers be equipped with and employ ATR software. 49 U.S.C. 44901(l). The backscatter AIT units in use at the time were unable to employ ATR software.

present a negligible risk to passengers, airline crew, airport employees, and TSA employees. 78 FR 18294–18296. Any future backscatter AIT units would also be tested to ensure compliance with applicable safety standards.

Regarding the marginal effects of x-ray radiation, as TSA noted in the NPRM, 78 FR 18295–18296, the ANSI/HPS standard reflects the standard for a negligible individual dose of radiation established by the National Council on Radiation Protection and Measurements at 10 microsieverts per year. Efforts to reduce radiation exposure below the negligible individual dose are not warranted because the risks associated with that level of exposure are so small as to be indistinguishable from the risks attendant to environmental radiation that individuals are exposed to every day. The level of radiation emitted by the Rapiscan Secure 1000 is so low that most passengers would not have exceeded even the negligible individual dose. The European Commission released a report conducted by the Scientific Committee on Emerging and Newly Identified Health Risks on the risks related to the use of security scanners for passenger screening that use ionizing radiation such as the general-use backscatter AIT machines.[83] The health effects of ionizing radiation include short-term effects occurring as tissue damage. Such deterministic effects cannot result from the doses delivered by security scanners. In the long term, it found that the potential cancer risk cannot be estimated, but is likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources, and background risk due to other factors.

Regarding commenters' concerns that ionizing radiation might cause deoxyribonucleic acid (DNA) damage, as TSA noted in the NPRM, the annual dose limits in ANSI/HPS N43.17 are based on dose limit recommendations for the general public published by the National Council on Radiation Protection and Measurements in Report 116, ''Limitations of Exposure to Ionizing Radiation.'' The dose limits were set with consideration given to individuals, such as pregnant women, children, and persons who receive radiation treatments, who may be more susceptible to radiation health effects. Further, the standard also takes into consideration the fact that individuals are continuously exposed to ionizing radiation from the environment. ANSI/HPS N43.17 sets the maximum permissible dose of ionizing radiation from a general-use system per security screening at 0.25 microsieverts. The standard also requires that individuals should not receive 250 microsieverts or more from a general-use x-ray security screening system in a year.

Regarding comments about whether AIT can distinguish between explosives and tissue when an explosive package is shaped to fit in with natural body contours, the AIT equipment is designed and tested to find such items.

Regarding comments about the procurement of backscatter technology and Rapiscan, all TSA acquisitions were in compliance with Federal procurement standards. TSA issued a competitive solicitation for companies to submit AIT machines for qualification testing, and while competitive pricing was submitted by two vendors, only Rapiscan was qualified and placed on the Qualified Product List before the planned award date of September 2009. The award was then made to Rapiscan for the initial order.

R. Millimeter Wave Technology

Comments: Some submissions specifically addressed millimeter technology. Many commenters, including individual commenters and non-profit organizations, stated that although TSA claims that millimeter wave scanners are safe, they were unconvinced. Several of these commenters stated TSA had not conducted long-term, independent testing of millimeter wave equipment. Others noted that the scanners still emit a form of radiation and may be harmful. A non-profit organization added that babies, small children, pregnant women, the elderly, and people with impaired immunity would be at a higher risk from non-ionizing radiation than others would. An individual commenter remarked that studies have shown a trend toward higher rates of brain and other tumors in those who use cell phones, which produce a similar form of non-ionizing radiation. Two other individuals suggested that millimeter wave exposure could be harmful to human DNA because of resonance effects.

Although some commenters supported the use of millimeter wave technology over backscatter technology, an individual and an advocacy organization stated they were disinclined to take the government at its word with regard to health assurances because the government has been wrong before, including TSA assurances about Rapiscan machines. An individual commenter stated that millimeter wave machines are no more acceptable than other scanners, but those who must fly will choose them to avoid a pat-down.

One individual commenter recommended another technology for detecting explosives—passive Terahertz (THz) imaging. According to the commenter, there would be no probing radiation, but the warm body emits sufficient THz radiation to form an image, with high explosives standing out in the image as a dark patch.

TSA Response: As discussed in the NPRM, millimeter wave imaging technology used by TSA to screen passengers meets all known national and international health and safety standards. 78 FR 18295. Millimeter wave units are tested for electromagnetic emissions prior to acceptance. The FDA examined the exposure to non-ionizing electromagnetic energy and found that the short duration of screening, approximately 1.5 seconds, and the very low levels of emissions showed that the energy emitted by millimeter wave technology systems is approximately a thousand times less than the limit set by the Institute of Electrical and Electronics Engineers (IEEE). FDA evaluated the Millimeter Wave AIT to determine if the RF emissions met the safety levels established for the general public in C95.1–2005. The exposure a person receives during one scan at a worst-case distance of 10 cm from the inner wall of the unit is on the order of 1000 times less than the IEEE standard's limit for the public exposure. IEEE Std 95.1 defines general public as ''individuals of all ages and varying health status . . . Generally, unless specifically provided for as part of an RF safety program, the general public includes, but is not limited to, children, pregnant women, individuals with impaired thermoregulatory systems, individuals equipped with electronic medical devices, and persons using medications that may result in poor thermoregulatory system performance.'' [IEEE Std 95.1–2005, page 7, 3.1.26]. TSA has posted a report on its Web site that includes the evaluation performed by the FDA.[84]

[83] The SCENIHR is an independent committee that provides the European Commission with the scientific advice it needs when preparing policy and proposals relating to consumer safety, public health, and the environment. The committee is made up of external experts. *See* SCENIHR (Scientific Committee on Emerging and Newly Identified Health Risks), Health effects of security scanners for passenger screening (based on X-ray technology), 26 April 2012.

[84] ''Compilation of Emission Safety Reports on the L3 Communications, Inc. ProVision 1000 Active Millimeter Wave Advanced Imaging Technology (AIT) System,'' Sept. 2012. *See, www.dhs.gov/advanced-imaging-technology-documents.*

TSA is aware of the paper cited by commenters that reportedly found that THz radiation could affect biological function, but only under specific conditions and extended exposure. The paper, ''DNA Breathing Dynamics in the Presence of a Terahertz Field,'' was published by scientists from the Theoretical Division and Center for Nonlinear Studies at Los Alamos National Laboratory in 2010. The millimeter wave machines deployed by TSA do not operate in the THz range, or at the power level referenced in the paper, and the exposure time for passengers screened by AIT is approximately 1,000 times less than the exposure time referenced in the paper.

TSA has evaluated other technologies to assess whether they are safe, meet all applicable government and industry standards, are effective against known and anticipated threats, and require the least disruption and intrusion on passenger privacy possible. For example, TSA has tested passive THz systems in the past and found that they were not effective in detecting explosive threats in an airport environment. Likewise, TSA considered Infrared technology but found that detection capability and operational effectiveness were limited. However, TSA continues to research and assess engineering developments and new technologies for use in the airport.

S. Concerns Regarding Privacy

Comments: Many submissions addressed concerns related to privacy. Many individual commenters, a non-profit organization, and advocacy groups expressed the opinion that the devices should be called ''Nude Body Scanners'' or ''Naked Body Scanners'' to indicate specifically how TSA uses them, and other commenters preferred ''Electronic Strip Searches'' or ''virtual strip searches'' or ''nude-o-scopes.'' Numerous individuals insisted that AIT scanners violate an individual's right to privacy, that TSA's privacy safeguards are inadequate, and that the scanners should not be used on children. Some commenters stated that if scanners are viewing anything under a person's clothing, then that person's privacy is not being protected, because anything under the clothing is intentionally hidden and not meant to be viewed by man or machine. An advocacy group agreed that AIT defeats the privacy-protecting function of clothing and allows an image of the unclothed person to be created. An individual commenter remarked that the problem with TSA's use of AIT for primary screening is it teaches people it is normal and acceptable for the government to use technology to look under their clothing. The commenter added that the body beneath one's clothing and the contents of one's pockets traditionally have been understood as among the most important and intimate zones of privacy.

One commenter noted that passengers must reveal private medical conditions to TSA officers who are not trained in medicine, and others stated that investigating private details of passengers' bodies is deeply offensive and has no security value. A community organization agreed that privacy is invaded when a passenger is forced to share personal secrets that are not otherwise observable in public—especially sensitive medical and gender identity issues. One commenter, however, expressed the opinion that over the years, TSA staff has become more respectful of individual passenger privacy.

A privacy advocacy group pointed out that since January 2008, TSA has published four Privacy Impact Assessments (PIAs) regarding the agency's deployment of body scanners at U.S. airports. The commenter opined that all of these have failed to identify the numerous privacy risks to air travelers. An individual commenter suggested that TSA should be required to regularly report to Congress about its efforts to discover weaknesses in its mechanisms to protect the privacy of individuals scanned by its systems.

Some submissions suggested other technologies and procedures for safeguarding privacy. Among the procedures recommended by one individual were: (1) Providing a generic image of all scanned passengers and (2) allowing a person to leave if selected for a manual search, provided the person exhibits no other suspicious behavior. One commenter suggested that if the AIT screening procedures detect potentially dangerous objects hidden in passengers' private areas, the passengers should be allowed to remove the suspicious objects, show them to TSA officers, and be rescreened using AIT. Another individual suggested developing technology to combat scanner fatigue, providing oversight in screening rooms, and addressing the threat of privacy or security breaches when the status of a passenger is relayed by two-way radio.

TSA Response: As stated previously, Federal law requires that all AIT equipment used to screen passengers must be equipped with and employ the use of ATR. The ATR software produces a generic outline that is publicly displayed on the equipment. The use of ATR mitigates privacy concerns because there is no individual image of a passenger's body, only a generic outline that is the same for passengers based on gender. The AIT equipment used by TSA is not able to store, transmit, or print any images. After each passenger is screened using the AIT, the TSO clears the generic outline of any alarms so that the next passenger may be screened. Signs are posted at the checkpoint and information is available on TSA's Web site showing a sample of the ATR generic outline and advising passengers that they may decline AIT and receive a thorough pat-down. The court in *Corbett* found that the ''scanners pose only a slight intrusion on an individual's privacy, especially in the light of the automated target recognition software installed in every scanner. The scanners now create only a generic outline of an individual, which greatly diminishes any invasion of privacy.'' [85]

TSA has posted information on AIT technologies and ATR on its Web site, and published a PIA in January 2008 with subsequent updates. TSA also conducted outreach with national press and privacy advocacy groups to discuss AIT. While most PIAs are required on information systems that collect information in identifiable form, which AIT does not, DHS nevertheless conducted PIAs on TSA's use of AIT. As explained in the PIA, ''the operating protocols of remote viewing for AIT machines that were not equipped with ATR software, coupled with no image retention, are strong privacy protections . . . ATR software provides even greater privacy protections by eliminating the human image . . . .'' [86]

TSA disagrees with the alternate procedures suggested by some of the commenters. Federal courts have upheld TSA's procedure to require passengers to complete the screening process once it has been initiated by the passenger. As the U.S. Court of Appeals for the Ninth Circuit explained in *Aukai*,

> The constitutionality of an airport search, however, does not depend on consent . . . and requiring that a potential passenger be allowed to revoke consent to an ongoing airport security search makes little sense in a post-9/11 world. Such a rule would afford terrorists multiple opportunities to attempt to penetrate airport security by 'electing not to fly' on the cusp of detection until a vulnerable portal is found. This rule would also allow terrorists a low-cost method of detecting systematic vulnerabilities in airport

[85] *Corbett*, 767 F.3d at 1181.

[86] Privacy Impact Assessment Update for TSA Advanced Imaging Technology, Jan. 25, 2011, *www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf.*

security, knowledge that could be extremely valuable in planning future attacks.

U.S. v. *Aukai*, 497 F.3d 955, 960–61 (9th Cir. 2007) (en banc) (internal citations omitted). Finally, TSA's procedures permit passengers generally to opt out of AIT screening and receive a thorough pat-down instead, which may be conducted in private and in the presence of a companion of the passenger's choosing.

T. Use of ATR Software

Comments: Some submissions discussed TSA's use of ATR software. Numerous submissions from individual commenters remarked that even though ATR software displays a generic outline on the screen at the checkpoint, ATR does not eliminate air travelers' privacy concerns. Many of these commenters, including individuals and advocacy groups, expressed opposition to the use of ATR because, according to the commenters, ATR can be disabled and the scanners are capable of producing explicit, nude pictures that may be viewed by TSA staff. Individual commenters and an advocacy group stated that ATR does not alleviate concerns about the intrusiveness of scanning, its ineffectiveness, the violation of privacy, and possible health effects. A few individuals and a professional association, however, expressed support for the use of ATR because the technology helps mitigate passengers' privacy concerns. An individual commenter stated that TSA took a year longer than legally allowed to cease use of AIT scanners without ATR software.

TSA Response: TSA's deployment of ATR software was completed in accordance with Federal law and before the established deadline. TSA agrees with commenters that the use of ATR software addresses privacy concerns since there is no individual image, and there is no need for a TSO to view an individual image. In addition, TSA believes that the ATR detection capability is commensurate to that of a TSO review and is likely faster, thereby decreasing the amount of time passengers must spend at the checkpoint. TSOs are not able to disable the software, and each AIT unit is delivered to the airport with software that precludes placing the unit into a mode that would allow TSOs to obtain unfiltered, passenger-specific images. Further, the equipment cannot store, transmit, or print individual images, and TSOs are not able to install or activate any such capability on the equipment.

U. Protection of Images

Comments: Commenters also addressed the issue of image protection controls. Numerous individual commenters suggested that they were not convinced by TSA's assertions regarding image protection. Several individual commenters mentioned reports of incidents involving recorded and leaked images from scanners, such as the reported release of 35,000 images created by a Rapiscan machine at a courthouse in Florida. Other individuals and advocacy groups warned that because the scanners have the capability to store and transmit images, at least some storage of images by TSA and viewing by others is likely. Some of these commenters alleged that TSA had falsely stated that previous imaging machines could not store, transmit, or print images.

A privacy advocacy group pointed out that the scanners were designed to include Ethernet connectivity, Universal Serial Bus access, and hard disk storage, but the proposed rule does not include safeguards against storing, copying, or otherwise circulating images. An advocacy group added that the scanners are worse than a physical strip-search because they produce an image that can be stored indefinitely, transferred around the globe in seconds, and copied an infinite number of times without the copies degrading. According to an individual commenter, law enforcement officers can record images without the passenger's knowledge. Some commenters, including individuals and a privacy advocacy association, recommended that TSA clarify what happens to the images captured, who gets to see them, and whether the practice of deleting the image after each screening is absolute. A couple of individual commenters also suggested that TSA should show the public exactly how detailed the image seen in the screening room is, or allow passengers being scanned to observe the personnel monitoring the images. A few individuals, however, expressed support for TSA's efforts to protect passenger privacy by ensuring that the images are anonymous and are automatically deleted from the system after the remotely located security officer clears them.

TSA Response: Federal law requires that all AIT equipment used to screen passengers be equipped with and employ ATR. TSA removed all AIT equipment that could not use ATR software by May 16, 2013, in advance of the statutory deadline. The ATR software does not produce an individual image but instead produces a generic outline that is publicly displayed on the equipment. A picture of the generic outline is posted at the checkpoint and on TSA's public Web site.[87] Consequently, the individual image has been eliminated and there is no longer any need for a TSO in a remote location to view the image.

Initial versions of AIT were manufactured with storage and transmittal functions that TSA required manufacturers to disable prior to installation at airports. TSA confirmed that these functions were disabled during factory acceptance testing and site acceptance testing. The TSOs were not able to activate the functions. As explained in the NPRM, images were transmitted securely between the unit and the viewing room so they could not be lost, modified, or disclosed.[88] The images produced were encrypted during this transmission and were completely deleted in the viewing room once the individual was cleared. The TSO in the viewing room was prohibited from bringing electronic devices such as cameras, cell phones or other recording devices into the viewing room. Violations of these procedures would subject the TSO to disciplinary action, up to and including termination. Note that the current versions of AIT do not have the capability to create an image; rather, they create internal code of the passenger using proprietary software that it analyzes and uses to show an alarm box on the generic outline, if appropriate.

The AIT devices at airports do not have the ability to transmit, store, or print images. While use of AIT in other locations, such as courthouses, was discussed in the comments, TSA does not operate AIT in those locations. AIT that is equipped with ATR software does not produce an individual image; even prior to the use of ATR, TSA's privacy safeguards, detailed in the NPRM, would have prevented the production, let alone release, of images described in the comments.[89]

V. Conducting a Pat-Down as the Alternative to AIT

Comments: Comments also addressed the use of the pat-down as the alternative to AIT. Many individual commenters and an advocacy group stressed the importance of having TSA retain the option to undergo a pat-down instead of AIT; although some pointed out that many passengers select the pat-down over AIT only because they consider it the lesser of two evils. Many

[87] *https://www.tsa.gov/travel/travel-tips.*

[88] 78 FR 18294.

[89] 78 FR 18294.

individual commenters expressed a strong preference for the pat-down; many also stated that they always request a pat-down in lieu of AIT screening. Some individual commenters, however, expressed strong opposition and criticism of current pat-down procedures. Some individual commenters expressed their preference to receive a pat-down, but stated that they feel ''punished'' by TSA staff when requesting the alternative screening measure. Several commenters opined that TSA screeners deliberately make the opt-out unpleasant so that passengers will use the AIT scanners.

Submissions included remarks about the adequacy of information and signs at screening checkpoints about the AIT screening process. For example, multiple commenters stated that TSA currently lists the scanner as optional, in small print on an 11 x 14 inch poster at a crowded checkpoint. Commenters suggested there is a lack of adequate signage informing passengers of the right to opt-out of AIT. One of these individual commenters suggested that, in order to allow passengers adequate time to read about their right to opt-out of AIT, these signs should be posted throughout the security waiting area instead of in the area where passengers are being called forward for screening. A commenter stated that different airports want people to indicate that they are opting out at different times, but passengers have no way of knowing when to opt out. An advocacy group stated that notification of the opt-out option is not large enough and is placed in an area where passengers will not see the notice. A non-profit organization stated that passengers continue to report that signs are not available, even though TSA stated in the NPRM that detailed explanation of AIT procedures is available on its Web site, and signs are posted at checkpoints.

Other individuals and a privacy advocacy group emphasized that the pat-down is not a reasonable alternative. Many individual commenters remarked that when they choose to opt-out of AIT, they are treated with suspicion, public ridicule, hostility, and retaliation (*e.g.*, long and intentional delays) by the screener, and often are unable to monitor their belongings. Other individuals and advocacy groups objected to the manner in which some TSA staff conduct pat-downs, stating they are more invasive and intrusive than necessary to detect weapons or explosives.

Numerous commenters, including a community organization, a non-profit organization, and individual commenters, characterized the pat-down as groping or sexual assault that involves touching or rubbing of the breasts and genitals of passengers. The pat-downs were referred to as rough, painful, invasive, offensive, intrusive, humiliating, demeaning, and degrading. Some commenters provided anecdotal accounts related to their experiences being screened by TSA. The majority of these comments referred to personal accounts of pat-downs, including statements that the pat-downs were abusive and extended wait times. Other individual commenters stated that because of their negative pat-down experiences, they have cancelled air travel plans. A number of individual commenters stated that in their experience, TSA employees generally treat passengers in a courteous and professional manner.

Commenters also expressed concerns regarding profiling. A few individual commenters, for example, stated that TSA staff intentionally chose young, female travelers for pat-downs at a higher rate than other travelers. Other commenters suggested that TSA staff discriminate against children and elderly women. It was the concern of an individual commenter that an enhanced pat-down of a child can be detrimental to the child's understanding of the appropriateness of an adult touching them. Furthermore, the individual commenter remarked that the separation of the child from their parent for screening results in distress for both the parent and child. Several individuals, a non-profit organization, and an advocacy group expressed concern for children that must undergo touching during pat-downs. Many individuals and an advocacy group also mentioned psychological trauma caused by pat-downs, particularly for rape survivors and victims of sexual abuse. A few individual commenters noted that pat-downs impose unnecessary risks, given that most TSA screeners do not change their gloves often enough to prevent the spread of disease.

TSA Response: TSA allows individuals generally to opt out of AIT screening and undergo a thorough pat-down instead. TSA has no requirement as to when a passenger should indicate that he or she does not wish to undergo AIT screening. Generally, passengers should make their request for a pat-down when they are directed to the AIT and prior to entering the AIT machine. Such requests can also be made earlier in the screening process. While AIT has been used to conduct primary passenger screening since 2009 and millions of passengers are aware of and have been screened by AIT, TSA posts signs to inform passengers that they may opt-out of AIT screening. TSA places these signs in the checkpoint prior to the AIT machine. Generally, the signs are 11 x 14 inches to avoid impeding the flow of passengers, because the signs are located in an area where passengers walk to enter the AIT unit. However, TSA permits signs that are 22 x 28 inches. TSA appreciates the commenters' input on the placement and font size associated with the signs, and may in the future revise signage practices to make this information even more prominent to passengers.

While commenters wrote that the thoroughness of the pat-down is inappropriate, it would not make sense to allow passengers to opt out of AIT unless the alternative has similar ability to detect both metallic and non-metallic threat items. The pat-downs are tailored to address the known threat posed by concealed metallic or non-metallic explosives or other weapons, including those concealed on culturally sensitive areas of the body in order to evade detection. The court in the *Corbett* decision upheld the constitutionality of the pat-down. ''The pat-downs also promote the governmental interest in airport security because security officers physically touch most areas of passengers' bodies . . . . Undeniably, a full-body pat-down intrudes on privacy, but the security threat outweighs that invasion of privacy.'' [90] The court noted that TSA's procedures when conducting a pat-down reduce the invasion of privacy.[91]

The pat-down procedures are described on TSA's Web site.[92] A pat-down is performed if a passenger cannot undergo WTMD or opts out of AIT screening. A pat-down is also performed to resolve alarms or anomalies. A less invasive pat-down may be performed on a random basis. TSA advises individuals entering the checkpoint to divest all items on their person and in their pockets to reduce the likelihood that an alarm will occur. A pat-down is conducted by a TSO of the same gender as the passenger. A passenger may request that the pat-down be performed in private. During a private screening, another TSA employee will always be present and a companion of his or her choosing may accompany the passenger. In addition, the passenger is permitted to bring his carry-on baggage to the location where the pat-down will take place, including any private screening area. A passenger may ask for a chair if he or she needs to sit down. Ordinarily

[90] *Corbett*, 767 F. 3d at 1182.

[91] *Id.*

[92] *https://www.tsa.gov/travel/frequently-asked-questions.*

a passenger will not be asked to remove or lift any article of clothing to reveal a sensitive body area. TSA has modified its pat-down procedures for children age 12 and under and adults age 75 and over to be less invasive and to reduce the likelihood that a pat-down is performed.[93] Further, TSA will not separate parents from their children during the screening process. Passengers may request that TSOs change their gloves before performing a pat-down. Since a pat-down is conducted to determine whether prohibited items are concealed under clothing, sufficient pressure must be applied in order to ensure detection. TSOs are trained to inquire whether a passenger has an injury or tender area prior to initiating the pat-down so that such areas are treated accordingly.

TSOs are trained to be courteous and respectful to all passengers and to provide assistance to facilitate the screening process. TSA will make every effort to be respectful of passengers' concerns, including those who have particular sensitivities to physical touching and to accommodate a person's needs. TSOs may not deliberately delay or modify a pat-down in order to convince passengers to choose AIT screening; such activity may subject a TSO to discipline, up to and including termination.

As explained on TSA's Web site, TSA has established a national hotline for passengers with disabilities, medical conditions, or other circumstances to assist passengers to prepare for the screening process prior to flying.[94] TSA recommends that passengers call the toll-free TSA Cares hotline, at 1–855–787–2227, 72 hours in advance of their flight for information about what to expect during screening.

Passengers who believe they have experienced unprofessional conduct at a security checkpoint may request to speak to a supervisor at the checkpoint or write to the TSA Contact Center at *TSA-ContactCenter@dhs.gov.* Passengers who believe they have been subject to discriminatory treatment at the checkpoint may file a complaint with TSA's Office of Civil Rights and Liberties, Ombudsman and Traveler Engagement at *TSA–CRL@tsa.dhs.gov*, or submit an online complaint at *https://www.tsa.gov/contact-center/form/complaints.*[95] Finally, travelers may also file discrimination complaints with DHS CRCL via CRCL's Web site at *http://www.dhs.gov/complaints.*

W. AIT Screening Procedures at the Checkpoint

Comments: Many submissions discussed AIT screening procedures at security checkpoints. Some comments suggested that AIT screening increases the wait time at security checkpoints. Specifically, a few individual commenters stated that the requirement to remove shoes, articles of clothing, belts, and other items slows the process of screening. Commenters generally stated that AIT machines are slow.

According to an individual commenter, screening procedures are not implemented consistently at checkpoints and airports because TSA employees are not familiar with the procedures. Another individual commenter stated that since metal detectors and pat-downs are the screening methods used for TSA employees and passengers using TSA's "Pre-Check" screening process, the general public should be screened in the same manner. Similarly, a few individuals suggested there are several loopholes in the AIT screening process (groups of passengers that are ineligible for AIT) that render AIT useless.

Others provided comments regarding the non-public nature of TSA's Standard Operating Procedures (SOPs). Most commenters questioned why information about screening procedures is not released to the public. An individual commenter stated that because the AIT scanners have been deployed, and "enhanced pat-downs" are in effect, TSA should be able to release procedures for the screening process. An advocacy group stated that, if TSA does not provide its SOPs to the public, the public will be unaware of the checkpoint requirements and what, if any, guidelines there are for decision-making by TSA staff or contractors as to what constitutes a screening. The commenter suggested that TSA has kept the SOPs from the public so screening practices can be varied and unpredictable. The commenter stated that as a result, travelers could not distinguish legitimate demands from illegitimate or unauthorized demands.

An individual commenter suggested that the majority of passengers are uninformed about the risks associated with AIT and the screening process. This commenter, as well as another individual, stated that passengers need to know what is expected of them at TSA checkpoints before they can give consent to how they will be searched. Similarly, another commenter stated that because TSA has the authority to fine passengers for refusing to complete screening, it is incumbent upon TSA to publish the details about the screening process.

A community organization stated that those with medical issues are often chosen for secondary screening at a higher rate than those without medical issues. According to a community organization, although the TSA Web site explains that the head coverings of travelers, including Sikh turbans, could be subject to additional security screening, TSA staff has advised Sikh travelers that screening of the turbans is mandatory, even if the screening device has not alarmed during screening. The same commenter also stated that Sikh travelers continue to experience disparate rates of secondary screening despite TSA's Web site stating that AIT scanners can detect threats under layers of clothing without physical inspection of the traveler. The commenter concluded that TSA should conduct public, independent audits of TSA screening practices to determine the extent of profiling based on race, ethnicity, religion and national origin. A non-profit organization, however, suggested that failure to profile passengers based on ethnicity, religion, and national origin would undermine risk-based security strategies.

Some commenters, including individuals and non-profit organizations, expressed concern regarding the potential theft of personal items during AIT screening. Several of these commenters suggested that alternatives like WTMD allow the passenger to maintain control of their non-metallic valuables during screening and that control is relinquished when a passenger is separated from their possessions to be screened by AIT.

TSA Response: TSA's procedures for checkpoint screening are described on TSA's Web site.[96] The description includes a specific explanation of AIT and pat-down procedures.[97] TSA uses AIT because it is the best technology currently available to address the known threat of nonmetallic explosives being concealed under clothing. Because the AIT alarms when it detects what it registers as an anomaly, at times additional screening must be performed to determine whether there is a threat. TSA advises passengers to remove all items from pockets to reduce the likelihood that the AIT will detect an item and that additional screening will be required. Passengers do not experience additional wait time due to

[93] *https://www.tsa.gov/travel/special-procedures/traveling-children* and *https://www.tsa.gov/travel/special-procedures/screening-passengers-75-and-older.*

[94] *https://www.tsa.gov/travel/passenger-support.*

[95] More information on TSA Civil Rights is available at *https://www.tsa.gov/travel/passenger-support/civil-rights.*

[96] *https://www.tsa.gov/travel/security-screening.*

[97] *Id.*

use of AIT equipment because the x-ray screening of carry-on baggage affects the overall screening process; in sum, passengers wait for their personal belongings regardless of which passenger screening technology is used. TSA encourages passengers to prepare for screening in advance by packing all personal items in their carry-on bag prior to entering the checkpoint in order to reduce the time spent in screening and to avoid the chance that such items will be left behind. As noted on the Web site, AIT screening is safe for all passengers and is generally available to all passengers.

TSA's SOPs are internal documents that contain instructions for TSOs on how to operate equipment and conduct screening. TSOs receive extensive training to perform screening as described in the SOPs. These documents are SSI and cannot be shared with the public. 49 CFR part 1520. The SSI status of these documents has been upheld by the courts and is outside the scope of this rulemaking.[98] However, public procedures and information regarding the screening process are described on TSA's Web site.

TSA's Pre✓™ program offers expedited screening for passengers identified as low-risk through pre-screening. For example, passengers who have a Known Traveler Number issued by TSA or U.S. Customs and Border Protection are considered lower risk because they have undergone a vetting process or background check. Because of the pre-screening, they are more likely to be eligible for expedited screening than passengers who have not undergone any type of pre-screening. TSA is encouraging all passengers to consider joining the program, and additional information is available on TSA's Web site.[99]

TSA does not engage in any type of religious profiling. Special consideration is given to passengers who wear religious head coverings. As explained on TSA's Web site, persons wearing any type of head covering may be subject to additional screening of the head covering if the TSO cannot reasonably determine that the head area is free of a threat item.[100] If it is necessary to remove the head covering, the passenger may request to remove it in a private screening area. All TSA employees are required to take religious and cultural awareness training, which includes information concerning certain types of head coverings. TSA's Web site also describes procedures for passengers with medical conditions.[101] While all passengers and items, including medical devices, must be screened prior to entering the sterile area of the airport, some medical devices must undergo additional screening in order to ensure that a threat item is not present. All such devices are permitted once cleared. Passengers with medical conditions may call the TSA Cares hotline to receive specific screening information.

TSA makes every effort to ensure that passengers are able to maintain sight of their carry-on baggage except while it is inside the x-ray machine. Generally, carry-on baggage is being x-rayed while the passenger undergoes AIT screening and usually the passenger completes AIT screening before the baggage screening is complete. TSA will cooperate with State and local law enforcement if a theft occurs. TSA has a zero-tolerance policy for theft by its officers. Any allegation of such activity is investigated, and if infractions are proven, offenders are disciplined, which can include removal from the agency's employment.[102]

X. AIT Technology Screening Procedures for Families and Individuals With Medical Issues

Comments: Some commenters discussed the adequacy of AIT screening procedures as they relate to families. Some individual commenters recommended that TSA not allow adults to conduct a pat-down on children. Furthermore, one of these commenters also stated that it is inappropriate for children under the age of 18 to be exposed to the AIT scanner. Although one individual commenter stated that children should never be separated from their parents, another individual commenter suggested that all travelers, including children and their families, should be subject to AIT because all other travelers are subject to AIT.

Many submissions addressed passengers with disabilities or medical conditions that make them ineligible for AIT screening. Several commenters expressed their general opposition to the use of AIT for those with medical conditions. Individual commenters explained that because of their insulin pumps they do not have a choice but to opt-out of AIT and therefore are subjected to invasive pat-downs and longer screening periods. Other commenters stated that the AIT scanners discriminate against those with a physical disability or medical issue. Some commenters suggested that travelers with physical disabilities should not be made to go through the often-taxing process of pat-down procedures. A privacy advocacy group stated that TSA has not considered the negative impact the proposed rule has on travelers with special needs, particularly those with medical devices. The commenter stated that aside from pat-downs, which the commenter described as embarrassing or humiliating, no alternative screening is discussed for those travelers who have medical devices, like prosthetics and pacemakers, which prevent them from being screened using an AIT scanner. An individual commenter expressed fear that the electromagnetic field of the AIT scanners may be calibrated to a level that would cause their heart pump to malfunction. An individual commenter stated that because the proposed rulemaking has not addressed the potential impacts that TSA screening activities may have on rape victims, TSA should stop using body imaging technology, cease the practice of pat-downs, and rely on the use magnetometers. An advocacy group and individual commenters expressed concern for the emotional effect that both pat-downs and body imaging technology can have on travelers who have experienced past emotional and physical trauma due to sexual assaults.

A number of individual commenters expressed concern regarding the AIT screening procedures and related privacy issues for transgender individuals. An advocacy group provided information regarding the term ''transgender'' and referred to Office of Personnel Management guidance on the process of gender transition. Several commenters, including advocacy groups, stated that transgender individuals are concerned that the screening process will lead to discrimination, the revelation of their gender status to screeners and others at the checkpoint, and humiliation. An individual commenter stated that transgender people often receive heightened scrutiny of their bodies and documents because of a lack of education and prejudice by TSA screeners. Some individual commenters and advocacy groups explained that the screening process for transgender individuals with prosthetics could be difficult because the prosthetics are detected as anomalies by the AIT scanners, which leads to a more extensive search of their person and questioning from TSA staff. Some individual commenters and advocacy

[98] *Blitz* v. *Napolitano*, 700 F.3d 733, 737 (4th Cir. 2012) (stating that ''the specifics of [TSA's checkpoint screening] procedures constitute SSI).

[99] *https://www.tsa.gov/tsa-precheck.*

[100] *https://www.tsa.gov/travel/frequently-asked-questions.*

[101] *https://www.tsa.gov/travel/special-procedures.*

[102] Since 2005, approximately 380 employees have been disciplined or terminated for theft.

groups discussed the need for an alternative to pat-downs and AIT screening for transgender individuals.

Some commenters, however, expressed support for the use of AIT. For example, travelers with joint replacements stated a preference for AIT because a full body search would otherwise be required with WTMD screening. An individual commenter who expressed support for AIT also recommended that the scanners be enlarged to accommodate medical equipment carried by travelers.

TSA Response: TSA's Web site contains information regarding screening procedures for children, travelers with disabilities and medical conditions, and transgender individuals. TSA has implemented procedures to make it easier for children under 12 to complete the screening process. For example, as explained on TSA's Web site at *www.tsa.gov/travel/special-procedures/traveling-children*, TSA will not separate adults from their children during screening. Children age 12 and under are allowed to leave their shoes on during screening. TSA has revised its pat-down procedures for children to be less invasive and its screening procedures more generally, to reduce the likelihood that a pat-down must be performed.[103] Absent extraordinary circumstances, pat-downs are only performed by TSOs of the same gender as the passenger. As discussed previously, the AIT has been tested and is safe for all passengers, including children.

TSA has specific screening procedures for passengers with disabilities and medical conditions, and those procedures are described on TSA's Web site.[104] These passengers are screened by the same technology as passengers without disabilities and medical conditions; however, additional screening of a passenger's equipment may also be required. As explained previously, the TSA Cares hotline can provide specific information for persons with disabilities and medical conditions. Depending upon the complexity of a passenger's needs, TSA Cares may forward a caller to disability experts at TSA who may arrange assistance at the airport, if necessary. TSA suggests that passengers with disabilities or medical conditions inform the TSO prior to undergoing screening. Passengers who prefer not to discuss their condition can obtain a Notification Card for discrete communications. The card is available at *www.tsa.gov/sites/default/files/disability_notification_card_508.pdf.* Passengers who have an insulin pump may be screened using AIT or may opt for a pat-down. The FDA millimeter wave report posted on TSA's Web site includes personal medical electronic device test results.[105] The FDA found that no effects were observed for any of the devices tested, including insulin pumps, pacemakers, neurostimulators, implantable cardio defibrillators, and blood glucose monitors, and that the risks that non-ionizing millimeter wave emissions could disrupt the function of the tested devices is very low.[106] TSA's Web site also advises that passengers with internal medical devices, such as a pacemaker or a defibrillator, should not be screened by a metal detector and should instead request to be screened using AIT or a pat-down. *See www.tsa.gov/travel/special-procedures.*

TSA advises passengers to remove all items from their pockets to lessen the possibility that a pat-down will be needed to resolve an anomaly detected by AIT. All AIT units used for screening are equipped with ATR software, which eliminates the individual image and only reveals a generic outline.

TSA recognizes the concerns of the transgender community and provides information on the screening process for transgender travelers on its Web site at *www.tsa.gov/travel/frequently-asked-questions.* TSA regularly meets with organizations representing the transgender community and works with them to discuss the screening process for transgender travelers. TSA notes that travelers may request a private screening with a witness or companion of the traveler's choosing at any point in the screening process. For travelers who have sensitivities to being touched, the majority of passengers can be screened without a pat-down so long as there is no need to resolve alarms. TSA is enhancing its training regarding the screening of transgender individuals to ensure that screening is conducted in a dignified and respectful manner.

TSA trains its officers to be courteous and to treat passengers with dignity and respect. Travelers who believe they have experienced unprofessional conduct at a security checkpoint are encouraged to request a supervisor at the checkpoint to discuss the matter immediately or to submit a concern to TSA's Contact Center at *TSA-ContactCenter@dhs.gov.* Travelers who believe they have experienced discriminatory conduct because of a protected basis may file a concern with TSA's Office of Civil Rights & Liberties, Ombudsman and Traveler Engagement (OCRL/OTE) at *TSA-CRL@tsa.dhs.gov*, or submit an online complaint at *https://www.tsa.gov/contact-center/form/complaints.*[107] Finally, travelers may also file discrimination complaints with DHS CRCL via CRCL's Web site at *http://www.dhs.gov/complaints.*

Y. Comments on the Proposed Regulatory Text

Comments: Many commenters addressed the regulatory text proposed in the NPRM. Many made the general assertion that the proposed rule is vague. Multiple commenters stated that the NPRM is not clear regarding a passenger's right to screening methods other than AIT. A few individual commenters suggested that, by not discussing alternative screening options, TSA is implying that passengers do not have a right to opt-out and be screened by a pat-down inspection. Further, an advocacy group requested that the language in the proposed rule should codify that all pat-down searches are to be conducted by officers of the same self-identified gender as the traveler, and not the gender listed on the identification document or the gender assigned to the passenger at birth. One of these commenters recommended that text be added to the regulation to specify alternatives for those with medical or other sensitive needs. An advocacy group stated that the failure to include information regarding an opt-out alternative in the proposed rule is in violation of the APA. An individual commenter suggested that text also be included to require appropriate notice to passengers about the use of AIT and information about the opt-out option be more extensive and posted. One of these commenters stated that the NPRM suggests that a passenger who opts-out of AIT screening is perceived as disrupting the security system. An advocacy group and individual commenters stated that the NPRM language stating AIT screening is currently optional indicates that TSA may impose mandatory AIT screening for all passengers in the future.

[103] TSA's screening procedures may be modified to respond to emerging threats and system vulnerabilities.

[104] *https://www.tsa.gov/travel/special-procedures.*

[105] 78 FR 18295. *See also https://www.tsa.gov/FOIA.*

[106] Compilation of Emission Safety Reports on the L3 Communications, Inc. ProVision 100 Active Millimeter Wave Advanced Imaging Technology (AIT) System, Version 2, DHS/ST/TSL–12/118, page v, September 1, 2012, available at *http://www.dhs.gov/sites/default/files/publications/tsa-compilation-of-emission-safety-reports-on-the-l3-communications-inc-ait-system.pdf.*

[107] More information on TSA Civil Rights is available at *https://www.tsa.gov/travel/passenger-support/civil-rights.*

A few individual commenters and advocacy groups stated that TSA should clarify key terms in the NPRM, including ''anomaly.'' A commenter stated that in the absence of any definitions of ''submit'' or ''screening,'' the rule would be unconstitutionally vague and overbroad. The commenter implied that such definitions are required in order for travelers to understand ''what is prohibited or what is forbidden'' by TSA. Similarly, an individual commenter and an advocacy group noted that the lack of details regarding screening and inspection leaves passengers uninformed regarding TSA's authority and what options passengers have. The advocacy group suggested that the lack of clarity leaves TSA checkpoint procedures unpredictable and inconsistent. An advocacy group recommended that if the word ''anomalies'' were changed to the detection of prohibited foreign items that pose special risks of creating physical danger in the aviation environment, the public's trust in TSA would increase.

Several commenters generally stated that the definition of AIT is ambiguous. A few commenters, including a privacy advocacy group, suggested that the definition of AIT was vague because it did not state that AIT involves the production of images. Similarly, a non-profit organization stated the definition of AIT is too broad in that it allows TSA to use other tools and technologies in addition to AIT. An individual commenter noted that the vagueness of the regulation leaves the reader with limited understanding of the intention of the NPRM. One individual commenter stated that the proposed regulatory text in the NPRM is unconstitutionally vague.

Similarly, an advocacy group suggested that the proposed rule should be revised to clarify the rights and responsibilities of passengers and TSA with regard to AIT scanning. The commenter stated that the *EPIC* opinion provides more information about TSA policy than the proposed rule and that the proposed rule does not fulfill the court order. This commenter concluded that the rulemaking process for AIT scanning should begin anew. According to an advocacy group, clarifying the limits of screening objectives will enhance the public's trust in TSA's screening program. Another individual commenter stated that the *EPIC* decision required TSA to develop written rules for screening at checkpoints. The commenter stated that the terminology used in these rules should be more descriptive of what will, and will not, occur during pat-downs.

Some commenters provided suggestions as to how the proposed rule could include protections for passengers. A non-profit organization requested that a ''code of conduct'' towards passengers and a ''passenger bill of rights'' be included in the regulations. Furthermore, an advocacy group suggested that (1) passengers have the option to be screened in private and with a witness of the passenger's choosing; (2) there be a limitation on the requirement for a passenger to lift or remove clothing; and (3) pat-downs be limited to the areas on the body where an anomaly was detected by the AIT scanner. The same advocacy group recommended that the TSA Traveler's Civil Rights Policy be codified in the final rule and should include nondiscrimination based on gender identity.

Some commenters recommended specific wording to be added to the proposed regulatory text to (1) allow TSA to search locations that are likely targets; (2) protect the Fourth Amendment concerns of private citizens; (3) eliminate costs associated with legal challenges; and (4) lower operational costs.

An individual commenter proposed adding text to clarify that screening to detect anomalies will be conducted using the least intrusive means. A community organization recommended expanding the proposed regulation to include specifics regarding how and when AIT can be used; when enhanced pat-down searches are to be conducted; that information on AIT be provided to passengers prior to AIT screening; to codify a pat-down search option; and to address the images generated by AIT. A non-profit organization suggested that the proposed rule define AIT as ''active'' imaging technology as opposed to ''advanced'' so the technology can be differentiated from ''passive'' imaging technology.

An advocacy group suggested that in order to assure passengers that images from the AIT scanners will not be retained, the definition of the AIT scanners should describe the technology as one that allows screening without subsequent retention of individual passenger image data. The same commenter proposed that training regarding how to work with diverse populations be required in the final rule.

A few commenters, including individual commenters and a non-profit organization, stated that TSA's summary of the proposed rule was a misrepresentation of the facts and screening options.

TSA Response: To address many of the comments on the proposed regulatory text, TSA is adopting the statutory definition of AIT codified at 49 U.S.C. 44901(l). The statute defines AIT more narrowly as ''a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body; and may include devices using backscatter x-rays or millimeter waves and devices referred to as 'whole-body imaging technology' or 'body scanning machines'.'' The definition of AIT in the final rule now refers specifically to ''a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body . . . .'' In addition, in recognition of privacy concerns, TSA is adopting the statutory language requiring the use of ATR software on any AIT used to screen passengers. The regulatory text now specifies that AIT must be equipped with and use ATR software. The regulatory text defines ATR as software that produces a generic image that is the same as the image produced for all individuals. Consistent with many comments received, this definition ensures that there are no passenger-specific images. TSA believes that the final rule's definition of AIT is more specific than the proposed definition in the NPRM and better ensures that the regulation is consistent with existing law. This definition also obviates the need for further requirements related to the potential storage and transfer of images, as the rule now requires images produced by AIT to be generic.

TSA declines to make a number of other changes to the regulatory text proposed by commenters. TSA does not refer to the option to undergo a pat-down instead of AIT in the regulatory text. As noted throughout this preamble, AIT use generally is optional. TSA recognizes that some passengers do not wish to be screened by AIT and generally, they may choose to undergo a pat-down. Other screening options are not permitted as the pat-down has the similar capability to detect both metallic and non-metallic threats. TSA also recognizes that some passengers are ineligible for AIT (for example, they are not able to stand unattended or raise their arms in the manner required for AIT screening). These passengers must undergo a pat-down in lieu of AIT. TSA also notes that it may require AIT use, without the opt-out alternative, as warranted by security considerations in order to safeguard transportation security. Thus, TSA has not codified an opt-out alternative in this rule.

As discussed above, in response to comments, TSA has removed the term ''anomaly'' from the regulatory text to avoid confusion regarding the meaning of the term. However, TSA is not adopting comments regarding the use of the terms ''screening'' and ''submit.'' These terms are used throughout TSA regulations; in the NPRM, TSA did not propose to modify any other regulatory provisions that use these terms, and TSA believes that it could be confusing to add a general definition that would affect those provisions. Nor does TSA believe that a definition specific to this section would be particularly useful, given that relatively few commenters found material ambiguity in the terms ''screening'' and ''submit.'' TSA notes that a definition of ''screening function'' is contained in 49 CFR 1540.5. TSA does not intend to alter that definition in this rulemaking. TSA's changes to the regulatory text are intended to maintain consistency with the definition of AIT developed by Congress to limit the use of AIT for screening passengers and to address privacy concerns. TSA believes that using a different definition or including terminology not used by Congress, such as ''active'' or ''passive,'' would not meaningfully enhance the clarity of the provision, and could create confusion about what is meant by ''active'' and ''passive.'' In addition, by adopting the statutory definitions in the regulation, TSA will deploy the types of AIT equipment that Congress intended to be used to conduct passenger screening.

As discussed in previous responses and in the NPRM, TSA's Web site provides a public description of AIT procedures for passengers. *See* 78 FR 18296–18297. The Web site also describes when a pat-down is performed, that a passenger may request private screening with a companion of the passenger's choosing, and that ordinarily a passenger will not be requested to remove or lift clothing to reveal a sensitive body area. TSA's screening procedures are sensitive security information, 49 CFR 1520.5(b)(9), and cannot be publicly divulged in significant additional detail. TSA strives to provide information on its Web site so that travelers will generally know what to expect when they arrive at an airport.

Congress has vested TSA with broad authority to use the equipment, measures and procedures TSA deems necessary to protect transportation security.[108] Current regulations already specify the responsibilities of passengers and other individuals who seek to enter the sterile area of an airport or board an aircraft. Regulations provide that ''[n]o individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft.'' *See* 49 CFR 1540.107(a). These regulations do not detail every particular screening method, policy, or technology that TSA employs at the checkpoint.[109]

In the NPRM, TSA proposed to codify the use of AIT to conduct security screening to comply with the ruling in *EPIC.* TSA is not adopting comments requesting that TSA also codify alternative screening options in the final rule. TSA may be unable to disclose details about some alternative screening options publicly. Federal law requires TSA to promulgate regulations to prohibit the disclosure of information obtained or developed in carrying out security that TSA decides would be detrimental to the security of transportation. 49 U.S.C. 114(r). TSA cannot publicly disclose all the information that would be necessary to allow for complete public discussion of security procedures and equipment, as some of the relevant information is SSI as specified in TSA regulations. *See* 49 CFR part 1520. In addition, some relevant information is classified and further restricted from public disclosure. It would not be practical for TSA to make every security measure public, as that would certainly make it easier for terrorists to circumvent such measures in order to carry out an attack.

In addition, codification of alternative screening options would seriously impede the flexibility needed to respond to security threats. TSA's procedures and equipment are designed to assist in the detection of concealed items that individuals are attempting to smuggle into the sterile area or on board an aircraft.[110] Depending on the circumstance, changes in certain procedures may be necessary on a global or case-by-case basis to respond in real-time to a threat, resolve an alarm, deal with equipment malfunctions, accommodate individuals with disabilities or other unique needs, or address other situations that could arise at the security checkpoint. For instance, sometimes types of clothing or physical attributes present particular challenges that require changes to screening techniques in order to conduct the thorough screening required to detect concealed items.

In short, TSA could not operate effectively if it was required to conduct notice and comment rulemaking whenever a change in a security equipment, policy, or procedure was needed. The APA generally does not require TSA to amend or issue regulations for most checkpoint screening equipment, policy, and procedure changes; for TSA to voluntarily submit to such a requirement would undermine TSA's ability to adapt quickly to new security threats and ''mire the agency in fruitless delay, expense, and inefficiency.''[111] Moreover, any additional regulatory text with sufficient flexibility for TSA to adapt quickly to new security threats would severely undercut the usefulness to the public of additional regulatory text. Instead, consistent with longstanding practice and the *EPIC* decision, TSA's regulations establish the requirement to undergo screening, and set the parameters under which TSA has the flexibility, within the bounds of its

[108] *See* 49 U.S.C. 114(e) (listing TSA's responsibilities to include ''day-to-day Federal security screening operations for passenger air transportation . . .''); 49 U.S.C. 114(f) (describing other TSA duties and powers to include ''develop policies, strategies, and plans for dealing with threats to transportation security . . . enforce security-related regulations and requirements . . . identify and undertake research and development activities necessary to enhance transportation security . . . inspect, maintain, and test security facilities, equipment, and systems . . . and oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities''); and 49 U.S.C. 44925 (directing DHS 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.'').

[109] Before TSA was established, the FAA operated under a very similar broad regulatory framework that also afforded discretion with respect to the specifics of checkpoint screening. *See, e.g.*, Airport and Airplane Operator Security Rules, 51 FR 1350 (Jan. 10, 1986) (final rule) (issuing former 14 CFR 107.20, which provided that ''[n]o person may enter a sterile area without submitting to the screening of his or her person and property in accordance with the procedures being applied to control access to that area''). In addition, just as TSA does now, the FAA typically responded to evolving threats by making changes to checkpoint screening procedures under its broad regulatory authority rather than by issuing new regulations. *Nader* v. *Butterfield*, 373 F. Supp. 1175, 1177 (D.D.C. 1974) (explaining that the FAA responded to ''an alarming rash of bomb threats and airplane seizures'' in 1972 by implementing new checkpoint screening procedures through a telegram emergency order to the agency's Regional Directors).

[110] *See George* v. *Rehiel*, 738 F.3d 562, 578 (3d Cir. 2013) (noting that TSA operates in ''a world where air passenger safety must contend with such nuanced threats as attempts to convert underwear into bombs and shoes into incendiary devices'').

[111] *Guardian Fed. Sav. & Loan Ass'n* v. *Fed. Sav. & Loan Ins. Corp.*, 589 F.2d 658, 668 (D.C. Cir. 1978).

statutory mandate as well as other applicable Federal laws and policies, to choose screening equipment, adopt specific screening policies, and ''prescribe the screening process.'' [112]

In addition, although TSA has determined not to codify additional policies and procedures in the regulatory text, TSA advises the public on what to expect at the checkpoint, and constantly strives to improve the screening experience. When TSA policies affecting screening are modified, TSA provides additional information to the public through its Web site as appropriate. TSA acknowledges the concerns expressed by commenters seeking assurance that they are being treated in accordance with established policies and procedures. TSA has posted screening information on its Web site to facilitate the secure and efficient processing of passengers when they arrive at an airport.[113] As explained above, TSA also provides various opportunities for individuals to obtain help in understanding the screening process, to express concerns regarding screening, and to submit complaints regarding unprofessional conduct by TSA personnel. Finally, TSA's training and procedures already require officers to treat every passenger with dignity and respect and make every effort to accommodate passengers' needs while processing through screening. Violations of these standards subject officers to discipline, up to and including termination.

Finally, regulatory text is not needed to address commenters' stated constitutional concerns as multiple courts of appeal have found that TSA's airport screening protocols do not violate the Fourth Amendment. For example, the *EPIC* decision holds that TSA's use of AIT is constitutional and meets legal requirements; although TSA's screening operations are of course subject to certain legal constraints, TSA is not required to describe or interpret every such constraint in this regulatory text. TSA has also explained its adherence to federal law and DHS policies regarding the use of race, ethnicity, gender, national origin, religion, sexual orientation, or gender identity in agency operations. To the extent that such generally applicable policies have applications in the checkpoint screening context, it would be unnecessary, unduly cumbersome, and outside the scope of this rule to reiterate such policies in the instant rulemaking in particular. Similarly, TSA adheres to the statutory requirements regarding the conduct of screening of persons and property and will not include SSI in its public rules. In response to the commenter who identified certain costs for TSA to include in the regulation, TSA notes that costs are described in the RIA accompanying this final rule.

Z. Costs of the Proposed Rule

Comments: Dozens of submissions addressed the overall costs associated with the proposed rule. Several individual commenters and a non-profit organization stated that AIT scanners would be too costly, and suggested that TSA invest in other, less expensive screening methods. Another individual commenter stated that the cost analysis should have included a rigorous probability and statistical analysis to estimate ''difficult to compute'' costs for sub-populations. For example, the commenter suggested that TSA include costs for travelers who are more vulnerable to radiation, immune-suppressed, or suffering from skin cancer. With regard to the RIA posted in the docket, an individual commenter asked TSA to clarify the units for the cost data included in Summary Tables 4 through 6.

TSA Response: TSA estimated the costs of AIT and compared to four and five other alternatives in the RIA for both the NPRM and final rule RIA, respectively. TSA determined that AIT has a number of advantages over the other alternatives. AIT maintains lower personnel cost and a higher passenger throughput rate than other alternatives considered (for detailed description of alternatives see Chapter 3 in both the NPRM and final rule RIAs). After weighing the qualitative advantages and disadvantages of each alternative, TSA elected to maintain AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats.

TSA performed its cost analysis using the most recent, comprehensive and readily available data. Federal law and regulations require all passengers to be screened prior to boarding an aircraft. There was no need to perform a probabilistic or statistical analysis to estimate the populations affected as TSA used its actual passenger screening records in its estimates. Furthermore, data used to determine AIT capabilities are based on years of tests on detection capabilities and performance standards. TSA did not include radiation-related costs in the RIA because the level of radiation from AIT was determined to be so low as to present a negligible risk to passengers, airline crew, airport employees, and TSA employees. The machines were tested, and doses were found to be below the ANSI/HPS standards. The standards consider the impact of radiation on individuals, such as pregnant women, children, and persons who receive radiation treatments, who may be more susceptible to radiation health effects. AIT equipment has been subject to extensive, independent testing that has confirmed that it is safe for individuals being screened, equipment operators, and bystanders. The exposure to ionizing x-ray beams emitted by the backscatter machines that were removed pursuant to statute, as well as the non-ionizing electromagnetic waves from the millimeter wave machines are well below the limits allowed under relevant national health and safety standards [114] (See Chapter 2, page 104 of the NPRM RIA).

The cost estimates in the NPRM RIA Summary Tables 4 through 6 are displayed in thousands of dollars, as presented in the table titles as ''Costs in $1,000s.'' For example, $1 shown in Table 4 represents one thousand dollars. In the final rule RIA, costs are presented in millions of dollars throughout the document to avoid confusion.

AA. Passenger Opportunity Costs

Comments: Dozens of submissions directly addressed passenger opportunity costs associated with the proposed rule. Individual commenters and advocacy groups stated that TSA did not include adequate costs for passenger delays due to AIT. Using average time lost passing through security and average wage rates, several of these commenters estimated additional passenger opportunity costs ranging from $450 million per year to $15.2 billion per year. One commenter estimated the additional delay in terms of lost lifetimes and stated the proposed rule would lead to 18 lifetimes lost per year due to waiting in passenger screening lines. An advocacy group cited a 2008 report that found TSA security increased delays by 19.5 minutes in 2004. A commenter also suggested that TSA estimate other opportunity costs associated with opt-outs, including the cost of enduring the

[112] *EPIC*, 653 F.3d at 3.

[113] *See* for example, *www.tsa.gov/travel/security-screening* and *www.tsa.gov/travel/special-procedures.*

[114] The FDA has found that millimeter wave is safe and states on its Web site ''[m]illimeter wave security systems which comply with the limits set in the applicable national non-ionizing radiation safety standard . . . cause no known adverse health effects.'' *http://www.fda.gov/Radiation-Emitting Products/RadiationEmittingProductsand Procedures/SecuritySystems/ucm227201.htm.*

pat-down itself, because both the passenger and the TSA agent would prefer to avoid the pat-down.

Many other commenters, including a non-profit organization and individuals, suggested that the proposed rule would increase wait times at the security checkpoints, leading to passenger delays. At least one comment referenced an examination of AIT use in Australia that found that passenger screening time through the trial lane took slightly longer than the passenger screening time through a standard screening lane, most likely caused by the higher alarm rate, with the data suggesting that the average passenger is six times more likely to alarm in the body scanner than the standard lane. Some commenters estimated that the process of opting out—including waiting for a TSO of the same-sex to perform the pat-down—from AIT would delay a passenger by at least 15 minutes. The commenters urged TSA to account for the additional time spent by passengers waiting to pass through airport security. An individual commenter suggested that AIT would reduce wait times for screening, particularly for passengers with joint replacements that would otherwise trigger WTMDs.

TSA Response: Overall passenger screening system times do not increase with AIT. Passengers currently experience delays at the checkpoint attributable to the screening of carry-on luggage and personal belongings, which has been a Federal requirement even before the creation of TSA, and which was included as part of the baseline for the passenger opportunity cost assessment. For more information on equipment throughput rate, see Regulatory Impact Analysis Chapter 2: AIT Deployment Costs. Although the AIT with ATR (current AIT technology being used) throughput rate is lower than the WTMD, the passenger screening system and passengers are constrained by the x-ray machines that screen carry-on baggage and personal belongings. With regard to examination of AIT in Australia, the commenter failed to cite the full context of the findings which stated ''This [additional seconds of delay] was caused by a number of factors, some of which can be mitigated through refining the process and procedures, and some of which will be minimized as screening officers and passengers becoming more familiar with the new technology.'' [115] Additionally, TSA's security checkpoints and standard operating procedures may differ from the logistics exercised in the trial in Australia. TSA relies on its own findings from the field to make a determination of wait times in the RIA. The small percentage of passengers who choose to opt out of AIT screening will incur opportunity costs due to the additional screening time needed to receive a pat-down. In the NPRM RIA, TSA estimated that 1.8 percent of all passengers opt-out of AIT and receive a pat-down. Only a small percentage of passengers will experience an increased wait time. TSA agrees that it should add additional time to account for waiting for a same gender TSO to perform the pat-down. However, TSA disagrees that an average wait would be as long as 15 minutes. TSA has added an additional 70 seconds to the total pat down procedure time to account for the time spent waiting for the same gender TSO. In some instances, a same gender TSO is only seconds away from the passenger and in other cases, the wait is longer. Based on TSA field tests, TSA estimates an average additional wait of 70 seconds. TSA already estimates that the pat-down procedure itself takes 80 seconds. In total, TSA estimates that, on average, a passenger that opts-out of AIT screening will incur an additional wait time of 150 seconds (70 second average wait time for the same gender TSO to meet the passenger and 80 seconds to complete the pat-down procedure). TSA estimated per passenger opportunity cost of opting out of AIT by multiplying the additional wait time by the average passenger value of time,[116] estimated at $43.44 per hour in the NPRM RIA. TSA used expected wage rates to base the value of a person's opportunity cost, which is widely accepted as an appropriate valuation of a person's value of time. The Passenger Opportunity Cost section, found in Chapter 2, page 49 of the NPRM RIA, explains in further detail the opportunity cost estimate and methodology. TSA was unable to quantify or monetize other intangible costs relating to opting out of AIT screening and receiving a pat-down (*e.g.*, personal preference). In the final rule RIA, the opt-out rate and passenger value of time have been revised to reflect the most recent data.

BB. Airport Utility Costs

Comments: A commenter suggested that TSA underestimated airport utility costs because the analysis uses a constant utility cost per unit installed over the 8-year lifecycle. The commenter stated that since electricity prices have increased at an average rate of 1.53 percent annually, if the analysis allowed for the price of electricity to grow at this rate, the total estimated utility cost would increase.

TSA Response: Energy cost fluctuations are driven by two factors: Real changes in costs and inflation. In the NPRM RIA, TSA accounted for real changes in utility costs by averaging prices for years 2007–2011 as reported by the U.S. Energy Information Administration. TSA used this average to estimate utility costs for the years 2012–2015. TSA did not incorporate annual inflation increases for any costs in the RIA in accordance with Office of Management and Budget (OMB) Circular A–4 guidelines.[117] In the final rule RIA, TSA once again used the U.S. Energy Information Administration for its historical energy prices in 2008–2012 and used their projections for real energy prices for 2013–2017.

CC. TSA Costs

Comments: Many comments addressed TSA's costs associated with the proposed rule. A commenter stated that by incurring $1.5 billion in costs to-date without following the proper protocol under the APA, TSA has committed a gross breach of its fiduciary responsibility. Other commenters suggested that TSA's AIT-related costs are unjustifiably high. Another commenter urged TSA to document and disclose all AIT-related costs, including purchase price, maintenance costs, and personnel costs.

Some submissions addressed TSA's personnel costs associated with the proposed rule. Some commenters stated that AIT operation requires more TSOs than the WTMD, which results in larger payroll costs. Another commenter disputed TSA's estimates of personnel costs. Specifically referencing the constant salary used to estimate personnel costs in the RIA, the commenter stated that using a salary level that grows over time by 1.15 percent would increase personnel costs by $33 million.

Many submissions addressed TSA's equipment costs associated with the proposed rule. A few commenters identified equipment costs that they stated were missing from the RIA. An individual commenter and a non-profit

[115] Department of Infrastructure and Transport, Australian Government, ''Optimal Technologies Proof of Concept Trial Report,'' Feb. 28, 2012.

[116] U.S. Department of Transportation, ''Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis,'' Sep. 28, 2011. DOT estimates an hourly rate of $42.10 in table 4 of this report and TSA inflated this estimate to 2011 dollars at $43.44. *http://www.dot.gov/sites/dot.dev/files/docs/vot_guidance_092811c.pdf.*

[117] Page 32 of OMB Circular A–4 states: ''In presenting the stream of benefits and costs, it is important to measure them in constant dollars to avoid the misleading effects of inflation in your estimates.''

organization asked TSA to clarify whether the analysis accounts for the cost of installing AIT scanners in every security lane. One commenter compared TSA's equipment costs to independent estimates and concluded that TSA's lower cost estimates do not include an estimate of the number of AIT scanners needed nationwide. Another commenter stated that the analysis does not include the cost associated with replacing the AIT scanners every 8 years. An individual commenter asked TSA to provide detail on the maintenance cost assumptions in the analysis. The commenter urged TSA to base AIT maintenance costs on actual experience (*e.g.*, total service calls required in recent years). Another commenter declared that the AIT machines are expensive and recommended other security-related equipment that TSA could invest in instead (*e.g.*, improved sensors for baggage).

TSA Response: With respect to comments regarding TSA's fiduciary responsibility, TSA has deployed AIT consistent with its statutory authority and as directed by Congress and the President. All costs incurred to deploy AIT have been accounted for and approved in the Federal budgeting process.

TSA estimated all personnel costs associated with the deployment of AIT. For the RIA, which accompanied the NPRM, TSA estimated this cost using assumptions from TSA's Screener Allocation Model (SAM) that dictates the allocation of personnel to each airport. The SAM takes into account the number of personnel it takes to operate WTMDs and AITs and also the different configurations (or ''modsets'') in which these machines are implemented. TSA based its estimation of personnel costs on the number of AIT machines that were forecasted to be deployed nationwide for years 2012–2015 and the number of personnel required to operate each machine. Finally, TSA applied the average TSO's fully loaded wage rate to estimate costs.[118] TSA did not incorporate annual increases in inflation for any costs in the RIA, including personnel costs, in accordance with OMB Circular A–4 guidelines. A full description of these costs is in Chapter 2 in both the NPRM and final rule RIA.

TSA estimated the full life cycle costs relating to the use and deployment of AIT. TSA divided the cost components into four categories: Acquisition, installation, and integration; maintenance; test and evaluation; and program management office (PMO) costs. With respect to the comment on the replacement costs, replacement costs are not included in a life-cycle analysis. The RIA analyzes costs and benefits for one life-cycle of AIT and therefore does not include replacement costs.

A full description of these costs is in Chapter 2 of both the NPRM and final rule RIA.

TSA compared AIT to other alternatives and concluded that AIT is the alternative that represents the best technology, currently available, to detect metallic and nonmetallic threats to commercial air travel.

DD. Other Costs

Comments: Hundreds of submissions addressed other costs associated with the proposed rule. Several commenters identified additional costs that they stated should have been included in the RIA. A few commenters, including an individual commenter and advocacy groups, suggested that the use of AIT would have a cost impact on the aviation and travel industries, which the RIA does not quantify. Some commenters cited a 2007 study that shows demand for air travel could decline by 6 percent on all flights and by about 9 percent on flights departing from the nation's 50 busiest airports, reduce airline revenue, and increase airline costs and passenger fees. Approximately 80 submissions addressed other travel impacts associated with the proposed rule. Many commenters, including non-profit organizations, an advocacy group, and individual commenters stated that the traveling public would avoid air travel, causing individuals to drive or take the train. Some of these commenters stated that there would be increased roadway fatalities because of the increase in motor vehicle travel (some estimated as many as 500 additional deaths per year). The commenters suggested that the analysis should account for the cost associated with these additional fatalities. Other commenters indicated that reduced air travel, including from international tourists, would affect the airline industry, and TSA should estimate these financial impacts.

Other commenters recommended that TSA include estimates for legal costs in the cost-benefit analysis because of the likelihood of further litigation regarding the use of AIT. An individual commenter suggested that AIT scanners would result in medical equipment costs to passengers (*e.g.*, damage to insulin pumps). An advocacy group urged TSA to include costs associated with infringement on civil liberties and on privacy, but acknowledged that these costs are not easily quantifiable. An advocacy group urged TSA to include passenger privacy impacts in the cost-benefit analysis.

A commenter requested that TSA provide clarification on the assumptions used to develop the AIT program management costs (*e.g.*, 10 percent of passenger screening costs). Another individual commenter suggested that TSA consider using a random selection AIT screening process in order to reduce the costs of the rule.

TSA Response: With respect to quantifying any loss from a decline in the demand for travel, TSA reviewed the study[119] cited in the comments. The study was published in 2007—before AIT was deployed—and therefore did not provide estimated impacts on airline revenues and passenger demand related to AIT. The study's results appear to have been based on security measures well outside the scope of AIT, such as the federalization of passenger security screening at all U.S. commercial airports and the requirement to begin screening all checked baggage in 2002. As TSA previously explained, the baseline from which the costs and benefits of this rule are estimated is not ''no TSA screening'' or ''no screening at all.'' The baseline of this rule is how TSA would accomplish screening without AIT. TSA used WTMD as the primary passenger screening technology at passenger screening checkpoints prior to the deployment of AIT. Therefore, the costs and benefits of this rule are compared to WTMD as the primary screening tool. Although it is possible that a security measure could be implemented that would have a measurable impact on the commercial aviation demand, in this case, TSA has not seen credible evidence that AIT is such a security measure.

TSA analyzed the potential cost impacts associated with the implementation of AIT in its cost analysis. TSA concluded that there are no additional legal costs to stakeholders for the deployment and use of AIT pursuant to TSA regulatory requirements. Litigation costs are not a direct cost of the rule because such costs do not result from compliance with the rule. Additionally, any estimate of litigation expenses would be highly speculative and would not inform TSA's decision of AIT deployment. However,

[118] A ''fully loaded'' wage rate includes the cost of wages paid to the employee plus the costs of employee benefits such as paid leave and health care.

[119] Blalock, Garrick, Kadiyali, Vrinda, Simon, and Daniel H., ''The Impact of Post 9/11 Airport Security Measures on the Demand for Air Travel,'' Journal of Law and Economics, Apr. 30, 2007, *http://dyson.cornell.edu/faculty_sites/gb78/wp/JLE_6301.pdf.*

TSA acknowledges that to the extent parties choose to enter into litigation on AIT, there are indirect costs associated with that litigation.

The most significant advantage of using AIT is the enhancement of air transportation security because AIT can detect nonmetallic threats concealed under clothing. It also reduces the need for a pat-down, which would be required with the WTMD for individuals with medical implants such as a pacemaker or a metal knee replacement. Thus, AIT reduces the cost and inconvenience to passengers with this medical equipment. As explained in a previous response, the FDA tested the effect of AIT on different types of medical devices, including insulin pumps, and found no impact. Thus, TSA does not include costs of medical devices in the analysis.

Before the development of the ATR software, TSA instituted rigorous safeguards to protect the privacy of individuals who are screened using AIT. The DHS Chief Privacy Officer conducted several PIAs to ensure that TSA adequately addressed privacy concerns related to AIT screening. The PIA describes the strict measures TSA uses to protect privacy. While TSA was unable to produce a quantitative impact of perceived privacy issues, TSA included a thorough qualitative discussion regarding this issue in the NPRM RIA (Chapter 2, page 99). Additionally, TSA did not receive any public comments providing a methodology to be used on the economic valuation of how perceived privacy issues could be calculated. Finally, the use of AIT to screen passengers has been upheld by the courts as reasonable under the Fourth Amendment, even prior to the mandatory use of ATR.

To run the passenger screening program, TSA provides internal PMO support and contractor support. Because PMO support reflects the day-to-day support of the entire screening program, TSA is unable to identify PMO spending allocated to AIT specifically. To account for these costs to AIT, TSA assumed that the PMO cost was 10 percent of the total cost of AIT in the NPRM RIA, based on subject matter expert estimates from other technology contracts. For the final rule, TSA revised this estimate to 15 percent based on an internal Life Cycle Cost Estimate analysis of the passenger screening program.

Finally, TSA addresses the use of random selection in its discussion of alternatives considered, apart from AIT, in Chapter 3 of the final rule's RIA.

EE. Benefits of the Proposed Rule

Comments: Approximately 20 submissions directly addressed the benefits associated with the proposed rule. Many individual commenters and a non-profit organization stated that TSA did not quantify the benefits of AIT or provide documentation to support the claims made in the benefits analysis. One of the commenters stated that it is not acceptable for TSA to keep its risk-based benefits analysis confidential, and urged TSA to assess the risk of a terrorist attack relative to the risks associated with AIT (*e.g.,* cancer and increased roadway fatalities). Another commenter recommended that TSA provide an estimate of how much AIT reduces the probability of a successful terrorist attack, or provide a break-even analysis that would estimate the number of terrorist threats that must be prevented in order to cover the costs of the AIT. A non-profit organization stated that the risk reduction benefits that TSA claims in the analysis are not attributable to AIT because there have been no successful terrorist attacks originating from U.S. airports since September 11, 2001, even before TSA began deploying AIT scanners. Another commenter stated that AIT scanners provide negligible security benefits.

Several individual commenters and a non-profit organization discussed benefits in terms of the number of attacks that need to be thwarted in order to justify the costs of the AIT rule. Some of these commenters, including two non-profit organizations, cited a research study that concluded AIT would need to avert more than one attack originating from a U.S. airport every 2 years in order to justify the cost of the scanners. The commenters stated that AIT would not achieve this threshold. An individual commenter suggested that had AIT scanners been used over the last 12 years, only two attacks would have been avoided. The commenter stated this would not have justified the cost. Another individual commenter stated that people are more at risk of dying in motor vehicle accidents than in a terrorist attack on an airplane originating in the United States. The commenter concluded that AIT would not be the most efficient approach to reducing risk. Other commenters stated that AIT would not increase security to the degree TSA claims until deployed in every airport and every security lane. A commenter argued that because ''a potential terrorist intent on downing an airliner with body-borne explosives would need only to observe which airports or security areas lack [AIT] scanners to defeat the security measure.'' The commenter suggested that the absence of an attack could not be attributed to AIT.

Some commenters recommended types of benefits that should be analyzed. An individual commenter suggested that TSA quantify the benefits of the rule in terms of lives saved and avoided disruptions to the economy. Another commenter stated that the analysis should consider the potential benefits of reallocating the costs associated with AIT to other screening methods.

TSA Response: TSA disagrees that AIT provides no security benefits. Contrary to commenters' belief that the lack of successful attacks shows AIT offers no security benefits, TSA believes the lack of successful attacks actually lends support to the opposite conclusion. Given the continued threat to commercial aviation from terrorist attacks, and the fact that the shift to nonmetallic explosives by terrorists presents a serious threat to homeland security, TSA needs technology capable of detecting non-metallic objects. AIT is a proven technology based on laboratory testing and field experience that provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger. In addition to AIT's ability to detect concealed objects, TSA also believes AIT offers a powerful deterrence effect. Morral and Jackson (2009) stated, ''Deterrence is also a major factor in the cost-effectiveness of many security programs. For instance, even if a radiation-detection system at ports never actually encounters weapon material, if it deters would be attackers from trying to smuggle such material into the country, it could easily be cost-effective even if associated program costs are very high.''[120] Given the demonstrated ability of AIT to detect concealed metallic and non-metallic objects, it is reasonable to assume that AIT acts as a deterrent to attacks involving the smuggling of a metallic or non-metallic weapon or explosive on board a commercial airplane. As an essential component in airports' compressive security system that can detect a non-metallic weapon or explosive concealed under a person's clothing, AIT plays a vital role in decreasing the vulnerability of

[120] Andrew R. Morral, Brian A. Jackson., ''Understanding the Role of Deterrence in Counterterrorism Security,'' 2009, Rand Homeland Security Program, *http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf.*

commercial air travel to a terrorist attack.

Other commenters stated that AIT might provide some level of security benefits, but that it was not worth the cost. Commenters stated the risk reduction benefits of AIT in particular made it a poor investment and that people are more at risk of dying in motor vehicle accidents than in a terrorist attack on an airplane originating in the United States. One commenter stated that risk of a terrorist attack to commercial aviation is so low that it is a risk that can be endured by the public. TSA disagrees that the risk reduction attributable to AIT does not make AIT worth using. TSA is charged with safeguarding the travelling public with respect to aviation and fulfilling legal mandates. Risk and national security are complex issues and commenters may not be considering that a perceived low level of risk may be due to deterrence provided by AIT or other national security efforts to prevent such attacks.

Another commenter stated that the benefits from AIT would not be fully realized until AIT is deployed at every airport and in every checkpoint lane. While TSA did not provide monetized benefits or ''degree of benefits,'' TSA did describe the fact that AIT is the only technology currently available for field deployment that can detect both metallic and non-metallic weapons and explosives. Additionally, implementing an ''all or nothing'' strategy for airport security ignores the fact that some airports are at a higher risk for a terrorist attack than others are. TSA uses a risk-based approach to deploy AIT machines in airports that are considered higher-risk in order to try to minimize risk to commercial air travel given TSA's finite resources. Other commenters stated that AIT is a poor investment for screening and that TSA should use its funds in another technology or manner altogether. Another commenter argued that the baseline security infrastructure (pre-AIT) is capable of handling the current level of risk to commercial air travel. Both conclusions discount the fact that currently, AIT is the only screening technology able to detect a non-metallic weapon or explosives concealed under a person's clothing. Eliminating AIT would increase the risk to successful terrorist attacks than what is currently incurred because it would leave commercial air travel more vulnerable to an attack with a non-metallic weapon or explosive. The commenters also stated that the risk of a terrorist attack to commercial air travel was less than that of a fatal motor vehicle accident. It is unclear to TSA how the risk associated with motor vehicles should influence TSA's decision making on airport screening practices. Regardless of the safety or security risks associated with other modes of transportation, TSA should pursue the most effective security measures reasonably available so that the vulnerability of commercial air travel to terrorist attacks is reduced.

Commenters that consider only the most easily quantifiable impacts of a terrorist attack, such as the direct cost of an airplane crashing, are only considering a portion of the impacts of an attack. As TSA explained in the NPRM's Initial RIA, terrorist attacks not only cause direct costs in lives lost and property damage, but also cause substantial indirect effects and social costs (such as fear) that are harder to measure but which must also be considered by TSA when deciding whether an investment in security is cost-beneficial. For example, Ackerman and Heinzerling state ''. . . terrorism 'works' through the fear and demoralization caused by uncontrollable uncertainty. Efforts to offset this fear by attaching necessarily arbitrary numbers to the probabilities of being harmed by a terrorist seem, especially in a post-September 11 world, ridiculous.'' [121] In addition, Pidgeon, Kasperson and Slovic state the 9/11 attacks had consequences that spanned ''a range of behavioral, economic, and social impacts.'' [122]

In addition, AIT use is fully consistent with TSA's mandate. The Administrator of TSA has overall responsibility for civil aviation security, and Congress has conferred on him authority to carry out that responsibility.[123] Federal law requires that he ''assess threats to transportation,'' and ''develop policies, strategies, and plans for dealing with threats to transportation security.'' [124] TSA agrees that it should incorporate consideration of costs and other factors into its risk management practices, *see, e.g.,* 49 U.S.C. 44903(b), but notwithstanding the suggestion of a number of commenters, it would be plainly contrary to congressional intent for TSA to ignore known terrorism risks to aviation security by relying on outdated screening practices until the next attack proves the commenters wrong. Based on TSA's experience using AIT in the airport environment, TSA believes that the use of AIT satisfies the express mandate of Congress.

TSA has added break-even analysis to the benefits section in the final rule. According to OMB Circular No. A–4, ''Regulatory Analysis,'' the break-even analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?'' [125] In both the NPRM and final rule RIAs, TSA also provided a qualitative assessment of the benefits of AIT. Low probability, high consequence events such as terrorist attacks are difficult to measure with any level of certainty. TSA analyzed the threats to the aviation sector and found that the use of AIT reduces the risk of metallic and non-metallic threats to airport security as described in Chapter 4 in both the NPRM and final rule RIAs. Both RIAs also qualitatively described some of the indirect impacts from a successful attack on commercial air travel. Specifically, TSA noted how the 9/11 attacks caused a negative impact on gross domestic product growth and that fear, a social cost, can lead to other social costs which would cause the economy to suffer if people are afraid to fly.

FF. Other Impacts of the Proposed Rule

Comments: Many submissions addressed health impacts associated with the proposed rule. Several individual commenters identified alleged health impacts that TSA should have accounted for in the cost-benefit analysis. The commenters suggested that the analysis should include costs or risk information for radiation-related illness, emotional distress, and special medical conditions.

Commenters also stated that using AIT scanners would lead to lost or stolen property. Another commenter stated that the RIA failed to account for decreases in economic productivity because of the rule. Further, an individual commenter suggested that the proposed rule is not justified because the investment in AIT scanners would not reduce mortality by as much as other government programs or initiatives. In particular, the commenter suggested that AIT would not prevent terror attacks but would instead redirect them to alternate locations. Another commenter stated that the analysis should consider the use of newer

[121] Frank Ackerman and Lisa Heinzerling, ''Priceless: On Knowing the Price of Everything and the Value of Nothing,'' 136–137 (2004).

[122] Nick Pidgeon, Roger E. Kasperson, and Paul Slovic, ''The Social Amplification of Risk,'' p. 16, 2003.

[123] 49 U.S.C. 114(d).

[124] 49 U.S.C. 114(f).

[125] *http://www.whitehouse.gov/omb/circulars_a004_a-4/.*

technologies that might work better and cost less.

TSA Response: With regard to comments on health concerns, the millimeter wave AIT systems used by TSA comply with the 2005 IEEE Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std.C95.1TM–2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494–522, published April 1998. TSA's millimeter wave units are also consistent with Federal Communications Commission OET Bulletin 65, Health Canada Safety Code, and RSS–102 Issue 3 for Canada. The FDA also confirmed that millimeter wave security systems that comply with the IEEE Std. C95.1TM–2005 cause no known adverse health effects.

TSA also addressed potential health concerns regarding the ionizing radiation emitted by general-use backscatter technology. The radiation dose a passenger receives from a general-use backscatter AIT screening has been independently evaluated by the FDA's Center for Devices and Radiological Health, the National Institute for Standards and Technology, the Johns Hopkins University Applied Physics Laboratory, and the American Association of Physicists in Medicine. All results affirmed that the radiation dose for individuals being screened, operators, and bystanders was well below the dose limits specified by ANSI/HPS N43.17.

TSA does not believe, and no compelling evidence has been submitted, that AIT increases the risk of lost or stolen property. Passengers are able to monitor their bags prior to submission into the x-ray machine and after x-ray screening is completed. The deployment of AIT does not create vulnerabilities in the security system since testing and experience have shown that AIT is the best technology currently available to detect metallic and nonmetallic threats (see Chapter 4 of both the NPRM and final rule RIA).

TSA does not believe, and no credible evidence has been submitted, that AITs reduce economic productivity. With regard to comments that AIT does not reduce mortality rates as much as other government programs or initiatives, the funding of other government programs is beyond the scope of this rule. Regardless of the effectiveness of other governments programs, TSA should pursue the most effective security measures so that the vulnerability of commercial air travel to terrorist attacks is reduced. TSA conducted an alternatives analysis and found AIT to be the most effective countermeasure for both metallic and non-metallic items concealed under a person's clothing. With respect to AIT redirecting attacks to other targets, TSA does not believe that the existence of other targets precludes TSA from ensuring the security of commercial air travel, which has a high level of risk. TSA included the costs of research and development for AIT and for the deployment of AIT technology (see Chapter 2 in both the NPRM and final rule RIA). TSA will continue to conduct research and evaluate new technologies to enhance transportation security.

GG. Regulatory Alternatives

Comments: Some submissions commented on Alternative 1 (no action). Several individual commenters and non-profit organizations expressed support for Alternative 1, and urged TSA to revert to the use of metal detectors as the primary screening method.

Multiple submissions also commented on Alternative 2 (combination of WTMD and pat-down). Several commenters suggested that screening consisting of pat-downs and metal detectors would be sufficient. A few commenters suggested that because AIT scanners are not effective and are intrusive, a combination of WTMD and pat-down screening should be used instead.

Many submissions commented on Alternative 3 (combination of WTMD and ETD screening). Individual commenters, a non-profit organization, and advocacy groups expressed support for Alternative 3 without providing additional substantive comment. Commenters suggested that the use of ETDs and WTMDs are more effective, less costly, and less intrusive.

Many submissions discussed other alternatives for TSA consideration. A non-profit organization, a privacy advocacy group, and individual commenters recommended that TSA return to using WTMDs and hand-wand metal detectors during the screening process. Other commenters urged TSA to rely on traditional police and intelligence work and canine explosives detection teams to detect and deter threats. A commenter recommended that TSA use mass spectrometry methods to detect threats in air samples. Other commenters suggested TSA explore other technologies to reduce reliance on AIT and pat-downs and to be able to detect explosives within body cavities. A non-profit organization recommended that TSA consider testing face recognition, explosives residue machines, and suspicious behavior systems for secondary screening. Another non-profit organization urged TSA to use less invasive screening technologies such as infrared imaging.

TSA Response: With regard to Alternative 1, recent events demonstrating that terrorists may use nonmetallic explosives to take down an aircraft highlight the need for a technology capable of detecting non-metallic threats concealed on passengers. Alternative 1 fails to address that threat. It also fails to meet the instruction provided in the Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack, issued January 7, 2010 as well as congressional directives. While this alternative imposes no additional cost burden, it does not mitigate the threat to aviation security posed by nonmetallic explosives and weapons. For this reason, TSA rejected this alternative in favor of deploying AIT to screening checkpoints.

Alternative 2 is more physically intrusive than AIT, significantly increases the wait times and opportunity costs for the traveling public, and is more costly with respect to personnel because it requires more TSOs to meet the high volume of passengers. In addition, this alternative does not provide the same level of screening as AIT in detecting nonmetallic threats because not every passenger would receive a pat-down, particularly when used only on a random basis. Based on field tests, TSA estimates the pat-down procedure takes 150 seconds to perform (70 second average wait time for the same gender TSO to meet the passenger and 80 seconds to complete the pat-down procedure). Therefore, performing pat-downs on a significant number of passengers necessitates either a substantial increase in staffing levels to maintain the current passenger throughput level (approximately 150 passengers per hour per lane) or abandonment of that throughput target altogether, with the attendant consequences for passengers described above. Finally, AIT is a machine-based methodology for detecting non-metallic threat items, which provides a more consistent outcome over time. TSA anticipates future advancements to AIT in detection capability, throughput, and privacy protection. Due to the reasons outlined above, TSA rejected Alternative 2.

With regard to Alternative 3, although ETDs would help reduce the risk of nonmetallic explosives being taken through the checkpoint, ETDs cannot detect other dangerous items such as weapons and improvised explosive device components made of ceramics or plastics, whereas AIT is capable of detecting anomalies concealed under clothing. Second, incorporating ETD screening into the current checkpoint screening process would negatively affect the passenger's screening experience. ETD screening—from swab to test results—takes approximately 20–30 seconds. The mid-point of this range (25 seconds) would slow passenger throughput levels below the current rate of 150 passengers per hour per lane, thereby possibly increasing passenger wait times and the associated opportunity cost. Third, while mechanical issues with ETDs are rare, throughput depends on the reliability and mechanical consistency of these machines. Additionally, alarms can and do occur from some innocuous products that may contain trace amounts of chemicals found in explosive materials, which may also impede throughput until the alarm is resolved. Finally, this alternative requires an increase in ETD consumables, including swabs and gloves. This imposes costs to keep sufficient amounts of these consumables in stock at all airports where TSA conducts screening. The logistical concerns of implementing this alternative, in addition to the limited capability of ETD screening to detect other non-explosive threats, are the reasons TSA rejected this alternative in favor of deploying AIT to mitigate the threat to aviation security posed by both metallic and nonmetallic weapons and explosives.

Some of the other alternatives discussed in the comments, such as explosives detection canine and behavior detection screening, are not as effective as AIT in screening a large volume of passengers in the least amount of time and require additional costs; however, TSA does use such alternatives whenever available as added layers of security at the airport.

HH. Comparative Analysis Between AIT and Alternatives

Comments: Many submissions addressed the adequacy of TSA's comparative analysis between AIT and the alternatives. Several commenters suggested that TSA did not provide an adequate justification for AIT relative to the alternatives. For example, a commenter stated that AIT is approximately 10 times more expensive than magnetometers, but that the analysis does not evaluate the costs and benefits of AIT against magnetometers. Another commenter recommended that TSA quantitatively compare the benefits of AIT to the baseline condition (*e.g.,* by how much does AIT reduce the probability of a successful terrorist attack). A privacy advocacy group suggested that TSA does not adequately characterize AIT's effectiveness in comparison to the alternatives. The commenter also stated that the analysis does not support TSA's conclusions that AIT is more effective than the alternatives, and does not identify AIT's weaknesses relative to the alternatives. This privacy advocacy group and a non-profit organization both suggested that the analysis does not adequately compare the effectiveness of AIT to Regulatory Alternative 3. As a result, TSA does not acknowledge that WTMD and ETD can be just as effective as AIT, and in terms of shortcomings, ETD and AIT share some of the same disadvantages. An advocacy group suggested that the NPRM describes the proposed alternatives in ''all or nothing'' terms, rather than proposing a layered approach using a variety of the screening methods described in the alternatives.

A few commenters made other recommendations to TSA with regard to alternatives. For example, an individual commenter urged TSA to conduct research on alternative screening technology, provide educational outreach on the security measures to the public, and train flight attendants and inform passengers of what to do in response to suspicious activity. A commenter recommended using AIT as a secondary screening method on a more limited basis. Another individual commenter asked why TSA does not require travelers to go through both AIT and WTMD. The commenter suggested that travelers should be subjected to both technologies.

TSA Response: Chapters 3 in both the NPRM and final rule RIA list the advantages and disadvantages of each alternative and explain the basis for TSA's finding that none of the alternatives was preferable to AIT in addressing the threat of nonmetallic explosives concealed under clothing. For example, WTMDs (Alternative 1) and ETDs (Alternative 3) are not as effective as AIT in detecting non-metallic anomalies. Pat-downs (Alternative 2) may be effective at detecting nonmetallic weapons but would place a greater burden on passengers as they are more physically intrusive and would increase wait times at the checkpoint.

TSA does not use an ''all or nothing'' approach, as alleged in a comment. TSA uses a number of security measures to prevent attacks on commercial air travel. AIT is another security measure included in the multiple layers of security currently deployed. WTMDs, ETDs, and pat-downs are also used for screening. TSA reviewed these alternatives with respect to risk reduction, cost, impact on passengers and operational feasibility and determined that AIT is the best technology currently available to detect metallic and nonmetallic threats concealed under clothing.

II. Other Comments on the Regulatory Impact Analysis

Comments: Many commenters cited existing research on the costs and benefits of AIT, or recommended new research on the costs and benefits of AIT. Individual commenters and an advocacy group recommended that TSA conduct a study of the various impacts of AIT, including privacy impacts. Another commenter referred to an analysis of AIT, which, according to the commenter, found that AIT would need to prevent two or three terrorist attacks comparable to the September 11, 2001, attacks each year in order to be cost effective. An individual commenter cited a cost-benefit analysis conducted by the Journal of Homeland Security and Emergency Management and questioned the cost-effectiveness of AIT. An advocacy group concluded that independent, scholarly risk management and cost-benefit analyses of AIT have been conducted. According to the commenter, these studies have found that AIT scanners do not reduce risk sufficient to justify the costs. Another advocacy group suggested that a cost-benefit analysis of AIT would identify how effective the scanners are at deterring terrorism compared to screening alternatives. Another commenter requested that an independent party analyze the costs compared to other possible investments, such as traffic safety or cancer research.

Several commenters declared that the cost-benefit analysis in the NPRM is insufficient and inadequate and referred to AIT as costly. The commenters suggested that the analysis does not justify the cost relative to the risks or improvement in TSA's ability to detect threats to safe air travel. A privacy advocacy group stated that TSA did not fully evaluate the costs and benefits of AIT as compared to WTMDs and ETDs, as required under Executive Orders (E.O.s) 13563 and 12866. An individual commenter urged TSA to account for all of the risks associated with AIT and include difficult-to-quantify costs in the analysis. A non-profit organization stated that despite their cost, AIT scanners are cost-beneficial in deterring aviation terrorism when compared to pat-downs.

TSA Response: TSA conducted a comprehensive cost-benefit analysis supported by the best available data. TSA was unable to quantify a dollar value for the perceived loss of privacy. While TSA was unable to produce a quantitative impact of perceived privacy issues, TSA included a discussion of the measures it took to mitigate the privacy concerns of AIT (Chapter 2 in both the NPRM and final rule RIA). In addition, Federal law requires all AIT to be equipped with and deploy ATR software, which does not produce an individual image, but instead displays a generic outline. TSA reviewed other cost-benefit analyses on AIT, including the ones cited by commenters, to inform its own cost-benefit analysis. TSA has included a break-even analysis in this final rule, which answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?'' and provides a qualitative assessment of the benefits of AIT. Low probability, high consequence events such as terrorist attacks are difficult to measure with any level of certainty. TSA analyzed threats to the aviation sector and found that the use of AIT reduces the risk of metallic and nonmetallic threats as described in the RIA. The RIA also qualitatively described some of the indirect impacts from a successful attack on commercial air travel (Chapter 2, page 98 in the NPRM RIA and Chapter 4 in the final rule RIA). TSA included a full RIA in the docket folder.

JJ. Initial Regulatory Flexibility Analysis

Comments: Individual commenters and an advocacy group commented on TSA's Initial Regulatory Flexibility Analysis (IRFA). A couple of commenters recommended that the analysis estimate the costs incurred by small business entities, such as sole proprietors. The commenters stated that the impacts on small entities would include time lost as well as lost revenue from tourists (*e.g.,* fewer air travelers, both foreign and domestic). An advocacy group urged TSA to withdraw the NPRM, prepare an RFA analysis that accounts for the impacts on small entities, and provide another opportunity for comment. The commenter suggested that the NPRM erroneously excludes individuals from the definition of ''small entities.'' The commenter stated that many individual travelers are self-employed individuals and sole proprietors that qualify as small entities. The commenter estimated that the impact on ''small entities'' is at least $2.8 billion per year.

TSA Response: Individuals are not considered ''small entities'' based on the definitions in the Regulatory Flexibility Act (5 U.S.C. 601) and therefore were not considered in our IRFA. The definition of ''small entities'' in the RFA comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. The RFA does not state the definition of ''small entities'' extends to ''individuals.'' TSA does agree as a general matter that a sole proprietor could be a small business if the individual is acting as a business, potentially generating revenues and incurring business costs. Nevertheless, TSA considered individuals in Chapter 6 of the RIA and determined that the main impact on a person traveling would be the extended wait time if that person opts out of AIT screening and undergoes a pat-down. As stated in both the NPRM and final rule RIA, AIT does not increase wait time for the general traveling public. TSA measured the ratio of individuals who opt-out of AIT to be approximately one percent of the total volume of passengers screened. Additionally, the pat-down for individuals who opt-out is estimated to be 150 additional seconds per screening and would not reflect a significant opportunity cost impact ($1.88 per screening).

KK. Other Regulatory Analyses

Comments: A few individual commenters suggested that TSA should have performed an Unfunded Mandates Reform Act (UMRA) analysis. A commenter stated that the proposed rule would affect State, local, and tribal governments because of the increased road traffic caused by the rule (*i.e.,* travelers substituting motor vehicle travel for air travel). The commenter explained that TSA failed to account for costs associated with State, local, and tribal governments responding to additional motor vehicle accidents and providing additional road maintenance. Another commenter stated that the costs of the rule would be passed onto passengers in the form of the September 11th Security Fee, which would be a burden triggering an analysis under the Unfunded Mandates Reform Act.

A non-profit organization and an individual commenter suggested that the proposed rule would have a substantial direct effect on States under E.O. 13132, Federalism. Both commenters discussed the experience of Texas, which attempted to pass an anti-groping law that would have affected TSA's screening process. According to the commenters, news reports stated that TSA sent the Texas legislature a letter threatening to close all Texas airports if the bill passed. The commenters suggested that TSA's interference with a State legislature's activity demonstrates the substantial direct effect AIT would have on States. A commenter also explained that States are responsible for inspecting radiological devices and licensing unit operators. As a result, the commenter suggested that the rule would require State governments to inspect the AIT units and license operators of AIT units, which would have a direct effect on States.

Two individual commenters stated that TSA must prepare an environmental impact statement in accordance with National Environmental Protection Act (NEPA). One of the commenters urged TSA to assess the human health impacts associated with AIT. The other commenter explained that the environmental impact statement would need to assess the impact of increased motor vehicle travel (*e.g.,* air pollution, traffic, and car accidents) on the environment.

TSA Response: TSA disagrees with comments regarding the UMRA. TSA determined that an UMRA analysis is not needed for the AIT NPRM as such an analysis is required if a proposed rulemaking ''results in the expenditure by State, local, and tribal governments, in the aggregate, or by the private sector, of $100,000,000 or more (adjusted annually for inflation) in any 1 year.'' As described in the RIA, 98 percent of the cost of AIT falls on the Federal Government. The remaining costs fall on airports who do not receive reimbursement for their utilities. These entities have an estimated utilities cost of $1.63 million (Chapter 2, of the final rule RIA). In addition, the Passenger Civil Aviation Security Service fee is set in statute and in TSA's regulations. *See* 49 U.S.C. 44940 and 49 CFR 1510.5. TSA did not propose to increase the fee in the NPRM.

TSA disagrees with comments claiming that deployment of AIT has a federalism impact. Federal law requires that screening be carried out by a Federal Government employee. 49 U.S.C. 44901(a). Prior to the creation of TSA, passenger screening was the responsibility of air carriers pursuant to regulations issued by FAA. Passenger screening is not conducted by State employees, and the final rule does not have a substantial direct effect on the states, the relationship between the Federal Government and the states, or on the distribution of power among the various levels of government. As to the proposed state legislation referred to by some commenters, note that Congress by statute made TSA responsible for passenger screening. 49 U.S.C. 114 and 44901. This AIT rulemaking does not alter that relationship.

Finally, an environmental impact statement under NEPA is not required. There is no evidence that use of AIT to screen passengers will have a non-negligible impact on motor vehicle travel. In addition, independent studies have confirmed that the exposure to non-ionizing electromagnetic waves from the millimeter wave AIT machines is below the limits allowed under relevant national health and safety standards and cause no known adverse health effects.

LL. Comments on the Risk Analysis

Comments: Many commenters addressed the issue of risk, risk management, and risk-reduction analysis. Some commenters suggested that the risks AIT is meant to mitigate do not justify the costs associated with AIT. One commenter stated that over the past 12 years, AIT scanners would not have prevented enough attacks to justify the costs (*i.e.,* only two bombings in the past 12 years and a cost of $3.6 billion). A non-profit commenter, an advocacy group, and an individual commenter all referenced a recent study to explain that the existing risk of a terrorist attack on an airliner does not justify the costs of AIT.

Another set of commenters urged TSA to provide a detailed risk reduction analysis to support the rulemaking, such as the classified version that TSA cited in the NPRM. The commenters suggested that TSA at least release a redacted version or a summary of its risk-reduction analysis of AIT. A non-profit organization stated that TSA is obligated to disclose whether AIT would be cost-effective in reducing this risk. The commenter cited another risk-reduction analysis that was published by academic researchers in a peer-reviewed journal to indicate that these analyses can be published without revealing technical details or threat information that may legitimately be kept confidential.

An individual commenter recommended that TSA design the AIT rule so that the agency would be able to conduct a ''look back'' analysis after the rule is implemented. The commenter explained that TSA would be able to collect empirical data on impacts such as AIT's effectiveness of detecting various security threats, and the amount of time added to the security screening process. Another individual commenter referenced the report and suggested that TSA analyze the cost and benefits of AIT in the areas of personal privacy, freedom, and convenience.

TSA Response: TSA uses internal information on screening capability, effectiveness, feasibility of airport screening, and costs to determine the implementation of security technology and procedures. Because of the sensitive nature of information on screening standard operating procedures, this information and any corresponding policy decisions remain classified and unavailable to the public. TSA included a break-even analysis in the final rule RIA that answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?'' This methodology is used in peer-reviewed journals and recommended by OMB Circular A–4 when benefits are difficult to quantify. In addition, given that TSA piloted and deployed AIT in 2007 and 2008, TSA has already conducted ''look-back'' analysis and has implemented program changes based on optimal risk-reduction.

MM. Other Comments on the NPRM

Comments: Some individual commenters made statements that because air travel is not as dangerous as other modes of transportation, resources should be directed to other transportation safety and high-profile events. Individual commenters suggested that the use of AIT might become common in other venues where security searches occur including courthouses, schools, stadiums, political rallies, and other places. An individual commenter stated that since TSA staff does not follow the ''liquid policy,'' it should be eliminated for travelers. According to the same commenter, the ''shoe policy'' could also be eliminated because shoes can be screened with WTMDs. A community organization provided a list of goals for airport security.

Some individual commenters stated that TSA staff is not trained in screening techniques or on how to behave professionally. A few individual commenters suggested that TSA create a process to hold TSA employees accountable for their actions. Individual commenters recommended that employees wear badges with contact information, such as their full name and badge number. A commenter also recommended that TSA place employees on probation for receiving three or more customer service reports within 6 months. Another individual commenter suggested that TSA publicize any existing processes for anonymous reporting. A few individual commenters expressed concern and provided information regarding the reported off-duty criminal activities of TSA screeners. Several commenters stated generally that the security at airports has not increased the safety of air travel.

TSA Response: The information TSA receives from intelligence-gathering agencies confirms that civil aviation remains a favored target for extremists and terror organizations. However, TSA has authority over all modes of transportation. With respect to maritime and surface transportation, TSA has always applied a risk-based approach to safeguard the movement of people and commerce. Such an approach provides flexibility to adjust to changing travel patterns and the ever-shifting threat environment. TSA conducts Visible Intermodal Prevention and Response operations across the country to prevent or disrupt potential terrorist planning activities. In addition, TSA often works with other Federal, State, and local government agencies to enhance security during special events, such as the Super Bowl and presidential inaugurations.

TSA is continually updating and enhancing the training of its TSOs to improve effectiveness and to reinforce that screening be conducted in a professional and courteous manner. TSA investigates all allegations of misconduct and takes appropriate action, which can include referral to law enforcement and termination of employment. TSOs wear identification badges. TSA's Web site, at *www.tsa.gov/contact-us,* provides information on various ways to contact TSA to ask questions and provide feedback. The TSA Contact Center is open seven days a week, and individuals may call 1–800–289–9673 or email at *TSA-ContactCenter@dhs.gov.* There is a direct link to an on-line form that travelers may fill out and submit.

TSA believes that its layers of security have vastly improved the security posture of the Nation's transportation systems. A terrorist has to overcome multiple security measures in order to carry out an attack and is more likely to be pre-empted, deterred, or fail during the attempt.

III. Rulemaking Analyses and Notices

A. International Compatibility

In keeping with U.S. obligations under the Convention on International Civil Aviation, it is TSA policy to comply with ICAO Standards and Recommended Practices to the maximum extent practicable. TSA determined that there are no ICAO Standards and Recommended Practices that correspond to this regulation.

B. Economic Impact Analyses

1. Regulatory Impact Analysis Summary

Changes to Federal regulations must undergo several economic analyses. First, E.O. 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), as supplemented by E.O. 13563, Improving Regulation and Regulatory Review (76 FR 3821, January 21, 2011), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to analyze the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. 2531–2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

In conducting these analyses, TSA has determined:

1. This rule is a significant regulatory action that is economically significant under sec. 3(f)(1) of E.O. 12866. Accordingly, the OMB has reviewed this regulation.
2. A Final Regulatory Flexibility Analysis suggests this rulemaking would not have a significant economic impact on a substantial number of small entities.
3. This rulemaking would not constitute a barrier to international trade.
4. This rulemaking does not impose an unfunded mandate on State, local, or tribal governments, or on the private sector.

These analyses, available in the docket, are summarized below.

2. Executive Orders 12866 and 13563 Assessment

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility.

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this RIA, TSA uses a 10-year period of analysis to align with the 10-year AIT life cycle from deployment to disposal.[126] TSA has revised the NPRM RIA assumption of an 8-year life cycle for AIT units to 10 years based on a recent LCCE report[127] from the OSC, which evaluated the performance metrics, and maintenance data from AIT units at airports. AIT deployment began in 2008, and TSA, therefore, includes costs that have already been borne by TSA, the traveling public, industry, and airports. Consequently, the RIA takes into account costs that have already occurred—in years 2008–2014—in addition to the projected costs in years 2015–2017. By reporting the costs that have already happened and estimating future costs in this manner, TSA accounts for the full life-cycle of AIT machines.

TSA presents AIT costs in tables 2 through 4. Table 2 reports the total costs from 2008–2014 to be $1,439.32 million (undiscounted).

TABLE 2—COST SUMMARY FROM 2008–2014 BY COST COMPONENT

[In $millions, undiscounted]

Year	Passenger opportunity costs	Airport utilities costs	TSA costs				Industry costs backscatter removal	Total
			Personnel	Training	Equipment	Utilities		
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	0.02	0.01	12.05	0.57	28.01	0.02	0.00	40.69
2010	0.42	0.13	57.20	33.64	118.66	0.23	0.00	210.28
2011	3.17	0.15	201.83	57.06	76.86	0.26	0.00	339.33
2012	5.28	0.28	219.75	23.31	101.59	0.37	0.00	350.58
2013	4.45	0.25	197.77	14.37	46.70	0.34	1.90	265.79
2014	3.05	0.18	131.22	12.21	41.28	0.37	0.00	188.31
Total	16.40	1.02	830.09	141.16	447.14	1.61	1.90	1,439.32

Note: Totals may not sum exactly due to rounding.

Table 3 reports total costs for projected years 2015–2017 to be $706.99 million (undiscounted), $666.47 million discounted at three percent, and $618.18 million discounted at seven percent.

[126] In the NPRM RIA, the AIT life cycle was estimated to be eight years. Therefore, the period of analysis for the RIA was also eight years.

[127] TSA's Office of Security Capabilities (OSC), ''Life Cycle Cost Estimate for Passenger Screening Program'' March 10, 2014. Lifecycle revisions are based on recent a useful life study for each type of transportation security equipment. These are TSA internal sensitive information reports based on OSC technology assessments.

TABLE 3—COSTS SUMMARY FROM 2015–2017 BY COST COMPONENT
[In $millions]

Year	Passenger opportunity costs	Airport utilities costs	TSA costs				Total
			Personnel	Training	Equipment	Utilities	
2015	$4.12	$0.20	$141.96	$41.25	$49.75	$0.40	$237.68
2016	4.20	0.20	141.96	54.89	25.06	0.40	226.72
2017	4.28	0.20	141.96	69.30	26.45	0.41	242.60
Total	12.59	0.61	425.89	165.45	101.25	1.20	706.99
Total (Discounted at 3%)	11.87	0.57	401.55	155.22	96.12	1.13	666.47
Total (Discounted at 7%)	11.01	0.53	372.55	143.07	89.97	1.05	618.18

Note: Totals may not sum exactly due to rounding.

Table 4 reports total costs for years 2008–2017 to be $2,146.31 million (undiscounted). During 2008–2017, TSA estimates that personnel and equipment life cycle costs are the largest categories of expenditures.

TABLE 4—TOTAL COST SUMMARY FROM 2008–2017 BY COST COMPONENT
[In $millions, undiscounted]

Year	Passenger opportunity costs	Airport utilities costs	TSA costs				Industry costs backscatter removal	Total
			Personnel	Training	Equipment	Utilities		
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	0.02	0.01	12.05	0.57	28.01	0.02	0.00	40.69
2010	0.42	0.13	57.20	33.64	118.66	0.23	0.00	210.28
2011	3.17	0.15	201.83	57.06	76.86	0.26	0.00	339.33
2012	5.28	0.28	219.75	23.31	101.59	0.37	0.00	350.58
2013	4.45	0.25	197.77	14.37	46.70	0.34	1.90	265.79
2014	3.05	0.18	131.22	12.21	41.28	0.37	0.00	188.31
2015*	4.12	0.20	141.96	41.25	49.75	0.40	0.00	237.68
2016*	4.20	0.20	141.96	54.89	25.06	0.40	0.00	226.72
2017*	4.28	0.20	141.96	69.30	26.45	0.41	0.00	242.60
Total	28.99	1.63	1,255.98	306.61	548.39	2.81	1.90	2,146.31

Note: Totals may not sum exactly due to rounding.

Implementing AIT into the passenger screening program is beneficial because it enhances commercial aviation security. AIT improves security by assisting TSA in the detection of non-metallic, as well as metallic, explosives concealed under the clothing of passengers. Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities (see the Background section in this preamble). The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. The examples presented below highlight the increased real world threats of non-metallic explosives to commercial aviation:

- On December 22, 2001, on board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.
- On December 25, 2009, a bombing plot by AQAP culminated in Umar Farouk Abdulmutallab's attempt to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In May 2012, AQAP developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

The deployment of AIT generates benefits that come from reducing security risks through AIT, which is capable of detecting both metallic and non-metallic weapons and explosives.[128] Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives. AIT is a proven technology based on laboratory testing and field experience and is an essential component of TSA's security screening because it provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger.

TSA uses a break-even analysis to frame the relationship between the potential benefits of the rulemaking and the costs of implementing the rule. When it is not possible to quantify or monetize a majority of the incremental benefits of a regulation, OMB recommends conducting a threshold, or ''break-even'' analysis. According to OMB Circular No. A–4, ''Regulatory Analysis,'' such an analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the nonquantified costs need to be) before the rule would yield zero net benefits?'' [129] In the break-even analysis, TSA compared the annualized cost for the deployment of AIT to the major

[128] Metal detectors and AITs are both designed to detect metallic threats on passengers, but go about it in different ways. Metal detectors rely on the inductance that is generated by the metal, while AIT relies on the metal's reflectivity properties to indicate an anomaly. AIT capabilities exceed metal detectors because it can detect metallic/non-metallic weapons, non-metallic bulk explosives and non-metallic liquid explosives.

[129] *http://www.whitehouse.gov/omb/circulars_a004_a-4/.*

direct benefits of preventing several potential terrorist attack scenarios.

TSA used five types of aircrafts to represent five different scenarios where an attacker detonates a body-bomb on a domestic passenger aircraft, the type of attack AIT is meant to mitigate. The five types of aircraft fall into two assigned categories: High-capacity, long range aircraft typically used for international travel; and medium-capacity and long-range aircraft typically used for cross-country travel or popular routes. TSA used the Bureau of Transportation Statistics' T–100 [130] data bank from 2014 to determine the most popular aircraft models for the two categories of aircrafts.[131] [132] TSA also used the T–100 from 2014 to determine the average load factor for each aircraft type.[133] These aircrafts were used in the break-even analysis and are listed below along with their specifications:

High Capacity

- Airbus A380–Airbus' long-range aircraft with a 544 seat capacity [134] and an average crew size of 13 (557 occupancy total) [135] with a market value of $428.0 million.[136]
- Boeing 777–200LR–Boeing's long-range aircraft with 317 seat capacity [137] and an average crew size of 9 (323 occupancy total) [138] and a market value of $305.0 million.[139]

Medium Capacity

- Boeing 737–700–A medium-range aircraft with a seating capacity range between 126 and 149 (median of 138 used to represent passengers and crew) [140] and a market value of $78.3 million.[141]
- Boeing 737–800–A medium-range aircraft with a seating capacity range between 162 and 189 (median of 176 used to represent passengers and crew) [142] and a market value of $93.3 million.[143]
- Airbus A320–100/200–A medium-range aircraft with a 150 seat capacity [144] and crew size of 6 (156 occupancy total) [145] and a market value of $97.0 million.[146]

To conduct the break-even analysis, TSA estimated the major direct costs for these attack scenarios, which can be viewed as the benefits of avoiding an attack. The break-even analysis does not include the macroeconomic impacts that could occur due to a major attack. In addition to the direct impacts of a terrorist attack in terms of lost life and property, there are other more indirect impacts, particularly on aviation based terrorist attacks that are difficult to measure. As noted by Cass Sunstein in the Laws of Fear, ''. . . fear is a real social cost, and it is likely to lead to other social costs. If, for example, people are afraid to fly, the economy will suffer in multiple ways . . . .'' [147] Given the lack of information to quantify these more intangible, but real economic impacts of a terrorist attack, the full benefits of AIT screening are underestimated in this break-even analysis.

TSA assumed all the passengers and crew are killed in each scenario and used the value of statistical life (VSL) of $9.1 million per fatality as adopted by the U.S. Department of Transportation (DOT) [148] to monetize the consequences from fatalities. TSA emphasizes that the VSL is a statistical value used here only for regulatory comparison and does not suggest that the actual value of a life can be stated in dollar terms.

The replacement cost of the aircraft and emergency response costs [149] [150] are added to the loss of life to sum up the total cost of each attack scenario. TSA then calculates the ratio between the estimated cost of a successful attack and the annualized cost of AIT using a seven percent discount rate.[151] By generating a ratio between these costs, TSA estimates how small the value of non-quantified benefits would need to be for the rule to yield zero positive benefits. Table 5 presents the number of attacks averted (expressed as a number of years between attacks) that would be required to break even for all five attack scenarios.

---

[130] U.S. Department of Transportation, Bureau of Transportation Statistics, ''T–100 Data bank.'' *http://www.transtats.bts.gov/DatabaseInfo.asp?DB_ID=111.*

[131] U.S. Department of Transportation, Bureau of Transportation Statistics, ''T–100 Domestic Segment (All carriers) Data bank,'' *http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air.* Selected fields: DepPerformed, Aircraft Type, and Year = 2014, All months.

[132] Boeing 737–700/700LR, Boeing 737–800, and Airbus A320–100/200 are the first-, fourth-, and fifth-most often-used aircrafts in 2014, respectively.

[133] U.S. Department of Transportation, Bureau of Transportation Statistics, ''T–100 Domestic Segment (All carriers) Data bank,'' *http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air.* Selected fields: Seats, Passengers, Aircraft Type, and Year = 2014, All months.

[134] Airbus.com, ''A380 Dimensions & Key Data.'' Accessed Aug. 12, 2015. *http://www.airbus.com/aircraftfamilies/passengeraircraft/a380family/specifications/.*

[135] Estimated thirteen crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and ten flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391, which state there must be at least one flight attendant per 50 passenger seats.

[136] Airbus.com, ''New Airbus aircraft list prices for 2015,'' *http://www.airbus.com/newsevents/news-events-single/detail/new-airbus-aircraft-list-prices-for-2015/.*

[137] Boeing.com, ''777–200/–200ER Technical Characteristics.'' Accessed Aug. 12, 2015. *http://www.boeing.com/boeing/commercial/777family/pf/pf_200product.page.*

[138] Estimated nine crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and six flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391, which state there must be at least one flight attendant per 50 passenger seats.

[139] Boeing.com, ''Commercial Airplanes Jet Prices, 2014 price,'' *http://www.boeing.com/boeing/commercial/prices/.*

[140] Boeing.com, ''737–700 Technical Characteristics.'' Accessed Aug. 12, 2015. *http://www.boeing.com/boeing/commercial/737family/pf/pf_700tech.page.*

[141] Boeing.com, ''Commercial Airplanes Jet Prices, 2014 price,'' *http://www.boeing.com/boeing/commercial/prices/.*

[142] Boeing.com, ''737–800 Technical Characteristics.'' Accessed Aug. 12, 2015. *http://www.boeing.com/boeing/commercial/737family/pf/pf_800tech.page*?

[143] Boeing.com, ''Commercial Airplanes Jet Prices, in 2014 price,'' *http://www.boeing.com/boeing/commercial/prices/.*

[144] Airbus.com, ''A320 Setting single aisle standards, Dimensions & Key Data.'' Accessed August 12, 2015. *http://www.airbus.com/aircraftfamilies/passengeraircraft/a320family/a320/specifications/.*

[145] Estimated six crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and three flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391, which state there must be at least one flight attendant per 50 passenger seats.

[146] Airbus.com, ''New Airbus aircraft list prices for 2015,'' *http://www.airbus.com/newsevents/news-events-single/detail/new-airbus-aircraft-list-prices-for-2015/.*

[147] Cass R. Sunstein, ''Laws of Fear,'' p. 127, 2005.

[148] U.S. Department of Transportation, ''Guidance on Treatment of Economic Value of a Statistical Life in U.S. Department of Transportation Analyses,'' *http://www.dot.gov/sites/dot.dev/files/docs/VSL%20Guidance%202013.pdf.*

[149] TSA uses a proxy estimate of $869,552 (inflated from $800,000 in 2009 dollars) from a lawsuit filed by The County of Erie, New York to recuperate emergency response costs from Colgan Air, Inc., in response to the Colgan Air Flight 3407 crash. *These costs include overtime, removal of human remains, cleanup of the aircraft and chemical substances, counseling for the surviving family members, and acquiring special equipment.*

[150] McGrory, Michael, ''Airlines Not Liable for Colgan Air Crash Clean-Up Costs; SmithAmunden Aerospace Report,'' March 20, 2013, *http://www.salawus.com/insights-alerts-70.html.*

[151] TSA estimates the annualized net cost of AIT deployment to be $204.57 million using a seven percent discount rate.

TABLE 5—FREQUENCY OF ATTACKS AVERTED TO BREAK-EVEN

[In $millions]

Aircrafts	Replacement and emergency response costs a	Total passengers + crew b	Load factor (%) c	Total consequence d = a + (b × c × VSL)	Attacks averted by AIT to break-even: total consequence/$204.57M e = d ÷ $204.57M
High Capacity:					
Airbus A380	$428.9	557	86	$4,811	1 attack per 23.52 yrs.
Boeing 777–200	305.9	326	84	2,791	1 attack per 13.64 yrs.
Medium Capacity:					
Boeing 737–700/700LR	79.2	138	80	1,075	1 attack per 5.25 yrs.
Boeing 737–800	94.2	176	84	1,434	1 attack per 7.01 yrs.
Airbus Industries A320–100/200	97.9	156	85	1,305	1 attack per 6.38 yrs.

In Table 6 and Table 7, TSA presents annualized cost estimates and quantitative benefits of AIT deployment and operation. In Table 6, TSA shows the annualized net cost of AIT from 2015 to 2017. As previously explained, costs incurred from 2008–2014 occurred in the past. However, given that the life cycle of the AIT technology considered in this analysis is 10 years, TSA has also added Table 7 showing the annualized net cost of AIT from 2008–2017.

TABLE 6—OMB A–4 ACCOUNTING STATEMENT FOR 2015–2017

[In $millions]

Category	Primary estimate		Minimum estimate	Maximum estimate	Source citation (final RIA, preamble, etc.)
BENEFITS					
Annualized monetized benefits (discount rate in parentheses)	(7%)	N/A			Final RIA.
	(3%)	N/A			Final RIA.
Unquantified benefits	The operations described in this rule produce benefits by reducing security risks through the deployment of AIT that can detect non-metallic weapons and explosives.				Final RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$235.56			Final RIA.
	(3%)	$235.62			Final RIA.
Annualized quantified, but unmonetized, costs	0		0	0	Final RIA.
Qualitative costs (unquantified)	N/A				Final RIA.
TRANSFERS					
Annualized monetized transfers: "on budget"	0		0	0	Final RIA.
From whom to whom?	N/A		N/A	N/A	None.
Annualized monetized transfers: "off-budget"	0		0	0	Final RIA.
From whom to whom?	N/A		N/A	N/A	None.
Miscellaneous analyses/category	**Effects**				**Source citation (final RIA, preamble, etc.)**
Effects on state, local, and/or tribal governments	None				Final RIA.
Effects on small businesses	No significant economic impact. Prepared FRFA.				FRFA.
Effects on wages	None				None.
Effects on growth	None				None.

TABLE 7—OMB A–4 ACCOUNTING STATEMENT FOR 2008–2017

[$millions]

Category	Primary estimate		Minimum estimate	Maximum estimate	Source citation (final RIA, preamble, etc.)
BENEFITS					
Annualized monetized benefits (discount rate in parentheses)	(7%)	N/A	....	....	Final RIA.
	(3%)	N/A	....	....	Final RIA.
Unquantified benefits	The operations described in this rule produce benefits by reducing security risks through the deployment of AIT that can detect non-metallic weapons and explosives.				Final RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$204.57	....	....	Final RIA.
	(3%)	$210.47	....	....	Final RIA.
Annualized quantified, but unmonetized, costs	0		0	0	Final RIA.
Qualitative costs (unquantified)	N/A				Final RIA.
TRANSFERS					
Annualized monetized transfers: "on budget"	0		0	0	Final RIA.
From whom to whom?	N/A		N/A	N/A	None.
Annualized monetized transfers: "off-budget"	0		0	0	Final RIA.
From whom to whom?	N/A		N/A	N/A	None.

Miscellaneous analyses/category	Effects	Source citation (final RIA, preamble, etc.)
Effects on state, local, and/or tribal governments	None	Final RIA.
Effects on small businesses	No significant economic impact. Prepared FRFA.	FRFA.
Effects on wages	None	None.
Effects on growth	None	None.

As alternatives to the preferred regulatory proposal presented in the NPRM and final rule, TSA examined three other options. The following table briefly describes these options, which include use of WTMD only (no action), increased use of physical pat-down searches that supplements primary screening with WTMDs, and increased use of ETD screening that supplements primary screening with WTMDs. These alternatives, and the reasons why TSA rejected them in favor of the rule, are discussed in detail in Chapter 3 of the regulatory impact analysis located in this docket and summarized in Table 8.

TABLE 8—ADVANTAGES AND DISADVANTAGES OF REGULATORY ALTERNATIVES

Regulatory alternative	Name	Description	Advantages	Disadvantages
1	WTMDs Only	The passenger screening environment remains unchanged. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.	• No additional cost burden • No additional perceived privacy concerns.	• Fails to meet the January 7, 2010 Presidential Memorandum and statutory requirement in 49 USC 44925.[152] • Does not mitigate the non-metallic threat to aviation security.
2	Pat-Down	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by with a pat-down on a randomly selected portion of passengers.	• Thorough physical inspection of metallic and non-metallic items. • Uses currently deployed WTMD technology. • Minimal technology acquisition costs.	• Employs a substantial amount of human resources. • Increase in number of passengers subject to a pat-down. • Increased wait times.

[152] *http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack.*

TABLE 8—ADVANTAGES AND DISADVANTAGES OF REGULATORY ALTERNATIVES—Continued

Regulatory alternative	Name	Description	Advantages	Disadvantages
3	ETD Screening	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses the threat of non-metallic explosive threats.	• Does not detect non-explosive non-metallic potential threats. • Increased wait times and associated passenger opportunity cost of time. • Increase in ETD consumable costs.
4	AIT as Secondary Screening.	TSA continues to use WTMDs as the primary screening technology. TSA supplements the WTMD screening by conducting AIT screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses non-metallic explosive threats.	• Primary screening does not detect non-metallic weapons or explosives. • Incremental cost of acquisition of AIT.
5	AIT	TSA uses AIT as a passenger screening technology. Alarms resolved through a pat-down.	• Addresses the threat of non-metallic explosives hidden on the body by safely screening passengers for metallic and non-metallic threats. • Maintains lower personnel cost and higher throughput rates than the other alternatives. • Adds deterrence value—the effect of would be attackers becoming discouraged as a result of AIT.	• Incremental cost of acquisition to TSA. • Incremental personnel cost to TSA. • Incremental training cost to TSA.

3. Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act (RFA) of 1980 requires agencies to consider the impacts of their rules on small entities. Under the RFA, the term ''small entities'' comprises small businesses, not-for-profit organizations that are independently owned and operated and are not dominant in their fields, and governmental jurisdictions with populations of less than 50,000. Individuals and States are not considered ''small entities'' based on the definitions in the RFA (5 U.S.C. 601).

This final rule codifies the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. The only additional direct cost small entities incur due to this rule is for utilities, because of increased power consumption from AIT operation. TSA identified 106 small entities (105 small governmental jurisdictions and one small privately-owned airport) based on the Small Business Administration size standards that potentially incur additional utilities costs due to AIT. Of the 106 small entities, seven currently have AITs deployed and are not reimbursed by TSA for the payment of utilities. Consequently, AIT causes seven small entities, or 1.5 percent (7/460) of all airports, to incur additional direct costs during the period of analysis.

These entities incur an incremental cost for utilities from an increased consumption of electricity from AIT operation. To estimate these costs, TSA uses the average kilowatts (kW) consumed per AIT unit on an annual basis. Depending on the size of the airport, TSA estimates the average additional utilities costs to range from $290 to $921 per year while the average annual revenue for these small entities ranges from $8.4 million to $213.3 million per year.[153] TSA estimates that the cost impact of AIT to affected small entities is less than one percent of their annual revenue. Therefore, TSA's Final Regulatory Flexibility Analysis suggests that this rule would not have a significant economic impact on a substantial number of small entities under section 605(b) of the RFA.

4. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this rulemaking and has determined that it will have only a domestic impact and therefore no effect on any trade-sensitive activity.

5. Unfunded Mandates Assessment

The UMRA is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of the UMRA requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may result in a $100 million or more expenditure (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector; such a mandate is deemed to be a ''significant regulatory action.''

This rulemaking does not contain such a mandate. The requirements of Title II of the UMRA, therefore, do not apply and TSA has not prepared a statement.

[153] TSA has changed the way that utilities costs were calculated from the NPRM in order to match the operating time of an AIT with its associated cost for additional utilities consumption. The change in the revenue range for small entities from the NPRM is due to the population of airports which has been adjusted to include all airports that are regulated under 49 CFR part 1542 since publication of the NPRM.

C. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501. *et seq.*) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA sec. 3507(d), obtain approval from the OMB for each collection of information it conducts, sponsors, or requires through regulations. The PRA defines a ''collection of information'' to be ''the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinion by or for an agency, regardless of form or format . . . imposed on ten or more persons.'' 44 U.S.C. 3502(3)(A). TSA did not receive any comments regarding the PRA. TSA has determined that there are no current or new information collection requirements associated with this rule. TSA's use of AIT to screen passengers does not constitute activity that would result in the collection of information as defined in the PRA.

As protection provided by the PRA, as amended, an agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a currently valid OMB control number.

D. Executive Order 13132, Federalism

TSA has analyzed this rulemaking under the principles and criteria of E.O. 13132, Federalism. TSA determined that this action will not have a substantial direct effect on the States, or the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government, and, therefore, does not have federalism implications.

E. Environmental Analysis

TSA has reviewed this rulemaking for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment. This action is covered by categorical exclusion (CATEX) number A3(b) and (d) in DHS Management Directive 023–01 (formerly Management Directive 5100.1), Environmental Planning Program, which guides TSA compliance with NEPA.

F. Energy Impact Analysis

The energy impact of this rulemaking has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 94–163, as amended (42 U.S.C. 6362). TSA has determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects in 49 CFR Part 1540

Air carriers, Aircraft, Airports, Civil Aviation Security, Law enforcement officers, Reporting and recordkeeping requirements, Screening, Security measures.

The Amendment

For the reasons set forth in the preamble, the Transportation Security Administration amends Chapter XII of Title 49, Code of Federal Regulations, as follows:

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

■ 1. Revise the authority citation for part 1540 to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44925, 44935–44936, 44942, 46105.

■ 2. In § 1540.107, add paragraph (d) to read as follows:

§ 1540.107 Submission to screening and inspection.

* * * * *

(d) The screening and inspection described in paragraph (a) of this section may include the use of advanced imaging technology. Advanced imaging technology used for the screening of passengers under this section must be equipped with and employ automatic target recognition software and any other requirement TSA deems necessary to address privacy considerations.

(1) For purposes of this section, advanced imaging technology–

(i) Means a device used in the screening of passengers that creates a visual image of an individual showing the surface of the skin and revealing other objects on the body; and

(ii) May include devices using backscatter x-rays or millimeter waves and devices referred to as whole body imaging technology or body scanning machines.

(2) For purposes of this section, automatic target recognition software means software installed on an advanced imaging technology device that produces a generic image of the individual being screened that is the same as the images produced for all other screened individuals.

Dated: February 23, 2016.

Peter V. Neffenger,

Administrator.

[FR Doc. 2016–04374 Filed 3–2–16; 8:45 am]

BILLING CODE 4910–52–P

Transportation Security Administration

Passenger Screening Using Advanced Imaging Technology

49 CFR Part 1540
Docket No. TSA-2013-0004
RIN 1652-AA67

Final Rule

Regulatory Impact Analysis and Final Regulatory Flexibility Analysis

February 18, 2016

Economic Analysis Branch
Office of Security Policy and Industry Engagement
Transportation Security Administration
Department of Homeland Security
Arlington, VA 20598

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

AIT	Advanced Imaging Technology
AQAP	Al Qaeda in the Arabian Peninsula
ATR	Automated Target Recognition
ATSA	Aviation and Transportation Security Act
BLS	Bureau of Labor Statistics
CAGR	Compound Annual Growth Rate
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DOT	Department of Transportation
EO	Executive Order
EPIC	Electronic Privacy Information Center
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FAT	Factory Acceptance Test
FDA	Food and Drug Administration
FRFA	Final Regulatory Flexibility Analysis
FTE	Full Time Equivalent
GDP	Gross Domestic Product
IED	Improvised Explosive Device
IID	Improvised Incendiary Device
IO	Image Operator
kW	kilowatts
LCCE	Life Cycle Cost Estimate

NAICS	North American Industry Classification System
NIST	National Institute for Standards and Technology
NPRM	Notice of Proposed Rulemaking
OMB	Office of Management and Budget
OTD	Office of Training and Development
OT&E	Operational Test & Evaluation
PMIS	Performance Management Information System
PMO	Program Management Office
PSP	Passenger Screening Program
QT&E	Qualification Test & Evaluation
RFA	Regulatory Flexibility Act
RIA	Regulatory Impact Analysis
SAT	Site Acceptance Test
SBA	Small Business Administration
SAM	Screener Allocation Model
SME	Subject Matter Expert
SO	System Operator
SSI	Sensitive Security Information
TSA	Transportation Security Administration
TSO	Transportation Security Officer
UMRA	Unfunded Mandates Reform Act
VSL	Value of a Statistical Life
WTMD	Walk Through Metal Detector

This page is intentionally left blank.

EXECUTIVE SUMMARY

Federal regulations must undergo several types of analyses, required by executive orders, acts, or statutes, before their publication. Executive Orders (EO) 13563[1] and 12866[2] direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits. EO 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. Under EO 12866, the Transportation Security Administration (TSA) must determine whether a regulatory action is significant[3] and therefore subject to the requirements of the EO and review by the Office of Management and Budget (OMB).

After conducting this Regulatory Impact Analysis (RIA), TSA determined that this final rule constitutes a "significant regulatory action" in accordance with the definition of economically significant under section 3(f) (1) of EO 12866. Accordingly, OMB reviewed this regulation.

The Regulatory Flexibility Act (RFA) of 1980 requires agencies to consider the economic impact of regulatory changes on small entities. The Trade Agreements Act[4] prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. In developing U.S. standards, this Act requires agencies to consider international standards and, where appropriate, to use them as the basis for U.S. standards. Finally, the Unfunded Mandates Reform Act of 1995[5] (UMRA) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

---

[1] http://www.reginfo.gov/public/jsp/Utilities/EO_13563.pdf
[2] http://www.reginfo.gov/public/jsp/Utilities/EO_12866.pdf
[3] Section 3(f) of the EO 12866 defines a "significant regulatory action" as any regulatory action that is likely to result in a rule that: (1) has an annual effect on the economy of $100 million or more, or adversely affects in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local or tribal governments or communities (also referred to as economically significant); (2) creates serious inconsistency or otherwise interferes with an action taken or planned by another agency; (3) materially alters the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raises novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the EO.
[4] 19 U.S.C. § 2531-2533
[5] Public Law 104-4

In conducting these analyses on the Passenger Screening Using Advanced Imaging Technology (AIT) Final Rule, TSA provides the following conclusions and summary information:

(1) TSA has determined that this final rule is a significant rulemaking within the definition of EO 12866, as estimated annual costs or benefits exceed $100 million in any year;
(2) TSA estimated that, of 460 U.S. airports affected by the final rule, seven are considered small. TSA estimated that the cost of the final rule results in less than a one percent impact on revenue for 100 percent of the small entities;
(3) TSA has determined that this final rule imposes no significant barriers to international trade as defined by the Trade Agreement Act of 1979; and
(4) TSA has determined that this final rule does not impose an unfunded mandate on State, local, or tribal governments as defined by the UMRA.

This executive summary highlights the costs and benefits of the final rule, which codifies the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. TSA estimates costs incurred by airport operators, the traveling public, the screening systems industry, and TSA. Some airport operators incur utilities costs for the additional electricity consumed by AIT machines. A small percentage of passengers who request to opt-out of AIT screening incur opportunity costs due to the additional screening time needed to receive a pat-down. A company that manufactures AIT machines incurs a cost to remove backscatter AIT units in 2013 that had been deployed in previous years.[6] TSA incurs equipment costs throughout the life cycle of AIT machines (testing, acquisition, maintenance, etc.), personnel costs for Transportation Security Officers (TSOs) to operate the AIT machines, utilities costs at reimbursed airports, and training costs of TSOs for the purpose of operating AIT machines.

The final rule is adopted to comply with a ruling of the United States Court of Appeals for the District of Columbia Circuit. In Electronic Privacy Information Center (EPIC) v. U.S.

---

[6] On December 21, 2012, TSA terminated part of its contract with the manufacturer of backscatter AITs. As a result of the contract termination, the manufacturer paid for the removal of the remaining units in the field.

Department of Homeland Security (DHS),[7] the court directed TSA to conduct notice-and-comment rulemaking on the use of AIT to screen passengers. TSA published a notice of proposed rulemaking (NPRM) on March 26, 2013, (78 FR 18287) and requested that comments be submitted by June 24, 2013. Private citizens, industry associations, advocacy groups, and non-profit organizations submitted comments. From all the comments received, many addressed either the regulatory impact analysis, regulatory flexibility analysis, or other economic issues. TSA summarized these comments and corresponding changes in the final rule section *II. Public Comments on the NPRM and TSA Responses*.

In response to public comments, TSA added a break-even analysis in the benefits section of this RIA. Additionally, TSA revised its RIA from the NPRM to include pertinent data that has become available since the publication of the NPRM, including an updated AIT deployment schedule.[8] TSA's changes to the RIA from the NPRM are:

- Revising the airport listings to include 460 airports instead of 448. The updated airport list includes new, previous, and former airports that operated AIT units and are regulated under 49 CFR part 1542;
- Updating the AIT life cycle and period of analysis from 8 to 10 years based on a recent life cycle cost estimate (LCCE) report[9] from the Office of Security Capabilities (OSC). Using the information from this report, TSA also revised its previous assumption about the share of Passenger Screening Program (PSP) expenditures spent on AIT technology;
- Revising the number of AIT units to be deployed from 821 to 793 throughout the period of analysis (2008-2017) based on new data;[10]
- Revising the total wait time for a passenger that opts-out of AIT from 80 to 150 seconds to include passenger time spent waiting for a same gender TSO to perform the pat-down;

[7] 653 F.3d 1 (DC Cir. 2011).
[8] The RIA from the NPRM can be found in the Passenger Screening Using Advanced Imaging Technology docket (Docket ID: TSA-2013-0004, RIN: 1652-AA67).
[9] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[10] The number of AIT machines in the field is a dynamic estimate. TSA may add or remove AIT machines abruptly for the purpose of addressing security risks or increasing efficiency in its passenger screening program.

- Revising the calculation of utilities costs to incorporate new data on the hours of AIT operation from the TSA's Performance Management Information System (PMIS) database;
- Refining the calculation of personnel costs by using information on specific labor hours dedicated to AIT operation in response to new data on hours of AIT operation;
- Revising the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs;
- Including a break-even analysis to answer the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?''
- Revised language within the RIA and final rule to state that passengers "may generally opt-out of AIT screening" to reflect current DHS policy;[11]

The revisions listed above are a result of public comments, acquirement of more recent data, and revisions to previous estimates since TSA published the NPRM. Table 1 presents a summary of the effects these changes from the NPRM to the final rule had on the costs and benefits in the RIA. The NPRM and final rule costs and benefits have been annualized for comparison.

---

[11] See Privacy Impact Assessment Update for TSA Advanced Imaging Technology (DHS/TSA/PIA-032(d)) December 18, 2015 https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf

Table 1: Changes in AIT Estimates from the NPRM to the Final Rule (Annualized at a 7% Discount Rate in 2014 dollars)

Variables	NPRM and FR Comparison			Description of Changes
	NPRM	Final Rule	Difference	
Annualized Industry Costs ($millions)				
Airport Utilities Costs	$0.19	$0.15	-$0.04	This estimate decreased due to the incorporation of newly available historical data on AIT hours of operation from the TSA's PMIS database.
Backscatter AIT Removal	$0.21	$0.18	-$0.03	Total cost in constant dollars remained the same, but annualized cost decreased because of the different periods of analysis between NPRM and final rule.
Annualized Passenger Costs ($millions)				
Opportunity Costs (Delay Costs)	$2.08	$2.60	$0.52	This estimate increased because the estimated duration of a pat-down increased from 80 to 150 seconds to include passenger wait time to be handed off to a same gender TSO.
Annualized TSA Costs ($millions)				
Personnel	$216.40	$117.17	-$99.22	TSA refined this estimate to account for labor hours dedicated to AIT operation. TSA used AIT operational hours recorded in PMIS as a basis for this estimate.
Training	$5.81	$27.68	$21.87	TSA revised the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs.

Variables	NPRM and FR Comparison			Description of Changes
	NPRM	Final Rule	Difference	
Equipment	$70.62	$56.53	-$14.08	TSA revised its cost estimates in 2014 -2017 to reflect the most recent LCCE document by OSC. TSA also revised some assumptions for cost estimates from 2008-2013 based on the recent LCCE.
TSA Utilities Costs	$0.25	$0.26	$0.01	This change reflects the revised estimate on AIT operation time and an increase of airport enrollment in TSAs utilities reimbursement program.
Total Costs	**$295.56**[12]	**$204.57**	-$90.99	The total cost decreased from the NPRM, primarily from the reduction in personnel costs.
Benefits				
Break-Even Analysis	Prevent 1 attack per 5.25 to 23.52 years considering only the major direct costs of an averted attack.			Per public comment, TSA has included a break-even analysis in the RIA.

Need for Regulatory Action

In 2010, EPIC and two individuals petitioned for review of a decision by TSA to screen airline passengers by using AIT. They argued that this use of AIT violates various Federal statutes and the Fourth Amendment to the Constitution of the United States and, in any event, should have been the subject of notice-and-comment rulemaking before being adopted.[13] In the decision rendered by the U.S. Court of Appeals for the District of Columbia Circuit in Electronic Privacy

[12] There was a calculation error in the NPRM's presentation of annualized costs. TSA has resolved this error and presented the correct annualized amounts in Tables 1 and 58 of this RIA. The calculation error in annualized costs did not affect any other cost estimates in the NPRM, including the estimated total cost of the rule and the estimated itemized costs presented in the NPRM.
[13] On Petition for Review of and Order of the U.S. Department of Homeland Security (07/15/11). USCA Case#10-1157. Document #1318805.

Information Center v. U.S. Department of Homeland Security,[14] the Court upheld the constitutionality of AIT screening and directed TSA to conduct notice-and-comment rulemaking on the use of AIT. The Court also allowed TSA to continue using AIT as part of its airport security operations. TSA developed a NPRM and a final rule to comply with the Court's decision.

Prior to the terrorist attacks of September 11, 2001, and the enactment of the Aviation and Transportation Security Act (ATSA),[15] air carriers were required to conduct the screening of passengers and property, and did so in accordance with regulations issued by the Federal Aviation Administration (FAA) and security programs approved by the FAA.[16] ATSA transferred that responsibility to TSA and required the TSA Administrator to provide for the screening of all passengers and property that will be carried aboard a passenger aircraft.[17] Federal law also requires the TSA Administrator to prescribe regulations to require air carriers to refuse to transport a passenger, or the property of a passenger who does not consent to a search, and to protect passengers and property on an aircraft against an act of criminal violence or aircraft piracy.[18] TSA has determined that AIT is the best method currently available to screen passengers for metallic and non-metallic threats concealed under clothing prior to entering the sterile area of an airport or boarding an aircraft. While there is no single technology or procedure that will protect against every terrorist threat, AIT is one layer among many that TSA uses to fulfill its statutory mandate.

---

[14] 653 F.3d 1 (D.C. Cir. 2011).

[15] Pub. L. 107-71 (Nov. 19, 2001)

[16] 14 C.F.R. part 108, 66 FR 37330 (July 17, 2001). The FAA Administrator prescribed regulations requiring air carriers to screen all passengers and property before boarding.

[17] 49 U.S.C. § 44901(a):
In general.--The Under Secretary of Transportation for Security shall provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation. In the case of flights and flight segments originating in the United States, the screening shall take place before boarding and shall be carried out by a Federal Government employee (as defined in section 2105 of title 5, United States Code), except as otherwise provided in section 44919 or 44920 and except for identifying passengers and baggage for screening under the CAPPS and known shipper programs and conducting positive bag-match programs.

[18] 49 U.S.C. § § 44902(a) and 44903(b).

Baseline and Cost

TSA used WTMD as the primary passenger screening technology in place at screening checkpoints prior to the deployment of AIT. WTMDs alarm if a passenger has metallic objects on his person. Passengers who alarm the WTMD receive additional screening to determine whether the metal object is prohibited. Current procedures for WTMD alarms allow a passenger to divest metallic objects from his person and pass through the WTMD until the alarm is resolved. If the alarm cannot be resolved by divesting metallic objects and repeating WTMD screening, or if the passenger cannot undergo WTMD screening, the passenger receives a pat-down.

When estimating the costs and benefits of a rulemaking, agencies typically estimate future expected costs and benefits resulting from a regulation throughout a fixed period of analysis. Agencies estimate regulatory costs and benefits on an incremental basis, or the costs and benefits of the regulation as compared to a baseline, or "status quo" scenario. For this final rule, TSA conducts a RIA which measures the incremental costs and benefits of AIT over the baseline of continuing to use WTMDs as the primary screening technology.

In this RIA, TSA uses a 10-year period of analysis to align with the expected duration of an AIT machine's life cycle. TSA revised the NPRM RIA assumption of an 8-year life cycle to 10 years based on a recent LCCE report.[19]. Given the existing Reliability, Maintainability, and Availability (RMA) fleet data, a life cycle exceeding ten years is likely achievable and TSA will continue to advance the life cycle projection as more RMA data becomes available. AIT deployment began in 2008 and TSA, therefore, includes costs that have already been borne by TSA, the traveling public, the screening systems industry, and airports. Consequently, the RIA takes into account costs that have already occurred — in years 2008-2014 — in addition to the

[19] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. Lifecycle revisions are based on a recent useful life study for each type of transportation security equipment. These are TSA internal sensitive information reports based on OSC technology assessments.

projected costs in years 2015- 2017.[20] By reporting the costs that have already happened and projecting future costs in this manner, TSA accounts for the full life cycle of AIT machines.

AIT Units Deployment

TSA uses historical data on AIT units deployed from 2008-2015 and projects the number of units to be deployed in 2016-2017 (based on TSA's current and expected screening technology funding) to inform its analysis. For this final rule, TSA used the most recent data available and updated the AIT deployment information used in the NPRM. TSA revised the numbers of units from the NPRM as more data became available. Due to this revision to the number of AIT units deployed, TSA also revised the number of in-service units throughout the period of analysis. Table 2 and Table 3 summarize the number of AIT units TSA projects to deploy and keep in service, by category of airport, over the period of analysis.[21]

[20] The 2015 cost estimates used historical data when available.

[21] TSA Airport Security Categories as defined by 49 CFR § 1542.103.

Table 2: AIT Units Deployment by Category of Airport[22] [23] [24]

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	17	15	0	0	0	**32**
2009	1	3	0	0	0	**4**
2010	273	133	17	2	0	**425**
2011	3	44	21	11	0	**79**
2012	208	39	61	36	0	**344**
2013	35	32	3	1	0	**71**
2014	3	2	1	1	0	**7**
2015	17	6	9	25	0	**57**
2016	0	0	0	0	0	**0**
2017	0	0	0	0	0	**0**

[22] Indicates initial deployment of AIT system.
[23] AITs may have been subsequently moved to another airport or a testing facility. Airport category may have also changed.
[24] Totals do not include AITs deployed to testing facilities, the TSA Academy at Federal Law Enforcement Training Centers (FLETC), or units located in warehouse awaiting deployment. AITs in testing capacities do not serve the purpose of this rule which is to screen passengers.

Table 3: Cumulative Number of AIT Units In-Service by Category of Airport[25] [26] [27]

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	17	15	0	0	0	**32**
2009	18	18	0	0	0	**36**
2010	292	150	17	2	0	**461**
2011	295	194	38	13	0	**540**
2012	501	233	101	49	0	**884**
2013	394	212	103	14	0	**723**
2014	393	227	95	14	0	**729**
2015	428	235	99	31	0	**793**
2016	428	235	99	31	0	**793**
2017	428	235	99	31	0	**793**

Total Costs and Benefits

TSA estimates the historical cost of AIT from 2008-2014 to be $1,439.32 million (undiscounted). Table 4 reports historical costs for each cost category. These costs, as with all monetized values displayed in this document, are expressed in 2014 dollars.

[25] Indicates end of the calendar year location of AIT system.
[26] AITs may have been subsequently moved to another airport or a testing facility. Airport category may also have changed.
[27] The table represents the number of AITs in service at each year's end.

Table 4: Cost Summary from 2008-2014 by Cost Component

(in $millions, undiscounted)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Industry Costs	Total
			Personnel	Training	Equipment	Utilities [28]	Backscatter Removal	
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	$0.02	$0.01	$12.05	$0.57	$28.01	$0.02	$0.00	$40.69
2010	$0.42	$0.13	$57.20	$33.64	$118.66	$0.23	$0.00	$210.28
2011	$3.17	$0.15	$201.83	$57.06	$76.86	$0.26	$0.00	$339.33
2012	$5.28	$0.28	$219.75	$23.31	$101.59	$0.37	$0.00	$350.58
2013	$4.45	$0.25	$197.77	$14.37	$46.70	$0.34	$1.90	$265.79
2014	$3.05	$0.18	$131.22	$12.21	$41.28	$0.37	$0.00	$188.31
Total	**$16.40**	**$1.02**	**$830.09**	**$141.16**	**$447.14**	**$1.61**	**$1.90**	**$1,439.32**

Note: Totals may not sum exactly due to rounding.

TSA estimates the projected cost of AIT from 2015-2017 to be $706.99 million (undiscounted), $666.47 million discounted at three percent, and $618.18 million discounted at seven percent. Table 5 reports projected costs for each cost category.

[28] TSA incurs incremental utilities cost for the deployment of AIT at airports enrolled in the utilities reimbursement program.

Table 5: Cost Summary from 2015-2017 by Cost Component

(in $millions)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Total
			Personnel	Training	Equipment	Utilities	
2015	$4.12	$0.20	$141.96	$41.25	$49.75	$0.40	$237.68
2016	$4.20	$0.20	$141.96	$54.89	$25.06	$0.40	$226.72
2017	$4.28	$0.20	$141.96	$69.30	$26.45	$0.41	$242.60
Total	**$12.59**	**$0.61**	**$425.89**	**$165.45**	**$101.25**	**$1.20**	**$706.99**
Total (Discounted at 3%)	**$11.87**	**$0.57**	**$401.55**	**$155.22**	**$96.12**	**$1.13**	**$666.47**
Total (Discounted at 7%)	**$11.01**	**$0.53**	**$372.55**	**$143.07**	**$89.97**	**$1.05**	**$618.18**

Note: Totals may not sum exactly due to rounding.

TSA estimates the total cost of AIT from 2008-2017 to be $2,146.31 million (undiscounted) and that TSA incurs over 98 percent of all costs. Table 6 reports total costs for each cost category.

Table 6: Total Cost Summary from 2008-2017 by Cost Component

(in $millions, undiscounted)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Industry Costs	Total
			Personnel	Training	Equipment	Utilities	Backscatter Removal	
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	$0.02	$0.01	$12.05	$0.57	$28.01	$0.02	$0.00	$40.69
2010	$0.42	$0.13	$57.20	$33.64	$118.66	$0.23	$0.00	$210.28
2011	$3.17	$0.15	$201.83	$57.06	$76.86	$0.26	$0.00	$339.33
2012	$5.28	$0.28	$219.75	$23.31	$101.59	$0.37	$0.00	$350.58
2013	$4.45	$0.25	$197.77	$14.37	$46.70	$0.34	$1.90	$265.79
2014	$3.05	$0.18	$131.22	$12.21	$41.28	$0.37	$0.00	$188.31
2015	$4.12	$0.20	$141.96	$41.25	$49.75	$0.40	$0.00	$237.68
2016	$4.20	$0.20	$141.96	$54.89	$25.06	$0.40	$0.00	$226.72
2017	$4.28	$0.20	$141.96	$69.30	$26.45	$0.41	$0.00	$242.60
Total	**$28.99**	**$1.63**	**$1,255.98**	**$306.61**	**$548.39**	**$2.81**	**$1.90**	**$2,146.31**

Note: Totals may not sum exactly due to rounding.

Benefits

Implementing AIT into the passenger screening program is beneficial as compared to WTMDs because it enhances commercial aviation security. AIT improves security by assisting TSA in the detection of non-metallic, as well as metallic, explosives concealed under the clothing of passengers. AIT may also provide the added benefit of deterrence—the effect of would-be attackers becoming discouraged as a result of increased security measures which would have the intended effect of reducing the likelihood of a successful attack.

The capability of AIT to detect both metallic and non-metallic weapons and both explosive and non-explosive weapons as compared to the WTMDs results in security benefits. The nature of the threat to transportation security has evolved since September 11, 2001. Terrorists continue to test security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. The examples presented below highlight the increased real world threats of non-metallic explosives to commercial aviation:

- On December 22, 2001, on-board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.
- In 2004, terrorists mounted a successful attack on two domestic Russian passenger aircraft using non-metallic explosives concealed on the torsos of female passengers.
- In 2006, terrorists in the United Kingdom plotted to bring liquid explosives on board an aircraft with the intention to construct and detonate a bomb while in flight.
- A bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in the December 25, 2009 attempt by Umar Farouk Abdulmutallab to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In a recent terrorist plot thwarted in May 2012, AQAP developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

As evidenced by these incidents,[29] TSA operates in a high-threat environment. As demonstrated by the device used in the December 25, 2009 attempt, terrorists look for security gaps or exceptions to exploit. Terrorists constructed the device and hid it on a sensitive part of the body to avert detection. If detonated, the lives of the almost 300 passengers and crew, and untold numbers of people on the ground, would have been in jeopardy.

[29] TSA is aware that these events occurred on flights originated outside the U.S. These incidents nonetheless highlight the ever-growing threat to commercial aviation from non-metallic explosives and demonstrate that terrorists continue to attack aviation through innovative means.

AIT is the only technology that will find both metallic and non-metallic items, and will find both explosives and non-explosives items. The WTMD only finds metallic items, thus does not find such threats as explosive devices made without metal, or other non-metallic items. The ETD will find only explosives, not metallic items (such as firearms) or non-metallic items that are not explosives (such as ceramic knives); the same is true for explosives detection canines. Pat-down screening is useful for finding both metallic and non-metallic items, and will find both explosives and non-explosives items, however, that method is slower than AIT and many persons consider pat downs to be more intrusive than AIT. Since it began using AIT, TSA has detected many kinds of non-metallic items, small items, and items concealed on parts of the body; examples of such are detailed in the body of the analysis.

TSA includes a break-even analysis to compare the potential security benefits of AIT with the cost of AIT. Agencies use a break-even analysis when quantification of benefits is not possible. According to OMB Circular No. A–4, ''Regulatory Analysis,'' such an analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the non-quantified costs need to be) before the rule would yield zero net benefits?''[30] TSA decided to include a break-even analysis based upon public comments made to the NPRM that requested this type of analysis.

TSA used five types of aircrafts to represent five different scenarios where an attacker detonates a body-bomb on a domestic passenger aircraft, the type of attack AIT is meant to mitigate. The five types of aircraft fall into two assigned categories: high-capacity, long range aircrafts typically used for international travel; and a medium-capacity and mid-range aircrafts typically used for cross-country travel or popular routes. TSA used the Bureau of Transportation Statistics' T-100 domestic segment data from 2014 to determine the most popular aircraft models for both categories of aircrafts.[31] The most popular aircraft models are defined as the aircraft that had the most departures performed.[32] TSA also includes the Airbus A380 and the Boeing

[30] http://www.whitehouse.gov/omb/circulars_a004_a-4/
[31] U.S. Department of Transportation, Bureau of Transportation Statistics. "T-100 Domestic Segment (All carriers) Data bank". http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air. Selected fields: DepPerformed, Aircraft Type, and Year = 2014, All months.
[32] Boeing 737-700/700LR, Boeing 737-800, and Airbus A320-100/200 are the first-, fourth-, and fifth-most often-used aircrafts in 2014, respectively based on departures from BTS T-100 data.

777-200 in this analysis because they are likely targets due to their higher seat capacity. TSA used the T-100 from 2014 to determine the average load factor for each aircraft type.[33] The load factor for each aircraft type is found by dividing the total sum of passengers in 2014 by the sum of available seats for each aircraft type.

To conduct the break-even analysis, TSA estimated the major direct costs for these attack scenarios, which can be viewed as the benefits of avoiding an attack. The break-even analysis does not include the difficult-to-quantify indirect costs of an attack. TSA assumed all the passengers and crew are killed in each scenario and used the value of statistical life (VSL) of $9.1 million per fatality as adopted by the U.S. Department of Transportation (DOT)[34] to monetize the consequences from fatalities. TSA emphasizes that the VSL is a statistical value used here only for regulatory comparison and does not suggest that the actual value of a life can be stated in dollar terms. In all scenarios, it is assumed that all passengers and crew lives are lost and the aircraft is destroyed.[35] Although it is possible for an attacker to detonate an explosive on an airplane without downing the airplane, only causing immediate casualties to those sitting near the attacker, there are examples of airplanes being downed from an explosion. TSA is unable to precisely quantify the resiliency of aircraft to all types of attacks taking into account the various factors that may occur in an explosion (e.g. where the attacker is seated, how much and type of explosives). Terrorists are also conscious opponents in that they are seeking to down the airplane and will likely target vulnerable areas of the aircraft to detonate their explosives. Given the imprecise nature of quantifying these factors and their associated risk, along with the fact that terrorists are constantly changing strategies to seek the most vulnerable area of an aircraft, TSA uses the break-even analysis. A break-even analysis squarely focuses on measuring the threshold of successful attacks—those that meet the terrorist goal of downing the aircraft—that need to be averted for the cost of AIT to equal its quantified benefits and does not attempt to measure the precise decrease in risk .

---

[33] U.S. Department of Transportation, Bureau of Transportation Statistics. "T-100 Domestic Segment (All carriers) Data bank". http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air. Selected fields: Seats, Passengers, Aircraft Type, and Year = 2014, All months.

[34] U.S. Department of Transportation. "Guidance on Treatment of Economic Value of a Statistical Life in U.S. Department of Transportation Analyses". http://www.dot.gov/sites/dot.dev/files/docs/VSL%20Guidance%202013.pdf.

[35] TSA does not include for the possibility that there are fatalities on the ground or secondary and tertiary economic effects.

The replacement cost of the aircraft and emergency response costs[36] [37] are added to the loss of life to sum up the total cost of each attack scenario. TSA then calculates the ratio between the estimated cost of a successful attack and the annualized cost of AIT using a seven percent discount rate. By generating a ratio between these costs, TSA estimates how small the value of non-quantified benefits would need to be for the deployment of AIT to yield zero net benefits.

Table 7 presents the number of attacks[38] averted compared to the baseline (expressed as a number of years between attacks) that would be required to break even for all five attack scenarios. In the least costly scenario (Boeing 737-700/700LR), AIT will need to prevent an attack at the magnitude described above once every 5.25 years for the direct cost of an averted attack to equal the annualized cost of AIT. In the most-costly scenario (Airbus A380), AIT will need to prevent an attack once every 23.52 years for the direct cost of an averted attack to equal the annualized cost of AIT.

[36] TSA uses proxy estimate of $869,552 (inflated from $800,000 in 2009 dollars) from a lawsuit filed by The County of Erie, New York to recuperate emergency response costs from Colgan Air, Inc. in response to the Colgan Air Flight 3407 crash. These costs include overtime, removal of human remains, cleanup of the aircraft and chemical substances, counseling for the surviving family members, and acquiring special equipment.
[37] McGrory, Michael, "Airlines Not Liable for Colgan Air Crash Clean-Up Costs", *SmithAmunden Aerospace Report*, March 20, 2013, http://www.salawus.com/insights-alerts-70.html
[38] In all scenarios, it is assumed that all passengers and crew lives are lost and the aircraft is destroyed. TSA does not include for the possibility that there are fatalities on the ground or secondary and tertiary economic effects.

Table 7: Frequency of Attacks Averted to Break-Even (in $millions)

Aircrafts	Replacement & Emergency Response Costs	Total Passengers + Crew	Load Factor	Total Consequence	Attacks Averted by AIT to Break-Even: Total Consequence / $204.57M
	a	b	c	d = a + (b x c x VSL)	e = d ÷ $204.57M
High Capacity					
Airbus A380	$428.9	557	86%	$4,811	1 attack per 23.52 yrs
Boeing 777-200	$305.9	326	84%	$2,791	1 attack per 13.64 yrs
Medium Capacity					
Boeing 737-700/700LR	$79.2	138	80%	$1,075	1 attack per 5.25 yrs
Boeing 737-800	$94.2	176	84%	$1,434	1 attack per 7.01 yrs
Airbus Industries A320-100/200	$97.9	156	85%	$1,305	1 attack per 6.38 yrs

Accounting Statement

Table 8 presents annualized costs and qualitative benefits of AIT in projected years (2015-2017). Costs incurred from 2008-2014 occurred in the past and therefore are not discounted. However, given that period of analysis is 10 years; TSA also added Table 9 showing the annualized net cost of AIT from 2008-2017 (full 10 year AIT life cycle including "sunk" costs from 2008-2014[39]). The costs are annualized and discounted at both three and seven percent and presented in 2014 dollars.

[39] TSA used negative discount rates for costs in years which have already occurred for the purpose of annualizing costs to 2014 dollars over the period of analysis.

Table 8: OMB A-4 Accounting Statement for 2015-2017 (in $millions)

Category		***Primary Estimate***	***Minimum Estimate***	***Maximum Estimate***	***Source Citation (Final RIA, preamble, etc.)***
BENEFITS					
Annualized monetized benefits (discount rate in parentheses)	(7%)	N/A			Final RIA
	(3%)	N/A			Final RIA
Unquantified benefits	The operations described in this rule produce benefits by reducing security risks through the deployment of AIT that can detect non-metallic weapons and explosives.				Final RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$235.56			Final RIA
	(3%)	$235.62			
Annualized quantified, but unmonetized, costs		0	0	0	Final RIA
Qualitative costs (unquantified)	N/A				Final RIA
TRANSFERS					
Annualized monetized transfers: "on budget"		0	0	0	Final RIA
From whom to whom?		N/A	N/A	N/A	None
Annualized monetized transfers: "off-budget"		0	0	0	Final RIA
From whom to whom?		N/A	N/A	N/A	None
Miscellaneous Analyses/Category	***Effects***				***Source Citation (Final RIA, preamble, etc.)***
Effects on state, local, and/or tribal	None				Final RIA
Effects on small businesses	No significant economic impact. Prepared FRFA.				FRFA
Effects on wages	None				None
Effects on growth	None				None

Table 9: OMB A-4 Accounting Statement for 2008-2017 (in $millions)

(Ten-year lifecycle)

Category	***Primary Estimate***		***Minimum Estimate***	***Maximum Estimate***	***Source Citation (Final RIA, preamble, etc.)***
BENEFITS					
Annualized monetized benefits (discount rate in parentheses)	(7%)	N/A			Final RIA
	(3%)	N/A			Final RIA
Unquantified benefits	The operations described in this rule produce benefits by reducing security risks through the deployment of AIT capable of detecting non-metallic weapons and explosives.				Final RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$204.57			Final RIA
	(3%)	$210.47			
Annualized quantified, but unmonetized, costs	0		0	0	Final RIA
Qualitative costs (unquantified)	N/A				Final RIA
TRANSFERS					
Annualized monetized transfers: "on budget"	0		0	0	Final RIA
From whom to whom?	N/A		N/A	N/A	None
Annualized monetized transfers: "off-budget"	0		0	0	Final RIA
From whom to whom?	N/A		N/A	N/A	None
Miscellaneous Analyses/Category	***Effects***				***Source Citation (Final RIA, preamble, etc.)***
Effects on state, local, and/or tribal	None				Final RIA
Effects on small businesses	No significant economic impact. Prepared FRFA.				FRFA
Effects on wages	None				None
Effects on growth	None				None

Alternatives

TSA examined four options to the preferred alternative presented in the final rule. Table 10 presents a comparison of the options considered, which include a continuation of the screening environment prior to 2008 (WTMDs only), increased use of physical pat-down searches that supplements primary screening with WTMDs, increased use of explosives trace detection (ETD) screening that supplements primary screening with WTMDs, and AIT screening that supplements primary screening with WTMDs. TSA discusses in detail these alternatives, and the reasons why TSA rejected them in favor of the preferred alternative, in Chapter 3 of this regulatory impact analysis.

Table 10: Advantages and Disadvantages of Regulatory Alternatives

Regulatory Alternative	Name	Description	Advantages	Disadvantages
1	WTMDs Only	The passenger screening environment remains unchanged. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.	• No additional cost burden. • No additional perceived privacy concerns.	• Fails to meet the January 7, 2010 Presidential Memorandum and statutory requirement in 49 USC 44925.[40] • Does not mitigate the non-metallic threat to aviation security.
2	Pat-Down	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by with a pat-down on a randomly selected portion of passengers.	• Thorough physical inspection of metallic and non-metallic items. • Uses currently deployed WTMD technology. • Minimal technology acquisition costs.	• Employs a substantial amount of human resources. • Increase in number of passengers subject to a pat-down. • Increased wait times.
3	ETD Screening	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses the threat of non-metallic explosive threats.	• Does not detect non-explosive non-metallic potential threats. • Increased wait times and associated passenger opportunity cost of time. • Increase in ETD consumable costs.

[40] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack

Regulatory Alternative	Name	Description	Advantages	Disadvantages
4	AIT as Secondary Screening	TSA continues to use WTMDs as the primary screening technology. TSA supplements the WTMD screening by conducting AIT screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses non-metallic explosive threats.	• Primary screening does not detect non-metallic weapons or explosives. • Incremental cost of acquisition of AIT.
5	AIT	TSA uses AIT as a passenger screening technology. Alarms resolved through a pat-down.	• Addresses the threat of non-metallic explosives hidden on the body by safely screening passengers for metallic and non-metallic threats. • Maintains lower personnel cost and higher throughput rates than the other alternatives. • Adds deterrence value—the effect of would be attackers becoming discouraged as a result of AIT.	• Incremental cost of acquisition to TSA. • Incremental personnel cost to TSA. • Incremental training cost to TSA.

Final Regulatory Flexibility Analysis

In accordance with the RFA, TSA has prepared a Final Regulatory Flexibility Analysis (FRFA) that examines the impact on small entities (5 USC 601 et seq.). TSA identified 106 small entities (105 small governmental jurisdictions and one small privately-owned airport) based on the Small Business Administration size standards that potentially incur additional utilities costs due to AIT. Of the 106 small entities, seven currently have AITs deployed and are not reimbursed by TSA for the payment of utilities. Consequently, seven small entities, or 1.5 percent (7/460) of all airports, incur AIT-related costs during the period of analysis.

These entities incur an incremental cost for utilities from an increased consumption of electricity from AIT operation. To estimate these costs, TSA uses the average kilowatts (kW) consumed per AIT unit on an annual basis. Depending on the size of the airport, TSA estimates the average additional utilities costs to range from $290 to $921 per year while the average annual revenue for these small entities ranges from $8.4 million to $213.3 million per year.[41] TSA estimates that the cost impact of AIT to affected small entities is less than one percent of their annual revenue. Therefore, TSA has determined that AIT would not have a significant economic impact on a substantial number of small entities under section 605 (b) of the RFA. Chapter 6 outlines the FRFA's assumptions and estimates.

Reporting and Recordkeeping

This final rule does not require additional reporting, recordkeeping, or other paperwork.

[41] TSA has changed the way that utilities costs were calculated from the NPRM in order to match the operating time of an AIT with its associated cost for additional utilities consumption. The change in the revenue range for small entities from the NPRM is due to the population of airports which has been adjusted to include all airports that are regulated under 49 CFR Part 1542 since publication of the NPRM.

CHAPTER 1: INTRODUCTION

TSA provides this RIA to present an economic analysis of the Passenger Screening Using Advanced Imaging Technology (AIT) Final Rule. This RIA presents a description of the screening environment prior to deployment of AIT (baseline scenario), the required or expected changes to this environment resulting from the use of AIT, and an assessment of the associated costs and burdens placed on affected industries, governments, and the traveling public resulting from the use of AIT.

Background

The nature of the threat to transportation security has evolved since September 11, 2001. Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. For example, threats to aviation security now include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. The examples presented below highlight the increased real world threats of non-metallic explosives to commercial aviation:

- On December 22, 2001, on-board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.
- In 2004, terrorists mounted a successful attack on two domestic Russian passenger aircraft using non-metallic explosives concealed on the torsos of female passengers.
- In 2006, terrorists in the United Kingdom plotted to bring liquid explosives on-board an aircraft with the intention to construct and detonate a bomb while in flight.
- A bombing plot by AQAP culminated in the December 25, 2009, attempt by Umar Farouk Abdulmutallab to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In a recent terrorist plot thwarted in May 2012, AQAP had developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

As evidenced by these incidents,[42] TSA operates in a high-threat environment. Globally, terrorists have attempted to board planes with explosives hidden on sensitive parts of the body in an effort to avoid detection.

Congressional Direction to Pursue AIT

In 2004, Congress authorized TSA to continue to explore the use of new technologies to improve its threat detection capabilities (49 U.S.C. 44925). Specifically, the law provides:

> Deployment and use of detection equipment at airport screening checkpoints
>
> (a) Weapons and explosives.--The Secretary of Homeland Security shall give a high priority to developing, testing, improving, and deploying, at airport screening checkpoints, equipment that detects non-metallic, chemical, biological, and radiological weapons, and explosives, in all forms, on individuals and in their personal property . . . the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.
>
> (b) [The TSA Administrator shall submit] . . . a strategic plan to promote the optimal utilization and deployment of explosive detection equipment at airports to screen individuals and their personal property. Such equipment includes walk-through explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners.

Additional references[43] in Congressional reports accompanying appropriations and authorizing legislation demonstrate Congress's continued direction to DHS and TSA to pursue enhanced screening technologies and imaging technology, specifically:[44]

---

[42] TSA is aware these events occurred on flights originated outside the U.S., where TSA does not have jurisdiction. However, they highlight the ever-growing threat to commercial aviation from non-metallic explosives.

[43] See also, sec. 109 of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (2001), as amended by sec. 1403(b) of the Homeland Security Act of 2002, Pub. L. 107-296, "(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air

1) Explanatory Statement, House Appropriations Committee Print for Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (FY09 DHS Appropriations) Pub.L. 110-329 at p. 640:

> The bill provides $250,000,000 for Checkpoint Support to deploy a number of emerging technologies to screen airline passengers and carry-on baggage for explosives, weapons, and other threat objects by the most advanced equipment currently under development. TSA is directed to spend funds on multiple whole body imaging technologies including backscatter and millimeter wave as directed in the Senate report.

2) H. Rep. 110-862 at p. 64, FY09 DHS Appropriations:

> Over the past year, TSA has made some advances in testing, piloting, and deploying next-generation checkpoint technologies that will be used to screen airline passengers and carry-on baggage for explosives, weapons, and other threats. Even with this progress, however, additional funding is necessary to expedite pilot testing and deployment of advanced checkpoint explosive detection equipment and screening techniques to determine optimal deployment as well as preferred operational and equipment protocols for these new systems. Eligible systems may include, but are not limited to, advanced technology screening systems; whole body imagers; . . . The Committee expects TSA to give the highest priority to

---

carrier or foreign air carrier in air transportation or intrastate air transportation" and Title IV of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 ". . .for procurement and installation of checked baggage explosives detection systems and checkpoint explosives detection equipment."

[44] Additionally, the following language appeared in S. Rep. No. 111-222, accompanying S. 3602, the Department of Homeland Security Appropriations Bill 2011 at 60-61: "As requested, $192,200,000 is provided to deploy an additional 503 AIT units bringing the total to 1,000. AIT units screen passengers for metallic and non-metallic threats—including weapons, explosives, and other objects concealed under layers of clothing. With this increase, there will be an AIT unit in most Category X, I, and II airports. The Committee is aware of efforts by TSA to deploy automated target recognition [ATR] capability with AIT units in fiscal years 2010 and 2011. ATR displays a passenger's image as a stick figure on a monitor attached to an AIT unit, improving privacy protections and eliminating the need for private rooms to view AIT images." Senate 3602 was not passed by Congress; rather, DHS's 2011 appropriations were provided through a series of continuing resolutions and Pub. L. 112-10, which appropriated funding at essentially the same level as in FY2010. Thus, while of limited legal effect, the statement does express the Senate Appropriation Committee's intent to fund AIT.

> deploying next-generation technologies to designated Tier One threat airports.

3) S. Rep. 110-396 at p. 60, FY09 DHS Appropriations:

> WHOLE BODY IMAGERS. The Committee is fully supportive of emerging technologies at passenger screening checkpoints, including the whole body imaging program currently underway at Category X airports. These technologies provide an increased level of screening for passengers by detecting explosives and other non-metal objects that current checkpoint technologies are not capable of detecting. The Committee directs that funds for whole body imaging continue to be spent by TSA on multiple imaging technologies, including backscatter and millimeter wave.

4) H. Rep.110-259, at page 363, Conference Report to Implementing Recommendations of 9/11 Commission Act of 2007, Pub.L. 110-53, sec. 1601 - Airport checkpoint screening fund:

> The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) asserted that while more advanced screening technology is being developed, Congress should provide funding for, and TSA should move as expeditiously as possible to support, the installation of explosives detection trace portals or other applicable technologies at more of the nation's commercial airports. Advanced technologies, such as the use of non-intrusive imaging, have been evaluated by TSA over the last few years and have demonstrated that they can provide significant improvements in threat detection at airport passenger screening checkpoints for both carry-on baggage and the screening of passengers. The Conference urges TSA to deploy such technologies quickly and broadly to address security shortcomings at passenger screening checkpoints.

In addition, on January 7, 2010, the President issued a "Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack," which charged TSA with aggressively pursuing enhanced screening technology in order to prevent further such attempts.

TSA recognizes the emerging threat of passenger-borne improvised explosive devices (IEDs) and the current trend of transitioning from devices with metallic components to those composed of non-metallic components in order to subvert WTMDs. As the previously mentioned attempted terrorist attacks demonstrate, the threat to aviation security is real and ever-evolving. Non-metallic weapons and explosives are now the foremost threat to commercial passenger aviation.

Section 44925 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. 108-458, 118 Stat. 3638 (December 17, 2004) directs the Secretary of Homeland Security to give a high priority to developing and deploying equipment at airport screening checkpoints that detects non-metallic, chemical, biological, and radiological weapons and explosives that terrorists may try to smuggle on board an aircraft. To address the emerging threat of non-metallic weapons and explosives, TSA began an evaluation to determine the maturity and effectiveness of various technologies designed to detect non-metallic threats on passengers. After analyzing the latest intelligence and studying available technologies, TSA determined that the addition of AIT to its layered security approach provided the best opportunity to address the vulnerability of commercial aviation security to the evolving threat of non-metallic weapons and explosives.

In 2007, TSA initiated a pilot operation at several airports to test the detection capability of AIT on passengers who alarmed the WTMD. In 2008, TSA expanded its testing of AIT to additional airports, where TSA used AIT as the primary screening technology. The December 25, 2009, attempted bombing of Delta Flight 253, although ultimately unsuccessful, further highlighted the increasing need to deploy nationwide a technology or process capable of detecting non-metallic threats on the body. In addition, following that attempted attack, President Obama issued the "Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack," which charged TSA with aggressively pursuing enhanced screening technologies to prevent such attempts in the future, while at the same time protecting passenger privacy.[45] In the wake of the December 25, 2009, attempted aircraft bombing, TSA hastened to expand the deployment and use of AIT as the primary passenger screening technology.

Market Failure

Terrorists pose a real threat to the aviation industry. Market failure, however, reduces the incentives for private firms to provide the socially optimal level of security to prevent these attacks. Regulations function as a tool to correct market failure. In this case, due to the economics of externalities, the free market fails to provide adequate incentives for entities in the aviation industry to make socially optimal investments in security measures that reduce the probability of a successful terrorist attack.

Externalities are a cost or benefit from an economic transaction experienced by parties "external" to the transaction. In the case of commercial aviation, the consequences of an attack or other security incident may be significantly larger than what would be realized by an individual airport operator or commercial aircraft operator. Due to this fact, the private market does not provide the incentive for profit-maximizing firms to unilaterally spend the socially optimal amount of resources to prevent or mitigate a terrorist attack.

Because companies nevertheless likely suffer serious consequences in the case of a terrorist attack, many invest significant resources in implementing security measures. In a competitive marketplace, however, a firm has limited incentive to make additional investments in security over their privately optimal amount. Making security investments above its privately optimal amount would increase a firm's cost of production and put the firm at a disadvantage against competitors who have not made similar investments.

Congress enacted the ATSA, Pub. L. 107-71, 115 Stat. 597 (November 19, 2001) to create TSA and give TSA authority over security in all modes of transportation. ATSA also transferred responsibility for the screening of all passengers and property carried aboard a passenger aircraft

---

[45] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack

operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation to TSA and corrects the market failure that existed prior to the 9/11 terrorist attacks.

Need for Regulatory Action

In 2010, the Electronic Privacy Information Center (EPIC) and two individuals petitioned for review of TSA's decision to screen airline passengers using AIT. In Electronic Privacy Information Center v. U.S. Department of Homeland Security, the court rejected EPIC's claims regarding the constitutionality of AIT and held that AIT screening does not violate the Fourth Amendment.[46]

EPIC also argued that use of AIT should have been the subject of notice-and-comment rulemaking before being adopted. The court determined that TSA did not justify its failure to initiate notice-and-comment rulemaking and instructed TSA to undertake such a rulemaking.[47]

Prior to the terrorist attacks of September 11, 2001, and the enactment of ATSA,[48] air carriers were required to conduct the screening of passengers and property and did so in accordance with regulations issued by the Federal Aviation Administration (FAA) and security programs approved by the FAA.[49] ATSA transferred that responsibility to TSA and required the TSA Administrator to provide for the screening of all passengers and property that will be carried aboard a passenger aircraft.[50] Federal law also requires the TSA Administrator to prescribe regulations to require air carriers to refuse to transport a passenger or the property of a passenger who does not consent to a search, and to protect passengers and property on an aircraft against an act of criminal violence or aircraft piracy.[51]

---

[46] 653 F.3d 1, 16 (D.C. Cir. 2011).
[47] Id. at 18.
[48] Pub. L. 107-71 (Nov. 19, 2001)
[49] 14 C.F.R. part 108, 66 FR 37330 (July 17, 2001). The FAA Administrator prescribed regulations requiring air carriers to screen all passengers and property before boarding.
[50] 49 U.S.C. § 44901(a):
In general.--The Under Secretary of Transportation for Security shall provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation. In the case of flights and flight segments originating in the United States, the screening shall take place before boarding and shall be carried out by a Federal Government employee (as defined in section 2105 of title 5, United States Code), except as otherwise provided in section 44919 or 44920 and except for identifying passengers and baggage for screening under the CAPPS and known shipper programs and conducting positive bag-match programs.
[51] 49 U.S.C. § § 44902(a) and 44903(b).

TSA evaluated AIT as an alternative to the walk through metal detector. TSA compared AIT to other transportation security equipment and manual processes, including explosive trace detection, pat-downs, and walk through metal detectors. Based on the testing results, TSA determined that AIT offers the most effective screening capability to detect both metallic and non-metallic threat items concealed underneath clothing.

Equipment

AIT screens passengers by detecting potential threats—which may be a weapon or explosive hidden underneath clothing—on a person.[52] TSA has introduced two different types of AIT units to date. First, TSA introduced the millimeter AIT system (referred to throughout as the millimeter units or machines). These machines bounce electromagnetic waves off the body; the reflection of these waves creates an image of the passenger that highlights potential threats. The backscatter AIT system (referred to throughout as the backscatter units or machines) scans passengers with low-energy x-ray beams at high speed. Backscatter machines detect, digitalize, and display the reflection of the beam on a monitor for a TSO to examine for potential threats.

Initially, the images produced by the AIT were viewed in a remote, windowless room by an Image Operator (IO). Because the IO was located away from the checkpoint, the IO was unable to see the passenger being screened. If the IO identified a potential threat, the IO verbally communicated the location of the potential threat via headset to the system operator (SO), who then conducted alarm resolution in accordance with standard operating procedures. The inability of both the AIT machine and the computer used by the IO to store the image provided an additional level of privacy protection. TSA refers to these systems throughout as "AIT with IO."

In 2012, TSA implemented software that both eliminated the need for the IO position and provided further privacy protection to passengers. This software, known as Automated Target Recognition (ATR), (referred to throughout as "AIT with ATR") uses algorithms to detect potential threats found during the scan of a passenger. A monitor attached to the AIT unit then displays a generic outline with highlights marking the location of the potential threat(s). AIT

[52] With regards to screening for gender, TSA's standard operating procedure is to screen passengers by the gender they present themselves.

with ATR does not require an IO; if the equipment does not detect a potential threat, the text "OK" appears on the monitor with no outline, and the TSO notifies the passenger that the screening is complete.

ATR software increases the passenger throughput rate of AIT while simultaneously decreasing the number of officers required to staff and operate the units. ATR software also eliminates the need to construct remote viewing rooms used by the IO to view the images. TSA approved ATR software for millimeter units. In 2011, TSA upgraded all millimeter AIT machines with the ATR software. Since May 16, 2013, all AIT units in the field have been equipped with ATR software. Any AIT unit that could not accommodate ATR software was removed from the airport.

Changes to the Screening Checkpoint

In order to deploy AIT, TSA made changes to checkpoint configurations and staffing levels. Prior to AIT, checkpoints consisted of lanes with WTMDs for passenger screening and x-ray machines to screen carry-on baggage. TSA initially deployed WTMDs in configurations, called modsets, of either a 1:1 or 2:2 configurations of x-ray machines to passenger screening technology. The difference between the two modsets implies that there will either be one x-ray and one WTMD or two x-rays and two WTMDs in a configuration. Before 2008, TSA began a checkpoint optimization program, in which TSA removed the second WTMD from 2:2 configurations modifying it to a 2:1 configuration. This is done because WTMDs maintain a sufficient throughput rate to support two x-ray machines.

AIT with ATR provides sufficient throughput to handle the throughput of one x-ray machine but is not currently sufficient to handle the throughput of two x-ray machines. Therefore, to date, AIT has been deployed in modsets with two x-ray machines and a co-located WTMD, modsets with one x-ray machine and one co-located WTMD, and modsets with one x-ray machine and no WTMD. Most AIT machines are co-located with a WTMD and service passengers from two x-ray machines (a 2:2 modset).

CHAPTER 2: AIT DEPLOYMENT COSTS

This chapter outlines TSA's estimates for the cost of AIT deployment from 2008-2017. Cost elements include utilities costs to airport operators and TSA, opportunity costs for passengers who opt-out of AIT screening, personnel and training costs to TSA, and equipment life cycle costs of AIT to a screening technology contractor and TSA.[53]

Population Data, Sources, and Assumptions

This section outlines the population estimates and assumptions used in this analysis. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. For this RIA, TSA uses a 10-year period of analysis to align with the 10-year AIT life cycle from deployment to disposal.[54] TSA has revised the NPRM RIA assumption of an 8-year life cycle for AIT units to 10 years based on a recent LCCE from an internal, acquisition sensitive information report.[55] Given the existing Reliability, Maintainability, and Availability (RMA) fleet data, a life cycle exceeding ten years is likely achievable and TSA will continue to advance the life cycle projection as more RMA data becomes available. AIT deployment began in 2008 and TSA, therefore, includes costs that have already been borne by TSA, the traveling public, the screening systems industry, and airports. Consequently, the RIA takes into account costs that have already occurred — in years 2008-2014 — in addition to the projected costs in years 2015- 2017.[56] By reporting the costs that have already happened and estimating future costs in this manner, TSA accounts for the full life cycle of AIT machines.

TSA uses the Performance Measurement Information System (PMIS) database to acquire information on the screening environment for the historical years in this analysis. PMIS gathers

---

[53] TSA recognizes that some screening services are completed through TSA contracts. The contracted screening is identical to TSA-conducted screening and fully funded by TSA including staffing, equipment, training, and management at the airport. For the purposes of this analysis, TSA does not differentiate between the contracted screening and TSA screening.
[54] In the NPRM RIA, the AIT life cycle was estimated to be eight years. Therefore, the period of analysis for the RIA was also eight years.
[55] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. Lifecycle revisions are based on a recent useful life study for each transportation security equipment. These are TSA internal sensitive information reports based on OSC technology assessments.
[56] The 2015 cost estimates used historical data when available.

data from airports in order to improve performance. This data informs TSA on the number of hours that AITs are in operation, passenger throughput, and AIT passenger throughput rates. TSA applies a compounded annual growth rate (CAGR)[57] based on historical years in PMIS to project for 2015-2017.

TSA also relies on program office subject matter experts (SMEs) to project changes in the AIT deployment, and make assumptions related to industry and labor throughout the RIA. Additionally, TSA uses the Passenger Screening Program's (PSP) LCCE[58] for AIT to project future life cycle costs and make assumptions on historical costs. Finally, TSA uses the Bureau of Economic Analysis (BEA) Gross Domestic Product (GDP) indexes to adjust all costs to 2014 dollars. These indexes are shown in Table 11.[59]

[57] A compounded annual growth rate (CAGR) is the year-over-year growth rate of a value over a specified period of time. In terms of finance, a CAGR would illustrate how an investment grew over time on an annual basis. TSA applied this same concept to estimate total passenger throughput for the projected years of this analysis.
[58] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[59] In accordance with Circular A-4, TSA uses a GDP deflator to state all dollars in constant 2014 dollars. The GDP inputs are from the Bureau of Economic Analysis, Table 1.1.4 "Price Indexes for Gross Domestic Product" from the National Income and Product Accounts Table, found at http://www.bea.gov/iTable/iTable.cfm?ReqID=9&step=1.

Table 11: Adjustment Index (Reflects adjustment to 2014 Dollars[60])

Year	Indexes
2008	1.096
2009	1.087
2010	1.074
2011	1.052
2012	1.033
2013	1.016
2014	1.000

Populations

TSA is responsible for screening passengers and property at all airports that are regulated under 49 CFR part 1542. For the purpose of this RIA, TSA accounts for the 460 airports that are either currently, or were at one point, regulated since the beginning of the period of analysis (2008). The population of regulated airports may change as the operation of airports changes.[61] TSA accounts for the historical and projected costs for the 156 airports which use AITs—although WTMDs will still be used in partnership with AITs for overflow, expedited screening, and certain other populations, such as crewmembers, passengers 12 years of age and under, and

[60] For example, a cost of $100 in 2008 would equal $109.60 in 2014 dollars ($100 x 1.096).

[61] Airports may be removed from Federal regulation or become federally regulated under 49 CFR part 1542. Airports may also change categories based on volume and other factors. All airports may reclassify under different categories, however, this more frequently occurs among the smaller airports.

individuals who qualify for TSA Pre✓™.[62] Table 12 shows the breakdown of part 1542-regulated airports into FAA's five categories.[63]

Table 12: Number of Airports by Category

FAA Category	Number of Airports
X	28
I	56
II	78
III	131
IV	167
Total	**460**

In 2012, Congress passed a law that affected the use of AIT. The FAA Modernization and Reform Act of 2012 mandated that, beginning June 1, 2012, TSA "shall ensure that any advanced imaging technology used for the screening of passengers…is equipped with and employs [ATR]; and complies with such other requirements as the Assistant Secretary determines necessary to address privacy considerations" (sec. 828). The TSA Administrator issued an extension under subparagraph (A) of this act, whereby TSA committed to meet this mandate by June 1, 2013. All general-use backscatter units used at TSA checkpoints were removed from all airports by May 16, 2013, because they could not meet the statutory requirement by the deadline.

[62] TSA Pre✓™ allows approved enrollees, select frequent flyers of participating airlines, and members of U.S. Customs and Border Protection (CBP) Trusted Traveler programs who are flying on participating airlines to receive expedited screening benefits during domestic travel. For more information on TSA Pre✓™, visit http://www.tsa.gov/tsa-precheck.
[63] FAA categorizes airports into groups based on passenger flow. Category X airports have the greatest number of passenger traffic and Category IV airports have the least.

TSA reallocated millimeter units in some circumstances to replace the removed backscatter machines. TSA based the replacement of backscatter machines on equipment needs that best addressed security risks at the airport, the expansion of TSA Pre ✓™ lanes, checkpoint configurations, the passenger volume at airports and at specific checkpoint lanes, and throughput rates. For example, if TSA originally had deployed a backscatter unit in an underutilized checkpoint, TSA did not replace the backscatter unit with a millimeter unit. TSA reallocated millimeter units in checkpoints where throughput was low enough that they could continue screening with fewer AIT machines and replaced backscatter units in checkpoints with high throughput. In order to backfill the removed backscatter units, TSA reallocated 73 millimeter units and reprioritized deployment of 61 purchased millimeter machines in 2012 totaling 134 backfill millimeter units.

In addition to this policy change, deployment of AIT may change as airports expand or contract their operations or become federally regulated or are removed from the part 1542-regulated airports population due to changing economic conditions. All of this highlights the dynamic environment of airport security and the inherent uncertainty in forecasting specific numbers of AIT units at each airport, along with other estimates in projected years.

Table 13 shows AIT deployment over the ten-year period of analysis. TSA uses historical data of AIT machines deployed from 2008-2015 and projects the number of machines deployed for 2016-2017. The numbers of units have been revised since the NPRM as more data has become available since TSA published the NPRM. Due to this revision to the number of AIT units deployed, TSA also revised the number of in-service units throughout the period of analysis.

Table 13: AIT Units Deployed by Airport Category[64] [65] [66]

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	17	15	0	0	0	**32**
2009	1	3	0	0	0	**4**
2010	273	133	17	2	0	**425**
2011	3	44	21	11	0	**79**
2012	208	39	61	36	0	**344**
2013	35	32	3	1	0	**71**
2014	3	2	1	1	0	**7**
2015*	17	6	9	25	0	**57**
2016	0	0	0	0	0	**0**
2017	0	0	0	0	0	**0**

Source: TSA Office of Security Capabilities
* Projected AIT units use the current distribution to project deployment for each airport category. This leads to non-whole numbers as estimates and the total may not equal the sum due to rounding.

Before the decision to remove all backscatter units, TSA removed 73 backscatter units from Category X airports at the end of 2012 as part of its reallocation plan. At the end of May 2013, all remaining backscatter units were removed: 94 units in Category X, 68 in Category I, 8 in Category II, and 4 in Category III. For the purpose of this analysis, TSA assumes these 174 backscatter machines were simultaneously removed at the end of May 2013.

---

[64] Indicates initial deployment of AIT system.
[65] AITs may have been subsequently moved to another airport or a testing facility. Airport category may have also changed.
[66] Totals do not include AITs deployed to testing facilities, the TSA Academy at FLETC, or units located in warehouse awaiting deployment. AITs in testing capacities do not serve the purpose of this rule which is to screen passengers.

Table 14 shows the number of in-service AIT units at the end of each year given the removal of backscatter units and other reallocation of millimeter units.[67]

Table 14: Cumulative Number of AIT Units In-Service by Category of Airport[68] [69] [70]

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	17	15	0	0	0	**32**
2009	18	18	0	0	0	**36**
2010	292	150	17	2	0	**461**
2011	295	194	38	13	0	**540**
2012	501	233	101	49	0	**884**
2013*	394	212	103	14	0	**723**
2014**	393	227	95	14	0	**729**
2015	428	235	99	31	0	**793**
2016	428	235	99	31	0	**793**
2017	428	235	99	31	0	**793**

Source: TSA Office of Security Capabilities
* Includes 73 backscatter units removed at the end of 2012 in addition to the units deployed throughout 2013.
** Includes 174 backscatter units removed at the end May 2013.

Because the decision to remove all backscatter machines from airports affected the deployment timing in 2013, TSA uses a weighted average to generate costs in 2013 for utilities and personnel

---

[67] Given the dynamic nature of PSP, AIT units constantly move within airports, between airports, and between airports and TSA testing facilities and warehouses. This makes any snapshot count of AIT units incomplete.
[68] Indicates end of the calendar year location of AIT system.
[69] AITs may have been subsequently moved to another airport or a testing facility. Airport category may also have changed.
[70] The table represents the number of AITs in service at each year's end.

costs to reflect this mid-year change. The appendix in this document outlines the assumptions and calculations used to estimate the weighted average costs for 2013.

Throughput

TSA defines the passenger throughput rate as the number of passengers that a checkpoint configuration can process per hour. This time includes pat-downs and alarm resolutions of a given technology in the configuration. Current passenger throughput rates at TSA checkpoints average approximately 150 passengers per hour for modsets with one x-ray machine, and 300 passengers per hour in modsets with two x-ray machines. The WTMD can handle more passengers than AIT; however, the x-ray screening of carry-on baggage throughput constrains the overall screening process. AIT machines have a passenger throughput rate of approximately 115 per hour for AITs with IO, and 240 to 270 with AITs with ATR. However, as of mid-2013, TSA no longer uses AITs with IO in the screening operation. Before 2013, AITs with IO were co-located with a WTMD to maintain the throughput rate of x-ray machines. Because all AITs may not be able to handle throughput in a modset with two x-ray machines, TSA co-locates the AIT with a WTMD to maintain the current throughput rate of 300 passengers per hour.[71] Therefore, the changes to the passenger screening program brought on by AIT do not add additional wait time to the overall system. An AIT co-located with a WTMD does not reduce total throughput per hour as x-ray baggage screening operates at lower throughput rates. Passengers experience no additional wait time because passengers wait for the x-ray screening of their personal belongings after they go through an AIT unit or a WTMD regardless of which screening technology is used. While some anecdotal cases may exist of passengers enduring a longer wait time from AIT, some passengers experience time savings from AIT. For example, individuals with metal, medical implants — such as a pacemaker or a knee replacement — avoid a pat-down which would have been required if they had been screened by a WTMD. Overall, AIT does not add additional wait time to passenger screening program.

---

[71] AIT is able to detect both metallic and non-metallic potential threats on a passenger's body, unlike WTMDs which can only detect metallic potential threats. This means that AIT provides an increased level of security as compared to WTMDs. When an AIT is co-located with a WTMD, the primary screening technology remains AIT. WTMDs are used when a passenger opts out of AIT screening or for lane management during periods of high traffic. The selection of passengers that go through a WTMD instead of AIT is random so possible attackers will not be able to exploit the use of WTMDs in co-located modsets.

TSA uses historical data from PMIS to estimate the total passenger throughput at checkpoints for 2008-2014. To project throughput for 2015-2017, TSA applies the FAA forecasted annual growth for passenger enplanements for U.S. commercial air carriers (1.9 percent) to the 2014 PMIS throughput total.[72] Table 15 displays the throughput totals used in this analysis.

Table 15: Past and Estimated Passenger Throughput

Year	Passenger Throughput
2008	682,154,959[73]
2009	626,962,827
2010	637,849,358
2011	638,253,416
2012	637,184,921
2013	638,556,795
2014	649,171,699
2015*	661,505,961
2016*	674,074,575
2017*	686,881,991

Source: PMIS Database[74]
* Estimates in 2015-2017 reflect throughputs that are projected to occur.

[72] FAA, "FAA Aerospace Forecast FY 2015-2035". Table 5, Appendix D, Revenue Passenger Enplanements, System, Avg. Annual Growth 2014-24, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/2015_National_Forecast_Report.pdf
[73] In 2008, TSA had a policy to screen the TSOs every time they left the sterile area of the checkpoint which helps to explain why the 2008 total throughput is substantially higher than 2009.
[74] Some throughput estimates have changed slightly from the NPRM RIA because, for the final rule RIA, data was retrieved directly from PMIS.

Employment Costs

TSA's Office of Finance and Administration (OFA) estimates TSO personnel costs. TSA uses the historic fully-loaded Full Time Equivalent (FTE) annual compensation rate[75] for TSOs (inflated to 2014 dollars) to estimate the personnel cost of AIT. To arrive at a fully-loaded hourly compensation rate across the TSO population, TSA divides the annual FTE compensation by the standard 2,080 hours of full-time employment. Table 16 shows the hourly FTE assumptions used throughout the analysis.

Table 16: TSO FTE Annual and Hourly Compensation Rates[76] in 2014 dollars

Year	**Fully Loaded FTE Compensation** a	**Hourly FTE** b = a ÷ 2,080 hours
2008	$58,971	$28.35
2009	$61,525	$29.58
2010	$64,706	$31.11
2011	$64,219	$30.87
2012	$62,867	$30.22
2013	$62,291	$29.95
2014-2017	$60,986	$29.32

[75] "Fully-loaded compensation" includes wages and certain benefits such as other personnel compensation, award money, overtime pay, health (including dental, optometry, etc.) insurance, life insurance, retirement contribution, workers compensation, and transit benefits. For example, of the $60,986 in average compensation a TSO receives in 2014, only $37,290 of it comes from (non-overtime) wages.

[76] All wages are real wage rates based in 2014 dollars and may fluctuate year-to-year depending on whether escalation of wages keeps up with inflation, the makeup of the workforce in years of experience, and pay grade level.

Utilities Costs to Airports

Some airport operators incur costs from the additional utilities consumed by AIT machines. Likewise, TSA incurs additional costs from certain airport operators who receive a utilities costs reimbursement. Airport operator utilities costs increase from the deployment of AIT, regardless of the modset. Table 17 breaks down the cumulative number of AIT units in non-reimbursed airports.

Table 17: Cumulative AIT Units In-Service in Non-reimbursed Airports[77]

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	5	5	0	0	0	**10**
2009	4	8	0	0	0	**12**
2010	115	38	11	2	0	**166**
2011	114	52	20	13	0	**199**
2012	231	45	60	49	0	**385**
2013	146	52	66	14	0	**278**
2014	111	65	52	14	0	**242**
2015*	125	61	52	31	0	**269**
2016*	125	61	52	31	0	**269**
2017*	125	61	52	31	0	**269**

* Estimates in 2015-2017 reflect projected deployment.

[77] Historical deployment information as presented in the final rule has changed from the figures published in the NPRM. TSA no longer includes the 5 units used in testing centers for costs related to airports.

TSA uses the U.S. Energy Information Administration (EIA) to retrieve electricity prices for airports. TSA uses EIA's interactive online tool[78]—based on EIA databases supporting the following reports: Electric Power Monthly, DOE/EIA-0226; Electric Power Annual, DOE/EIA-0348; and the EIA Regional Short-Term Energy Model— to acquire historical and projected prices of electricity for 2008-2016 for the commercial sector. Because the EIA cites prices in nominal dollars, TSA uses the indexes in Table 11 to adjust the prices to 2014 dollars. TSA uses EIA's *Annual Energy Outlook 2015* to estimate the 2017 price of electricity in the commercial sector.[79] EIA reports the price of electricity for the commercial sector in 2013 as $29.70 per million British Thermal Units (BTUs) and projects the 2020 price to be $31.10 per million BTU. TSA calculates the CAGR between the 2013 and 2020 to be 0.66 percent.[80] TSA applies this annual rate to the 2016 price to forecast electricity price in 2017. Table 18 describes the process of calculating electricity prices for the commercial sector in 2014 dollars.

---

[78] EIA, "Short-Term Energy Outlook", Table 7c: U.S. Regional Electricity Prices (Cents per Kilowatthour), Annual Frequency, 2008-2016, Commercial Sector – U.S. Average, https://www.eia.gov/forecasts/steo/tables/?tableNumber=21#startcode=2008
[79] Table C3. Electricity price for the commercial sector. http://www.eia.gov/forecasts/aeo/pdf/0383(2015).pdf
[80] TSA uses CAGR with the 2013 price of $29.70 and 2020 price of $31.10 to estimate an annual growth rate of 0.66 percent. 0.66 percent = [(31.10 ÷ 29.70)^(1 ÷ 7 years)] -1.

Table 18: Prices of Electricity for Commercial Sector

Year	Cited Price	Source & Methodology	Price in $2014 per kWh
2008	$0.1026	Latest data available from EIA databases supporting the following reports: Electric Power Monthly, DOE/EIA-0226; Electric Power Annual, DOE/EIA-0348. Cited prices were adjusted to 2014 dollars using GDP deflator.	$0.1124
2009	$0.1016		$0.1104
2010	$0.1019		$0.1094
2011	$0.1023		$0.1076
2012	$0.1009		$0.1042
2013	$0.1026		$0.1042
2014	$0.1074		$0.1074
2015	$0.1062	EIA Regional Short-Term Energy Model.	$0.1062
2016	$0.1080		$0.1080
2017	N/A	Projection based on an estimated 0.66 percent compounded annual growth rate.[81] Growth rate was calculated based on electricity prices projected in 2020 in EIA's *Annual Energy Outlook 2015*.	$0.1087[82]

TSA uses the prices of electricity with the average electrical output per AIT machine for each airport category to calculate the utilities cost. According to TSA's OFA, AIT machines consume 1.02 kWh during operation and 0.70 kWh when idle. TSA calculates average energy consumption per AIT machine by using the operational-hours data in PMIS to calculate the

[81] TSA uses CAGR with the 2013 price of $29.70 and 2020 price of $31.10 to estimate an annual growth rate of 0.66 percent. 0.66 percent = [(31.10 ÷ 29.70)^(1 ÷ 7 years)] -1.
[82] $0.1087 = $0.1080 [price in 2016] × (1 + 0.66 percent).

average number of operation hours per AIT machine between 2008 and 2015.[83] TSA assumes the remainder of the time these AIT machines are idle and uses these average for this time period to estimate an average daily energy consumption by airport category. Table 19 below illustrates these calculations.

Table 19: Energy Consumption per AIT per day by Airport Category Code

Airport Category	Average Operational Hours per AIT per day for 2008-2015 a	Energy Consumption during Operation b	Average Idle Hours per AIT per day for 2008-2015 c = 24 –a	Energy Consumption During Idle d	Daily AIT Energy Consumption (kWh) per AIT e = (a × b) + (c × d)
X	9.4		14.6		19.80
I	8.0		16.0		19.37
II	5.8	1.02	18.2	0.70	18.64
III	6.1		17.9		18.76
IV	5.8		18.2		18.64

Note: Totals may not sum exactly due to rounding.

TSA combines the daily energy consumption rate with the distribution of AITs in-service (Table 14) for each airport category to calculate the number of kilowatts of electricity consumed each year by AIT machines. Table 20 below illustrates these calculations.

[83] 2015 is the only year in this window that is projected (not based on historical data).

Table 20: Annual Energy Consumption of AIT in Non-Reimbursed Airports in kilowatts

Year	Cumulative AIT Deployment at Non-Reimbursed Airports					Energy Consumed ∑ (AIT units by Airport Category x AIT Energy Consumption per day for Airport Category x 365.25 days)[84]
	X	I	II	III	IV	
2008	5	5	0	0	0	71,543
2009	4	8	0	0	0	85,540
2010	115	38	11	2	0	1,189,206
2011	114	52	20	13	0	1,417,717
2012	231	45	60	49	0	2,733,440
2013*	146	52	66	14	0	2,426,713*
2014	111	65	52	14	0	1,716,009
2015	125	61	52	31	0	1,903,943
2016	125	61	52	31	0	1,903,943
2017	125	61	52	31	0	1,903,943

*Estimates in 2013 reflect a weighted average based on the removal of backscatter units. (See the Appendix for details).

Table 21 illustrates how TSA calculates the cost of electricity for AIT using the electricity consumption and prices of electricity.

[84] For example, in 2010: (115 Cat X AITs × 19.80 kW + 38 Cat I AITs × 19.37 kW + 11 Cat II AITs × 18.64 kW + 2 Cat III AITs × 18.76 kW) × 365.25 days = 1,189,206 kW.

Table 21: AIT Utilities Cost

(in $ millions, undiscounted)

Year	Energy Consumption (kW) a	Electricity Price ($ per kWh) b	AIT Utilities Cost c = a x b ÷ $1 million
2008	71,543	$0.1124	$0.008
2009	85,540	$0.1104	$0.009
2010	1,189,206	$0.1094	$0.130
2011	1,417,717	$0.1076	$0.153
2012	2,733,440	$0.1042	$0.285
2013	2,426,713	$0.1042	$0.253
2014	1,716,009	$0.1074	$0.184
2015	1,903,943	$0.1062	$0.202
2016	1,903,943	$0.1080	$0.206
2017	1,903,943	$0.1087	$0.207

* Estimates in 2015-2017 reflect throughputs that are projected to occur.

To account for the net change in utilities costs, TSA subtracts the utilities costs of WTMDs that were removed because of AIT deployment, and then disposed, from AIT utilities costs. Unlike AIT, WTMD consumes the same rate of electricity when it is operational and idle at a rate of 0.04 kWh, or 350.64 kW per year.[85] TSA multiplies the number of WTMDs removed by the energy consumption rate and the price of electricity to estimate the cost of electricity from the removed WTMDs. Table 22 illustrates these costs.

[85] 350.64 kW = 0.04 kWh × 24 hours × 365.25 days.

Table 22: Removed WTMDs Utilities Cost

(in $ millions, undiscounted)

Year	**WTMDs Removed** a	**WTMD Annual Energy Consumption Rate** b	**Electricity Price ($ per kWh)** c	**WTMDs Utilities Cost** d = (a x b x c) ÷ 1 million
2008	0	350.64	$0.1124	$0.000
2009	0		$0.1104	$0.000
2010	0		$0.1094	$0.000
2011	0		$0.1076	$0.000
2012	35		$0.1042	$0.001
2013	48		$0.1042	$0.002
2014	54		$0.1074	$0.002
2015	61		$0.1062	$0.002
2016	61		$0.1080	$0.002
2017	61		$0.1087	$0.002

TSA estimates the utilities costs to industry by subtracting the utilities costs from the removed WTMDs from the additional utilities cost of AITs from 2008-2014 as approximately $1.02 million (undiscounted). Table 23 reports total costs from 2008-2014.

Table 23: Net Airport Utilities Costs from 2008-2014

(in $millions, undiscounted)

Year	**AIT Cost from Non-Reimbursed Airports** a	**Removed WTMD Costs from Non-Reimbursed Airports** b	**Net AIT Utility Costs** c = a – b
2008	$0.008	$0.000	$0.008
2009	$0.009	$0.000	$0.009
2010	$0.130	$0.000	$0.130
2011	$0.153	$0.000	$0.153
2012	$0.285	$0.001	$0.284
2013*	$0.253	$0.002	$0.251
2014	$0.184	$0.002	$0.182
Total			**$1.017**

Note: Totals may not sum exactly due to rounding.
*Estimates in 2013 reflect a weighted average based on the removal of backscatter units. (See the Appendix for details).

TSA projects the airport utilities costs to be approximately $0.61 million (undiscounted), $0.57 million discounted at three percent, and $0.53 million discounted at seven percent. Table 24 reports total costs from 2015-2017.

Table 24: Net Airport Utilities Costs from 2015-2017

(in $millions)

Year	**AIT Cost from Non-Reimbursed Airports** a	**Removed WTMD Cost from Non-Reimbursed Airports** b	**Net AIT Utility Costs** c = a – b
2015	$0.202	$0.002	$0.200
2016	$0.206	$0.002	$0.203
2017	$0.207	$0.002	$0.205
Total			**$0.608**
Discounted at 3%			**$0.573**
Discounted at 7%			**$0.532**

Note: Totals may not sum exactly due to rounding.

Passenger Opportunity Cost

A WTMD can handle higher throughput than an AIT machine. The x-ray screening of carry-on baggage, however, maintains a lower throughput rate than both WTMD and AIT and, thus, constrains the overall throughput rate of the screening process. Passenger-throughput rates at TSA checkpoints average approximately 150 passengers per hour for modsets with one x-ray machine, and 300 passengers per hour in modsets with two x-ray machines.[86] In a modset with one x-ray machine, one AIT, and one WTMD, the AIT unit maintains a higher throughput than the x-ray machine and therefore does not constrain the screening operation assuming that divestment protocols and procedures are followed. In a modset with two x-ray machines, TSA co-locates the AIT with a WTMD to maintain the throughput rate of 300 passengers per hour

[86] AIT machines currently have a passenger throughput rate of approximately 240 to 270 per hour.

because an AIT unit alone may not be able to handle this throughput. While some anecdotal cases may exist of passengers enduring a longer wait time from AIT, some passengers experience time savings from AIT. For example, individuals with metal, medical implants — such as a pacemaker or a knee replacement — avoid a pat-down which would have been required if they had been screened by a WTMD. As is the case for WTMDs, AIT can alarm for permitted, non-harmful items such as body piercings and certain clothing, shoes, and jewelry with a high metal content. TSA acknowledges and expects that travelers wish to avoid alarms for non-harmful items as such alarms can cause anxiety and discomfort to the traveler. TSA's website[87] presents some steps individuals can take to reduce the likelihood of triggering an alarm. Overall, the use of AIT does not add wait time to the passenger screening process.

Passengers generally may decline AIT and opt instead for a pat-down performed by a TSO. TSA conducts these pat-downs in the checkpoint area or in a private room. Only the small percentage of passengers opting out of AIT screening in favor of a pat-down experience increased wait times. TSA estimates the cost to these passengers by calculating the opportunity cost of a passenger's time. Opportunity cost measures the next best use of a resource, or, in this case, a passenger's time. The opportunity cost of a passenger's time measures the value of time that a passenger must forego from spending on other activities due to their increased time spent in a checkpoint area. TSA uses the Department of Transportation's (DOT) "Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis" to estimate an average opportunity cost of a passenger's time at $45.14 per hour (for an All Purposes traveler).[88] [89] TSA multiplies the opportunity cost of a passenger's time by the amount of time it takes for a passenger that opts out of AIT to go through a pat-down, which takes on average 150 seconds.

---

[87] https://www.tsa.gov/travel/frequently-asked-questions

[88] U.S. DOT, "Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis", Table 4, TSA uses the All Purpose hourly rate of $43.70 in 2012 dollars. In 2014 dollars, this equates to $45.14 per hour. https://www.transportation.gov/sites/dot.gov/files/docs/USDOT%20VOT%20Guidance%202014.pdf.

[89] TSA uses All Purpose hourly rate because AIT affects all travelers. The All Purpose value of travel time hourly rate is a weighted average of personal and business rates using data on the distribution of trip purpose.

TSA estimates that a passenger that opts out of AIT will incur an opportunity cost of $1.88 ($45.14 x 0.04167 hours).[90]

TSA estimates the number of passengers receiving a pat-down from historical data on passenger opt-out rates. In the NPRM, TSA assumed an opt-out rate of 1.8 percent each year. Since the NPRM was published, PMIS provided TSA with historical opt-out rates for 2009-2014 and TSA uses these values in this RIA. In 2008, TSA did not collect an opt-out rate and therefore uses the 2009 opt-out rate in 2008 because of its proximity in time, which means the AIT screening program would have had similar logistical factors as both years were in the initial phase of implementing AIT. For 2015-2017, TSA uses the historical average opt-out rate from 2009-2014 (0.78 percent). Additionally, for the projected AIT throughput for 2015-2017, TSA assumes that 42.37 percent of passenger throughput will go through the expedited screening process.[91] The expedited screening process generally uses WTMD as the primary screening technology. The remaining passengers are assumed to receive AIT screening.

To estimate the passenger population that opts out, TSA multiplies passenger throughput by the percentage of passengers who receive an AIT screening and by the opt-out rate in each year. TSA calculates the total opportunity cost of time by multiplying the total number of passengers who have opted out by the opportunity cost per pat-down. TSA estimates the passenger opportunity cost from 2008-2014 as $16.40 million (undiscounted). Table 25 reports the total costs from 2008-2014.

[90] TSA estimates 150 seconds for a pat-down based on field tests—70 seconds to wait for a same gender TSO and 80 seconds to perform the pat-down. The 150 second pat-down is equivalent to 0.04167 hours.
[91] This percentage was reported from TSA's Office of Security Operations from data collected from September 2015 to December 2015. This data collection coincides with the ending of certain managed inclusion programs that were aimed at diverting some passengers in standard line to expedited screening lines if the queue times at checkpoints become too great.

Table 25: Passenger Opportunity Costs from 2008-2014

(in $millions, undiscounted)

Year	**Number of Passenger Screenings per Year** a	**AIT Throughput Percent of Total Passengers** b	**Passenger Opt-Out Rate** c	**Number of Opt-Outs** d = a x b x c	**Total Cost for Opt-Outs** e = d x $1.88 ÷ 1 million
2008	682,154,959	0.10%	0.41%	2,816	$0.01
2009	626,962,827	0.45%	0.41%	11,695	$0.02
2010	637,849,358	4.01%	0.88%	225,018	$0.42
2011	638,253,416	21.10%	1.25%	1,687,317	$3.17
2012	637,184,921	45.79%	0.96%	2,807,793	$5.28
2013	638,556,795	56.04%	0.66%	2,365,163	$4.45
2014	649,171,699	48.14%	0.52%	1,619,360	$3.05
Total					**$16.40**

Note: Totals may not sum exactly due to rounding.

TSA projects the passenger opportunity cost from 2015-2017 as approximately $12.59 million (undiscounted), $11.87 million with three percent discounting, and $11.01 million with seven percent discounting. Table 26 reports the total costs from 2015-2017.

Table 26: Passenger Opportunity Costs from 2015-2017

(in $millions)

Year	**Number of Passenger Screenings per Year** a	**AIT Throughput Percent of Total Passengers** b	**Passenger Opt-Out Rate** c	**Number of Opt-Outs** d = a x b x c	**Total Cost for Opt-Outs** e = d x $1.88 ÷ 1 million
2015	661,505,961	42.37%	0.78%	2,189,855	$4.12
2016	674,074,575	42.37%	0.78%	2,231,463	$4.20
2017	686,881,991	42.37%	0.78%	2,273,860	$4.28
Total					**$12.59**
Discounted at 3%					**$11.87**
Discounted at 7%					**$11.01**

Note: Totals may not sum exactly due to rounding.

Discussion on Potential Distributional Effects of Screening

Every person and item must be screened before entering a secure area of the airport. AIT screening is an essential tool to help TSA detect both metallic and nonmetallic explosives and other dangerous items concealed under clothing. In the absence of alarms, AIT screening provides most passengers with the ability to avoid a physical screening – a benefit to passengers that have sensitivities to being touched. Similarly, passengers with metal implants or internal medical devices might experience time savings going through the AIT because they avoid alarm resolution from the WTMD – which may include physical screening. On the other hand, some passengers with physical disabilities or external medical devices may experience difficulty with AIT machines. Generally, passengers undergoing screening will have the opportunity to decline AIT screening in favor of physical screening. Travelers may request a private screening with a witness or companion of the traveler's choosing at any point in the screening process.

TSA recognizes that some travelers may have other concerns with the screening. For example, the transgender community has expressed privacy concerns related to screening transgender individuals. A transgender person will be screened as he or she presents at the security checkpoint. The AIT used to screen passengers has software that looks at male and female anatomy differently. AIT displays potential threats, however, on a screen showing a generic outline of a person – which is the same for all passengers. As previously noted, travelers may request a private screening with a witness or companion of the traveler's choosing at any point in the screening process. TSA recognizes the concerns of the transgender community and has worked with the community to improve the screening experience for these individuals. In addition, TSA is enhancing its training regarding the screening of transgender individuals to ensure that screening is conducted in a dignified and respectful manner.

Similarly, some passengers may be concerned about the screening of passengers wearing certain clothing and head coverings, including religious head coverings. Under TSA's standard procedures, passengers wearing head coverings or loose fitting or bulky clothing may be required to undergo additional screening, which may include physical screening. Persons wearing any type of head covering may be subject to additional screening of the head covering if the security screener cannot reasonably determine that the head area is free of a threat item.[92] If it is necessary to remove the head covering, the passenger may request to remove it in a private screening area. All employees are required to take religious and cultural awareness training, which includes awareness and sensitivities concerning certain types of head coverings.

Personnel Cost to TSA

TSA incurs a cost for additional labor hours dedicated to operate AIT machines. TSA estimates this cost using assumptions from TSA's Screener Allocation Model (SAM), which dictates the allocation of personnel to each airport, and the hours of operation as recorded in PMIS. The SAM estimates a personnel staffing level of 3.5 TSOs per lane for lanes with one WTMD. For lanes with a WTMD and an AIT with IO unit, the SAM estimates a 5.0 personnel staffing level. All AIT machines before 2012 were equipped with IOs. For lanes with a WTMD and an AIT with ATR unit, the SAM estimates a 4.5 personnel staffing level. Therefore, TSA estimates a personnel difference of 1.5 TSOs per lane for lanes with AIT with IO (5 – 3.5) and 1.0 TSO per lane for those with AIT with ATR (4.5 – 3.5). In 2012, all millimeter units switched to ATR software while backscatter units continued to use IO technology until they were removed from airports in 2013.

TSA uses PMIS data to estimate the number of operational hours per AIT unit for 2009-2014. For 2015-2017, TSA applies the average number operational hours per AIT from the last historical year (2014). For 2008, TSA assumes the same average number of hours as in 2009 because of the proximity in time between these years, making it likely that both years would have had similar logistical issues related to the initial phase of AIT implementation.

To estimate personnel costs from AIT, TSA multiplies the personnel difference estimate by the number of hours an AIT is in operation by the weighted average fully-loaded compensation rate of a TSO (estimated in Table 16) and by the number of AIT-covered checkpoint lanes. Table 27 shows the average number of operational hours per AIT unit in each year.

---

[92] http://www.tsa.gov/travel/frequently-asked-questions

Table 27: Calculation of Average Hours per AIT Annually

Year	AIT Units In Service a	Total AIT Operational Hours b	Hours Per AIT c = b ÷ a
2008*	32	N/A	4,388
2009	36	157,971	4,388
2010	461	714,268	1,549
2011	540	2,549,784	4,722
2012	884	3,759,569	4,253
2013**	622	2,881,842	4,637
2014	729	2,613,135	3,585
2015***	793	2,842,546	3,585
2016***	793	2,842,546	3,585
2017***	793	2,842,546	3,585

* In the absence of data, TSA uses 2009 data for 2008 in calculating average operational hours per AIT annually.
** TSA uses a weighted average to account for the mid-year backscatter reallocation. See Appendix for details.
*** Estimates in 2015-2017 reflect throughputs that are projected to occur.

Along with personnel difference and hours of operation, TSA bases its cost estimate for additional personnel on the number of checkpoint lanes covered by AIT units. AIT units may be placed in a 1:1 or 2:1 modset. A 1:1 modset has one lane dedicated to one AIT machine and one x-ray screening machine. A 2:1 modset has two lanes dedicated to one AIT machine and two x-ray screening machines – most AIT units are in 2:1 modsets with a WTMD. AIT units may switch from a 1:1 or 2:1 modset in any given time in order to meet the specific throughput needs of an airport. To calculate the cumulative number of lanes, TSA took a snapshot picture in 2012 of the percentage of AITs in each modset which is presented in Table 28. Table 28 also demonstrates the calculation of average number of lanes per AIT for each category of airport.

Table 28: AIT Modsets and Lanes

Category	Percentage of AIT Modset 1:1 a	Percentage of AIT Modset 2:1 b	Avg. Lanes per AIT c = (a x 1) + (b x 2)
X	29%	71%	1.71
I	27%	73%	1.73
II	25%	75%	1.75
III	74%	26%	1.26
IV	99%	1%	1.01

TSA uses the average lanes per AIT with the number of AITs in-service (Table 14) to calculate the number of cumulative lanes in each year. For example, in 2008, TSA estimates a total number of 55 lanes were covered in 2008.[93]

Table 29 presents the cost TSA incurs for the period of 2008-2014 for the additional labor hours necessary to operate and screen passengers with AIT machines. TSA estimates the cost of personnel from 2008-2014 to be $830.09 million (undiscounted).

[93] 55 lanes = (17 AITs in Cat X x 1.71) + (15 AITs in Cat I x 1.73) + (0 AITs in Cat II x 1.75) + (0 AITs in Cat III x 1.26) + (0 AITs in Cat IV x 1.01).

Table 29: Personnel Costs from 2008-2014

(in $millions, undiscounted)

Year	Lanes with IO	Hours for IO		Lanes with ATR	Hours for ATR		Total Hours	Hourly Compensation	Total
	a	b = a x Avg Hrs per AIT	c = b x 1.5 TSO per lane	d	e = d x Avg Hrs per AIT	f = e x 1 TSO per lane	g = c + f	h	i = g x h ÷ 1 million
2008	55	241,416	362,124	0	0	0	362,124	$28.35	$10.27
2009	62	271,681	407,521	0	0	0	407,521	$29.58	$12.05
2010	791	1,225,786	1,838,678	0	0	0	1,838,678	$31.11	$57.20
2011	923	4,357,958	6,536,937	0	0	0	6,536,937	$30.87	$201.83
2012	422	1,796,074	2,694,111	1,076	4,576,553	4,576,553	7,270,664	$30.22	$219.75
2013*	124	574,624	861,936	1,238	5,741,952	5,741,952	6,603,888	$29.95	$197.77
2014	0	0	0	1,249	4,475,487	4,475,487	4,475,487	$29.32	$131.22
Total									**$830.09**

Note: Totals may not sum exactly due to rounding.
*Estimates in 2013 reflect a weighted average based on the removal of Backscatter units. (See the Appendix for details).

Table 30 present costs of personnel from 2015-2017 to be $425.89 million (undiscounted), $401.55 million with three percent discounting and $372.55 million with seven percent discounting.

Table 30: Personnel Costs from 2015-2017

(in $millions)

Year	**Lanes with ATR**	**Hours for ATR**		**Hourly Compensation**	**Total**
	a	b = a x Avg Hrs per AIT	c = b x 1 TSO per lane	d	e = c x d ÷ 1 million
2015	1,351	4,841,773	4,841,773	$29.32	$141.96
2016	1,351	4,841,773	4,841,773	$29.32	$141.96
2017	1,351	4,841,773	4,841,773	$29.32	$141.96
Total					**$425.89**
Discounted at 3%					**$401.55**
Discounted at 7%					**$372.55**

Note: Totals may not sum exactly due to rounding.

Training Cost to TSA

TSA incurs costs to train TSOs to operate and effectively screen passengers with AIT machines. TSOs take several training courses—some initial and some recurring—on AIT operation and screening. TSA bases its training cost estimates on the number of employees who participated in each course as reported by TSA's Office of Training and Development (OTD). TSA based training cost estimates in this analysis on the data provided by OTD.

TSOs participated in seven different training courses from 2008-2013. These courses train TSOs on all standard operating procedures and capabilities, including the handling of certain groups who may experience disparate burdens from AIT (see *Discussion on Potential Distributional Effects of Screening* subsection on page 67 for more information about these individuals). The courses include (each course's duration is in parentheses):

- Original AIT training (16 hours)
- Standards training (0.25 hours)
- Standard Operating Procedure (SOP) Revision training (0.5 hours)
- Initial AIT with IO training (27 hours)
- Training to transfer from AIT with IO to AIT with ATR (at airports where AIT with IO was deployed prior to ATR development but later upgraded to ATR software) (4 hours)
- Initial AIT with ATR training (8 hours)
- Recurrent AIT training (3.5 hours)
- Mission Essential: Threat Mitigations (10 hours)

TSA uses SMEs from OTD to estimate the future composition of training and project the number of employees that will participate in training. By 2014, TSA discontinued Original AIT Training, Standards Training, AIT w/ IO Training, and IO to ATR Training and therefore TSA projects no TSOs to participate in these courses past 2013. In 2015, TSA developed and implemented the Mission Essential: Threat Mitigations (ME:TM) training. To project training participation in future years, TSA uses information provided by SMEs from OTD to make assumptions about the future of AIT training.

TSA estimates the number of TSOs participating in SOP Revision Training in projected years based on the number of TSOs operating AIT machines. TSA estimates personnel participating in SOP Revision Training in 2014-2017 by dividing the total number of operational AIT hours (found in Personnel Costs) for those respective years and dividing it by the average number of hours a TSO works annually (1,885 hours).[94] For AIT w/ATR Training, TSA examined the number of personnel that participated in historical years (2008-2014) and selected the number with the highest participation (46,806 TSOs in 2012) as its proxy estimate for projected years. Given the lack of data, we select this number as a conservative estimate for projected participation. It is likely to be greater than the actual participation due to the fact that TSA

[94] TSA estimates that TSOs, on average, work 1,885 hours annually. This is based on financial records from the Office of Finance and includes all hours worked for full-time and part-time TSOs. To estimate number of personnel who take the Standards training course in 2014, TSA divides the 5,343,800 operational AIT hours in 2014 by 1,885 to estimate that at least 2,835 TSOs are operating AITs. TSA assumes these personnel are taking the Standards course. This same methodology is used for 2015-2017.

deploys significantly less AIT machines in 2015-2017 than were deployed in 2012. For Recurrent Training, TSA assumes that all of the TSOs who took Recurrent Training in 2013, in addition to all the TSOs who took AIT w/ IO, IO to ATR, and AIT w/ ATR courses in 2013, will take Recurrent Training in 2014.[95] For 2015-2017, TSA uses this same method to calculate Recurrent and ME:TM training costs using TSOs who participated in training from the previous year. Lastly, OTD informed TSA of future changes in training requirements. Based on this information, TSA increases the duration for SOP Revision Training from 0.5 hours to 2 hours and decreases duration for Recurrent Training from 3.5 hours to 0.5 hours in 2015-2017.

In 2015, TSA developed a new training effort, the ME:TM training, which incorporates information specific to the capabilities and limitations of the AIT machine and related those limitations to the purpose of the SOPs, and the need for consistency and vigilance in implementation of the SOPs. This new development is incorporated into the new hire training curriculum and covers the most current policies and procedures. For the development of this program, it took 12 TSA managers three weeks to create the training program. TSA estimates their fully-loaded wage rate to be $84.90 per hour[96] which results in a cost of $122,252.[97] TSA also had 50 of their academy instructors trained on the new training effort for three weeks. TSA uses the fully-loaded wage rate of an average TSO of $29.32 per hour to estimate a cost of $175,921.[98] Lastly, TSA trained 1,000 field instructors on the new training effort for two days. TSA uses the fully loaded wage rate of an average TSO to estimate a cost of $469,123.[99] TSA sums these different cost components to estimate a one-time training development cost of $767,296 in 2015.

---

[95] In 2013, 33,014 TSOs participated in Recurrent training, 2,370 TSOs participated in AIT w/ IO training, 8,678 TSOs participated in IO to ATR training, and 33,144 TSOs participated in AIT w/ ATR training. Therefore, TSA assumed 77,206 TSOs (33,014 + 2,370 + 8,678 + 33,144) participate in Recurrent training in 2014. This same methodology is used for 2015.
[96] Fully-loaded wage rate is in 2014 dollars and based on projected outlays from TSA's Office of Finance and Administration. Wage is rate is based on a GS-15 level employee and includes wages, benefits, retirement contribution, bonuses, and transit benefits.
[97] $122,252 = $84.90 per hour × 12 managers × 120 hours.
[98] $175,921 = $29.32 per hour × 50 academy instructors × 120 hours.
[99] $469,123 = $29.32 per hour × 1,000 field instructors × 16 hours.

Table 31 and Table 32 present the number of personnel that participated in each course for each year.[100] TSA calculates the total training cost by multiplying the number of personnel by the number of hours in each year. Column A is the sum of all of the total training hours dedicated by TSOs in each year. TSA multiplies this sum by the average TSO compensation rate to calculate total training costs for each year.

[100] 2014 and 2015 are projected. All other years are based on historical data.

Table 31: Training Costs from 2008-2014

(in $millions, undiscounted)

Year	Original AIT Training		Standards Training		SOP Revision Training		Initial AIT w/ IO Training		IO to ATR Training		Initial AIT w/ ATR Training		Recurrent Training		Total Training Hours	Comp Rates ($)	Total Cost
	Personnel	Hours	Personnel	Hours	Personnel	Hours	Personnel	Hours	Personnel	Hours	Personnel	Hours	Personnel	Hours	a = ∑ (Personnel x Hours)	b	c = a x b ÷ 1 million
2008	0		0		0		1		0		0		0		27	$28.35	$0.00
2009	733		6		0		282		0		0		0		19,344	$29.58	$0.57
2010	1,768		13,518		2,521		38,824		1		7		0		1,081,236	$31.11	$33.64
2011	14	16	15,983	0.25	27,599	0.5	62,581	27	441	4	17,336	8	0	3.5	1,848,158	$30.87	$57.06
2012	0		3,631		2,957		14,141		1,368		46,806		1,988		771,071	$30.22	$23.31
2013	0		648		601		2,370		8,678		33,144		33,014		479,866	$29.95	$14.37
2014	0		0		2,375		0		0		18,144		77,206		416,560	$29.32	$12.21
Total																	**$141.16**

Source: TSA Office of Training and Development (OTD).
Note: Totals may not sum exactly due to rounding

Table 32: Training Costs from 2015-2017

(in $millions)

Year	SOP Revision Training		Initial AIT w/ ATR Training		Recurrent Training		ME:TM Training		Total Training Hours	Comp Rates ($)	Develop-ment Costs	Total Cost
	Personnel	Hours	Personnel	Hours	Personnel	Hours	Personnel	Hours	a = ∑ (Personnel x Hours)	b	c	d = (a x b + c) ÷ 1 million
2015	2,569		46,806		95,350		95,350		1,380,761	$29.32	$767,296	$41.25
2016	2,569	2	46,806	8	142,156	0.5	142,156	10	1,872,224	$29.32		$54.89
2017	2,569		46,806		188,962		188,962		2,363,687	$29.32		$69.30
Total												**$165.45**
Discounted at 3%												**$155.22**
Discounted at 7%												**$143.07**

Source: TSA Office of Training and Development (OTD).
Note: Totals may not sum exactly due to rounding

AIT Life Cycle Cost to TSA

To estimate the equipment life cycle cost of AIT, TSA divides the cost components into four categories: acquisition, installation, integration, and disposal; maintenance; test and evaluation; and program management office (PMO) costs.

TSA's OSC manages the PSP which includes several technologies. This creates difficulties for TSA in estimating a life cycle cost of a single technology because many of the costs to test, evaluate, maintain, and manage the technologies occur through private contracts covering the suite of technologies. OSC developed LCCEs for the PSP in 2011 and 2012, which—along with SME input—serves as the basis for equipment costs in 2008-2013.[101] [102] In 2014, OSC developed a project-specific LCCE for FY2014-FY2026.[103] TSA bases cost estimates in 2014-2017 on the more recent LCCE but kept the categorization of costs from previous years.

TSA needs to make assumptions on the proportion of contract funds dedicated to AIT implementation. The most recent LCCE reports that the percentage of all AIT technology costs relative to the total cost of the PSP from FY2014-FY2026 is approximately 14.99 percent.[104] TSA applies this percentage when allocating the program level cost to AIT from a PSP cost estimate in lieu of specific information. Because the 2014 LCCE is more comprehensive than its predecessor, TSA uses this percentage in all years of the analysis (2008-2017).[105]

In 2013, TSA removed all backscatter units from its checkpoints in order to meet the statutory requirement to use only AIT equipped with ATR to conduct passenger screening. TSA accounts for the removal of all 247 backscatter units by the end of May 2013. To ensure that these airports continue to screen passengers with AIT, TSA reallocated 73 units and reprioritized the

---

[101] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program". November 22, 2011, Version 2.7. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[102] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" June 22, 2012, Version 3.8. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[103] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. The LCCE was project-specific, or in other words, organized its costs by the type of technology in the PSP. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[104] In the PSP program, TSA dedicates 14.99 percent of total costs to AIT from FY2014-FY2026 ($395,555,080 AIT cost / $2,639,126,340 total cost).
[105] TSA uses this methodology because the previous LCCE in 2012 did not have a detailed breakdown of costs by screening technology and no similar ratio could be reproduced.

deployment of 61 millimeter machines purchased in 2012.[106] These 134 millimeter units backfill the need created by the removal of the backscatter machines. Throughout this section, TSA illustrates how changes in the deployment of AIT and the removal of backscatter machines affected the equipment costs of AIT.

Acquisition, Installation, Integration, and Disposal

To estimate the acquisition cost of new AIT units in historical years (2008-2013), TSA uses market prices as reported by SMEs for the millimeter unit and the backscatter unit of $155,696 and $167,268, respectively. Once an AIT unit is acquired, TSA incurs installation costs to place it at the screening checkpoint and synergize it with the rest of the passenger screening technologies in its modset. SMEs from OSC estimate the installation cost for the millimeter and backscatter technology as $5,733 and $2,525 per unit,[107] respectively. Next, TSA incurs integration costs per AIT unit, which is the cost of removing the existing technology from its current location and reconfiguring a modset to the new technology. SMEs from OSC estimate the cost of integration at $31,560 per unit, regardless of the manufacturer.[108] Integration costs do not include the cost of disposal for WTMDs. In addition to the WTMDs removed due to the installation of new AIT units, 247 backscatter units were removed from airports in 2012 and 2013. Both TSA and industry incurred costs from the removal of these units. TSA removed 73 of the 247 backscatter units at the end of 2012 prior to the statutory requirement to use only AIT equipped with ATR to screen passengers.[109] TSA assumed a per-unit cost of $10,941 to remove a backscatter machine from the airport and incurs a cost of $0.80 million.[110] Because these costs also capture the removal of technology, TSA includes it with the integration costs associated with AIT deployment in 2012.

---

[106] TSA purchased the 61 reprioritized units in 2012 but were not deployed until 2013 to check points that had lost or were about to lose their backscatter units.
[107] Both estimates are based on rates provided by two individual contractors, These two unit costs are different likely from many factors, ranging from specifics on their product, to their own internal cost factors (e.g., labor rates), to other characteristics known only by that company.
[108] The cost of reallocation depends on the current configuration of the passenger screening environment; TSA uses the $31,560 estimate as a conservative cost estimate as most reallocations cost less than $30,000.
[109] The total units of removed AITs have been scaled down from the figure published in the NPRM to coincide with the revised estimate of total backscatter units in the final rule.
[110] TSA bases the $10,941 removal cost on TSA's Office of Security Capabilities cost estimate assuming an $8,416 removal cost, a $2,314 shipping cost and a $210 warehouse rigging cost, as shown in Table 39.

Disposal costs capture the cost of disposing WTMDs which are no longer going to be used for airport screening. TSA does this when the surface area of the passenger lane constrains the modset to one technology. TSA estimates that 56 WTMDs are disposed of in 2012 and 20 in 2013. TSA estimates the additional cost of a WTMD disposal at $585 per unit which results in disposal costs of $32,769 (56 x $585) in 2012 and $11,703 (20 x $585) in 2013.[111]

For estimating lifecycle costs in 2014, TSA relied on SME input. Starting in 2014, TSA is expected to acquire next-generation AIT machines (AIT-2), which have a per-unit price of $263,729 in 2014.[112] The next-generation AIT machines are smaller in height and diameter and weigh less than the first- generation AIT machines. TSA tests the next-generation AITs to the same detection standards and use the same millimeter wave technology as the first-generation machines. For WTMD disposal in 2014, TSA reports these costs to be $17,640.[113]

In Table 33, TSA estimates the costs of acquisition, installation, integration, and disposal for historical years (2008-2014) as $195.32 million (undiscounted).

---

[111] TSA accounts for the removal of the WTMDs through the AIT reallocation cost; however the physical disposal is not captured in the reallocation cost.
[112] TSA bases the AIT-2 per-unit cost on SME input instead of the March 2014 LCCE. This is because of the dynamic nature of AIT and the PSP, which led to revisions to projected procurement quantity and unit prices since the completion of the LCCE in early 2014.
[113] The 2014 LCCE reports these costs as $0 in FY2014 and $69,450 in FY2015. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. These costs, expressed in 2013 dollars, were then inflated to 2014 dollars.

Table 33: TSA Acquisition, Installation, Integration, and Disposal Costs from 2008-2014 (in $millions, undiscounted)

Year	Millimeter Deploy-ment a	Backscatter Deploy-ment b	Millimeter Delayed Deploy-ment[114] c	Acquisition Cost d = [(a x $155,696 + b x $167,268] ÷ 1 million	Installation Cost e = [(a – c_{+1}[115] + c) x $5,733 + b x $2,525] ÷ 1 million	Integration Cost[116] f=[(a + b – c_{+1} + c) x $31,560] ÷ 1 million	Disposal Cost g = (disposed WTMDs x $585) ÷ 1 million	Total Cost h = d + e + f + g
2008	28	0	0	$4.36	$0.16	$0.88	$0.00	$5.40
2009	3	0	0	$0.47	$0.02	$0.09	$0.00	$0.58
2010	208	247	0	$73.70	$1.82	$14.36	$0.00	$89.88
2011	78	0	0	$12.14	$0.45	$2.46	$0.00	$15.05
2012	352	0	0	$54.80	$1.67	$9.98	$0.03	$66.49
2013	70	0	61	$10.90	$0.75	$4.13	$0.01	$15.80
2014*	7	0	0	$1.85	$0.04	$0.22	$0.02	$2.12
Total								**$195.32**

Note: Totals may not sum exactly due to rounding.
* Costs from 2014 differ from 2008-2013 and do not follow the formulas in the table header (except for installation and integration costs). See the section before the table for details on the cost for 2014.

In the years 2015-2017, TSA is expected to acquire next-generation AIT machines (AIT-2), which have a per-unit price of $117,508 in 2015.[117] The next-generation AIT machines are

[114] 351 AIT machines are procured in 2012, but 61 have their deployment delayed to 2013 to replace reallocated backscatter machines. These 61 machines incur acquisition costs in 2012, but incur installation and integration in costs in 2013.
[115] c_{+1} denotes the value in the "c" in the next year. For example, c_{+1} in the year 2012 is 61.
[116] In 2012, Integration Costs include $0.80 million from the removal of 73 backscatter machines in addition to the typical integration costs associated with AIT ($9.18 million).
[117] TSA bases the AIT-2 per-unit cost on SME testimony instead of the March 2014 LCCE. This is because of the dynamic nature of AIT and the PSP, which led to revisions to projected procurement quantity and unit prices since the completion of the

smaller in height and diameter and weigh less than the first- generation AIT machines. TSA tests the next-generation AITs to the same detection standards and use the same millimeter wave technology as the first-generation machines. TSA does not expect to procure any additional AIT units in 2016 or 2017; and, therefore, no acquisition, installation, or integration costs occur. For WTMD disposal costs in 2015-2017, TSA assigns the WTMD disposal costs from the 2014 LCCE, which reports these costs to be $59,299 in 2015; $25,875 in 2016; and $22,840 in 2017.[118]

In Table 34, TSA estimates the cost of acquisition, installation, integration, and disposal for projected years 2015-2017 as $8.93 million (undiscounted), $8.67 million with three percent discounting, and $8.34 million with seven percent discounting.

Table 34: TSA Acquisition, Installation, Integration, and Disposal Costs from 2015-2017 (in $millions)

Year	Millimeter Deployment a	Acquisition Cost b = a x $117,508 ÷ 1 million	Installation Cost c = a x $5,733 ÷ 1 million	Integration Cost d = a x $31,560 ÷ 1 million	Disposal Cost e	Total Cost f = b + c + d + e
2015	57	$6.70	$0.33	$1.80	$0.06	$8.88
2016	0	$0.00	$0.00	$0.00	$0.03	$0.03
2017	0	$0.00	$0.00	$0.00	$0.02	$0.02
Total						**$8.93**
Discounted at 3%						**$8.67**
Discounted at 7%						**$8.34**

Note: Totals may not sum exactly due to rounding.

LCCE in early 2014. As of the completion of this document, TSA plans on ordering 53 units, 3 for testing and 50 for deployment between 2014 and 2015.

[118] The 2015 LCCE reports these costs as $0 in FY2014, $69,450 in FY2015, and $25,110 in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2015 includes the second, third, and fourth quarter of FY2015; and the first quarter of FY2016. This cost, expressed in 2013 dollars, is then inflated to 2014 dollars. This same methodology is used to calculate calendar year costs for 2016 and 2017. These costs, expressed in 2013 dollars, were then inflated to 2014 dollars.

Maintenance

TSA divides maintenance costs into three subcategories: project-specific maintenance, non-project-specific investments, and non-project-specific maintenance. TSA estimates these costs separately for each year of the analysis period. Project-specific maintenance costs directly tie to maintenance expenditures for AIT units. TSA estimates the maintenance expenditures of AIT based on out-of-warranty maintenance (OOWM), call center services, and general maintenance support services. Additionally, the acquisition price of AIT includes a 2-year warranty, thus maintenance costs occur between 2010 and 2015 for units acquired in 2008-2013. TSA used the estimated per-unit OOWM cost for an AIT machine reported in the 2011 LCCE of $19,504 per year.[119] To calculate project-specific maintenance for 2008-2013, TSA multiplies the per-unit cost by the active number of out-of-warranty AIT units per year.

Non-project-specific investments include investments made to the maintenance infrastructure of PSP technologies. For example, these include a ticketing call center and general maintenance support services.[120] The call center covers the maintenance requests, while the general maintenance support services manage all maintenance-related projects, including day-to-day logistics. To estimate the portion of the cost attributable to AIT in historical years, TSA scales the total investment in maintenance cost to the percentage of AIT-specific costs relative to the total overall cost of PSP, estimated as 14.99 percent from the 2014 LCCE. TSA uses this percentage to estimate non-project-specific investments for 2008-2013 which is estimated to be $12.22 million annually (14.99 percent x $81.54 million as reported in the 2012 LCCE[121]).

TSA categorizes other maintenance costs as non-project-specific maintenance costs, which encompass general support services. TSA scales the total cost to determine the cost attributable

---

[119] Siemens – HSTS04 – 09 – C – CT3173 contract supports the out-of-warranty maintenance with an estimated $17,943 per-unit cost (inflated from 2009 dollars to 2014 dollars to $19,504 per-unit).

[120] These services, as a part of the larger PSP, existed before and after the onset of AIT. TSA estimates a constant cost for these services each year since the contract remained unchanged by AIT and thus independent of the AIT units deployed.

[121] Siemens – HSTS04 – 09 – C – CT3173 contract supports the Ticketing Call Center with an estimated $78,933,640 (inflated from 2012 dollars to 2014 dollars to $81,538,450).

to AIT. TSA estimates historical costs in 2008-2013, to be $3.91 million annually (14.99 percent x $26.06 million).[122]

For 2014, TSA uses the AIT-specific maintenance costs from the most recent LCCE of $11.92 million in 2014.[123] For non-project-specific investment, TSA uses the percentage of AIT costs compared to all PSP technologies directly from the most recent LCCE —21.14 percent in 2014—and applies these percentages to the total non-project-specific investment from the 2014 LCCE to calculate AIT's share to be $16.17 million (21.14 percent x $76.48 million) in 2014.[124] To estimate costs of non-project-specific maintenance, TSA bases its estimates directly from the most recent LCCE and scales the total non-project-specific maintenance for PSP relative to AIT using the same percentage for the individual year which TSA calculates this cost to be $1.94 million (21.14 percent x $9.19 million) for 2014.[125]

TSA estimates the cost of project-specific maintenance, non-project-specific investment, and non-project-specific maintenance from 2008-2014 as approximately $143.61 million (undiscounted). Table 35 presents these costs.

[122] Logical Essence – HSTS04 – 09 – C – CT3101 ($5,853,197.66) and GST – Task Order 2 – HSTS04 – 10 – J – CT305 ($19,378,042) provide general support services to a total of $25,231,240 (inflated from 2012 dollars to 2014 dollars to $26,063,871).

[123] The 2014 LCCE reports these costs as $11.64 million in FY2014, $12.75 million in FY2015, and $13.91 million in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. This cost, expressed in 2013 dollars, is then inflated to 2014 dollars. The same method is used for 2015, 2016, and 2017.

[124] The 2014 LCCE non-project-specific investment costs as $83.30 million in FY2014, $59.28 million in FY2015, and $55.12 million in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. Calendar year 2015 includes the second, third, and fourth quarter of FY2015; and the first quarter of FY2016. This cost, expressed in 2013 dollars, is then inflated to 2014 dollars.

[125] The 2014 LCCE non-project-specific maintenance costs as $9.27 million in FY2014, $8.95 million in FY2015, and $8.79 million in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. Calendar year 2015 includes the second, third, and fourth quarter of FY2015; and the first quarter of FY2016. This cost, expressed in 2013 dollars, is then inflated to 2014 dollars.

Table 35: Maintenance Costs from 2008-2014

(in $millions, undiscounted)

Year	**Cumulative Units** a	**Project Specific Maintenance** b = a x $19,504 ÷ 1 million	**Non-project Specific Investment** c = $12,221,070 ÷ 1 million	**Non-project Specific Maintenance** d = $3,906,481 ÷ 1 million	**Total** e = b + c + d
2008	0	$0.00	$12.22	$3.91	$16.13
2009	0	$0.00	$12.22	$3.91	$16.13
2010	28	$0.55	$12.22	$3.91	$16.67
2011	31	$0.60	$12.22	$3.91	$16.73
2012	486	$9.48	$12.22	$3.91	$25.61
2013	317	$6.18	$12.22	$3.91	$22.31
2014*	N/A	$11.92	$16.17	$1.94	$30.03
Total					**$143.61**

Note: Totals may not sum exactly due to rounding.
* Costs from 2014 differ from 2008-2013 and do not follow the formulas in the table header. See the section before the table for details on the cost for 2014.

To estimate the AIT-specific maintenance costs for 2015-2017, TSA uses the AIT-specific maintenance costs from the most recent LCCE of $13.04 million in 2015, $14.61 million in 2016, and $16.78 million in 2017. For non-project-specific investment for 2015-2017, TSA uses the percentage of AIT costs compared to all PSP technologies directly from the most recent LCCE —28.79 percent in 2015, 13.16 percent in 2016, and 13.45 percent in 2017—and applies these percentages to the total non-project-specific investment from the 2014 LCCE to calculate AIT's share to be $16.36 million (28.79 percent x $56.81 million) in 2015, $6.71 million (13.16 percent x $50.95 million), and $5.93 million (13.45 percent x $44.11 million). To estimate costs of non-project-specific maintenance for 2015-2017, TSA bases its estimates directly from the most recent LCCE and scales the total non-project-specific maintenance for PSP relative to AIT using the same percentage for the individual year. TSA calculates this cost to be $2.56 million

(28.79 percent x $8.91 million) for 2015; $1.15 million (13.16 percent x $8.77 million) for 2016; and $1.14 million (13.45 percent x $8.49 million) for 2017.

TSA estimates the cost of project-specific maintenance, non-project-specific investment, and non-project-specific maintenance from 2015-2017 at approximately $78.27 million (undiscounted), $74.03 million with three percent discounting, and $68.96 million with seven percent discounting. Table 36 presents maintenance costs for years 2015-2017.

Table 36: Maintenance Costs from 2015-2017

(in $millions)

Year	Project Specific Maintenance a	Non-project Specific Investment b	Non-project Specific Maintenance c	Total d = a + b + c
2015	$13.04	$16.36	$2.56	$31.96
2016	$14.61	$6.71	$1.15	$22.47
2017	$16.78	$5.93	$1.14	$23.85
Total				**$78.27**
Discounted at 3%				**$74.03**
Discounted at 7%				**$68.96**

Note: Totals may not sum exactly due to rounding.

Test and Evaluation

Before any new technology enters the field, TSA performs several stages of testing and evaluation. This section outlines these stages of testing and evaluation, from before procurement to final deployment.

In the initial stage, TSA performs a qualification test and evaluation (QT&E). At this critical stage, QT&E evaluates a system’s ability to meet the technical requirements specified by TSA and reflects the first test stage prior to procurement. QT&E occurs at two facilities, the

Transportation Security Laboratory (TSL) and TSA Systems Integration Facility (TSIF). These two facilities perform independent testing on each technology. QT&E occurs when TSA first considers a technology and for any subsequent upgrades of that technology. Next, TSA performs the operational test and evaluation (OT&E). This sequence of testing independently validates the extent of operational effectiveness for candidate systems and determines the suitability in the airport environment. OT&E also includes the safety testing for radiation emission. Both QT&E and OT&E only occur during the first year of acquisition within each procurement cycle—2008 for AIT-1 and 2011 for AIT-2. According to the 2011 and 2012 LCCEs, TSA spent $743,441[126] on QT&E and $687,483[127] on OT&E for AIT-1 in 2008 and $3.41 million[128] on QT&E and $30.39 million[129] on OT&E for AIT-2 in 2011.

The next two stages of testing consist of the factory acceptance test (FAT) and the site acceptance test (SAT). FAT encompasses independent verification of equipment at the contractor facility, to verify compliance with all requirements in the procurement specification. FATs include test requirements applicable to the operational environment (e.g., power, voltage, electromagnetic, stress, loading, live interfaces, threat resolution, etc.). SAT encompasses independent verification of installed equipment to confirm the set-up of the equipment. It also validates the operational configuration of the units, and confirms compliance with contractual requirements. TSA conducts FATs at the Original Equipment Manufacturer (OEM) facility and SATs on-site at the airports. TSA conducts both through TSA's Test & Evaluation Support Services contracts. A FAT and a SAT occur for each unit before deployment. For 2008-2013, TSA bases the FAT and SAT costs on 2011 LCCE cost data which is $526 and $908 per unit, respectively.[130] FATs and SATs occur for the 61 millimeter units acquired in 2012 but whose deployment was delayed until 2013. For these reallocated millimeter units, TSA assumes FAT tests occur in 2012 and SAT tests occur in 2013; this timing is reflected in the cost estimates.

---

[126] Originally reported as $683,938 in 2009 dollars. TSA inflated this amount to 2014 dollars.
[127] Originally reported as $632,459 in 2009 dollars. TSA inflated this amount to 2014 dollars.
[128] Originally reported as $3,298,272.71 in 2012 dollars. TSA inflated this amount to 2014 dollars.
[129] Originally reported as $29,420,752.14 in 2012 dollars. TSA inflated this amount to 2014 dollars.
[130] FAT and SAT costs are based on the Battelle HSTS04-05-D-DEP027 contract costs in 2009 inflated to 2014 dollars.

TSA incurs PMO costs to run and facilitate the various stages of testing. TSA estimates these costs separately from the general PSP PMO costs. Because TSA manages all PSP technologies under one contract, TSA applies the 14.99 percent ratio to the total cost of the support services contract to estimate PMO costs for AIT. For 2008-2013, TSA estimated annual PMO testing costs to be $535,758.[131] Additionally, TSA uses a large contract to support engineering services, changes, and initiatives. TSA accounts for the research and additional cost of upgrading the technology from AIT with IO to AIT with ATR and other subsequent research and development associated with the AIT platform. Again, this large contract covers the suite of technologies in the PSP. To allocate a portion of these costs to AIT for 2008-2013, TSA scales the total cost by the 14.99 percent ratio and estimates a cost of $7.93 million in 2008, $8.18 million in 2009, $8.34 million in 2010, $8.05 million in 2011, $5.97 million in 2012, and $3.29 million in 2013.[132]

For QT&E costs in 2014, TSA uses the most recent LCCE to assign costs of $2.98 million. For OT&E in 2014, TSA assigns the estimate from the most recent LCCE which is a cost of $1.56 million. TSA uses the most recent LCCE to assign FAT/SAT costs for AIT in projected years which estimates a cost of $47,625 in 2014. Similarly, TSA bases PMO & engineering services costs on the most recent LCCE. In order to more align costs with the 2014 LCCE, TSA presents PMO and support engineering costs together and bases it on the System Documentation and Related Data and Training cost categories in the LCCE. These two categories capture similar costs as PMO & engineering services used in historical years such as engineering data, support data, management data, the development of training materials, and other associated costs. TSA reports these costs to be $1.58 million for 2014.[133]

Table 37 presents the cost of testing and evaluation from 2008-2014 as $88.19 million (undiscounted).

---

[131] $535,758 = 14.99% x $3,518,264 (TESS, 2012 LCCE). This value is then inflated from 2013 dollars to 2014.
[132] Based on line item projections of Engineering Support Services/Change/Initiatives in both the 2011 and 2012 LCCEs. These report years were adjusted for inflation to 2014 dollars and to calendar year from fiscal year outlays.
[133] The 2014 LCCE system documentation and related data costs as $0 in FY2014, $861,330 in FY2015, and $0 in FY2016; the training costs as $630,230 in FY2014, $3.48 million in FY2015, and $0 in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. Calendar year 2015 includes the second, third, and fourth quarter of FY2015; and the first quarter of FY2016. These costs were then inflated from 2013 to 2014 dollars.

Table 37: Testing and Evaluation Costs from 2008-2014

(in $millions, undiscounted)

Year	**QT&E** a	**OT&E** b	**FAT/SAT** c = AIT deployed x ($526+ $908)[134] ÷ 1 million	**PMO Costs** d = $535,758÷ 1 million	**Engineering Services** e	**Total** f = a + b + c + d + e
2008	$0.74	$0.69	$0.04	$0.54	$7.93	$9.94
2009	$0.00	$0.00	$0.00	$0.54	$8.18	$8.72
2010	$0.00	$0.00	$0.65	$0.54	$8.34	$9.53
2011	$3.41	$30.39	$0.11	$0.54	$8.05	$42.49
2012	$0.00	$0.00	$0.45	$0.54	$5.97	$6.95
2013	$0.00	$0.00	$0.12	$0.54	$3.29	$3.95
2014	$2.98	$1.56	$0.48		$1.58	$6.60
Total						**$88.19**

Note: Totals may not sum exactly due to rounding

For QT&E and OT&E costs in projected years, TSA uses the most recent LCCE to assign costs of $207,302 and $1.58 million in 2015, respectively. Since there were no procurements of AIT in 2016 and 2017, there were no associated QT&E and OT&E costs in those years.

TSA uses the most recent LCCE to assign FAT/SAT costs for AIT in projected years which estimates a cost of $1.30 million in 2015; $56,205 in 2016; and $64,679 in 2017. Similarly, TSA bases PMO & engineering services costs on the most recent LCCE. In order to more align costs with the 2014 LCCE, TSA presents PMO and support engineering costs together and bases it on the System Documentation and Related Data and Training cost categories in the LCCE. These

[134] TSA assumes that the 2013 delayed deployment millimeter units underwent FATs in 2012 and SATs in 2013. FATs occur before acquisition while SATs occur at deployment to the airport.

two categories capture similar costs as PMO & engineering services used in historical years such as engineering data, support data, management data, the development of training materials, and other associated costs. TSA reports these costs to be $3.31 million in 2015, and $0 in 2016 and 2017.[135]

Table 38 presents the cost of testing and evaluation from 2015-2017 as $6.52 million (undiscounted), $6.33 million with three percent discounting, and $6.08 million with seven percent discounting.

Table 38: Testing and Evaluation Costs from 2015-2017

(in $millions)

Year	**QT&E** a	**OT&E** b	**FAT/SAT** c	**PMO & Engineering Services** d	**Total** e = a + b + c + d
2015	$0.21	$1.58	$1.30	$3.31	$6.40
2016	$0.00	$0.00	$0.06	$0.00	$0.06
2017	$0.00	$0.00	$0.06	$0.00	$0.06
Total					**$6.52**
Discounted at 3%					**$6.33**
Discounted at 7%					**$6.08**

Note: Totals may not sum exactly due to rounding.

[135] The 2014 LCCE system documentation and related data costs as $0 in FY2014, $861,330 in FY2015, and $0 in FY2016; the training costs as $630,230 in FY2014, $3.48 million in FY2015, and $0 in FY2016. These expenditures were converted to calendar year—which aligns with the RIA. Calendar year 2014 includes the second, third, and fourth quarter of FY2014; and the first quarter of FY2015. Calendar year 2015 includes the second, third, and fourth quarter of FY2015; and the first quarter of FY2016. These costs were then inflated from 2013 to 2014 dollars.

Program Management Office Cost

To run the PSP program, TSA uses both internal and outside contractor PMO support.[136] PMO costs for the PSP include budget and financing, acquisition program documentation, deployment support, program support, testing and evaluation planning, communications support, executive support, and other costs relating to managing the program. Because PMO support relates less to the cost of technologies and more to the day-to-day support of the program, TSA is unable to directly allocate spending to AIT. However, TSA estimates that 10 percent of the total PSP cost equates to the cost of general PMO. To estimate an annual PMO cost, TSA multiplies the total average annual PSP cost in the 2014 LCCE (for FY2014-FY2026) of $206.26 million[137] by 10 percent. Then, TSA divides the annual PMO cost by the eight main screening technologies to spread the costs evenly among all technologies. TSA estimates an annual PMO cost of $2.58 million per technology, which is then used for AIT in this analysis. This annual cost is applied throughout the period of analysis (2008-2017), and TSA estimates the cost of PMO for this duration as approximately $25.78 million (undiscounted), $25.05 million discounted at three percent, and $24.20 million discounted at seven percent.

Reallocation

TSA accounts for the reallocation of 73 previously deployed millimeter AIT units to other airports in 2013 due to the removal of backscatter units. Based on previous deployments, TSA estimates an average per-unit cost to reallocate a millimeter AIT unit at $29,154, as shown in Table 39.[138] This cost includes:

- Systems integration;
- Removal, re-installment, shipping, rigging warehouse, other equipment relocation; and
- Ancillary equipment and infrastructure adjustments.

[136] Deloitte – HSTS04 – 08 – F – CT8600 contract supports the PSP program.
[137] Total PSP lifecycle cost from 2014 LCCE is $2,639.13 million. TSA divided this by 13 years (FY2014-2026) to estimate average annual cost of PSP and inflates this amount from 2013 to 2014 dollars.
[138] TSA's Office of Security Capabilities provided estimates based on the reallocation plan.

TSA multiplies the unit cost of reallocation by the 73 units. The reallocation cost to TSA is $2.13 million, as shown in Table 39.

Table 39: Reallocation Cost of Millimeter Units in 2013

Cost Category	**Per-Unit Cost**
Systems Integration Drawing Revisions	$2,630
Cost to Remove AIT	$8,416
Adjust WTMD and Install Security Glass	$1,105
Shipping	$2,314
Rigging Warehouse	$210
Cost to Reinstall	$7,890
Systems Integration Oversight	$3,472
Systems Integration Program Management	$1,599
Other Equipment Relocation at Install Airport	$802
Ancillary Equipment Adjustments	$526
Infrastructure Adjustments	$189
Per-unit Cost to Reallocate an AIT	**$29,154**
Total Units Reallocated	**73**[139]
Total Cost for Reallocation	**$2,128,209**

Note: Totals may not sum exactly due to rounding

[139] The total units for relocated AITs have changed from the figure published in the NPRM. TSA no longer includes units used in testing centers for costs related to airports.

Baseline Cost

TSA accounts for the costs that would have occurred without the introduction of AIT. For this calculation, TSA first estimates the additional number of WTMDs that would be in operation in the absence of AIT deployment. TSA then subtracts these WTMD-related costs from the total AIT costs in order to calculate incremental life cycle cost for AIT. To estimate baseline costs, TSA assumes that WTMDs continues as the primary technology in the airport screening environment. TSA uses SME input provided by TSA's OSC, to approximate the cumulative number of WTMDs that have been replaced by AIT units from 2008-2017.

TSA assumes an annual maintenance cost of $727 per WTMD.[140] TSA did not include PMO costs associated with WTMDs because of the small number of disposed WTMD units, compared to the total number out in service. This small amount would have an insignificant impact to the overall PMO cost, which is tied to a large contract to service the suite of technologies in the PSP.

From 2008-2014, TSA projects the baseline cost to be approximately $158,530 undiscounted. Table 40 presents these costs.

[140] Siemens – HSTS04 – 09 – C – CT3173 contract supports the out-of-warranty maintenance. Based on the contract TSA estimates the out-of-warranty maintenance cost at $669 per WTMD. TSA inflated this from 2009 dollars to 2014.

Table 40: Baseline Costs from 2008-2014

(in $millions, undiscounted)

Year	Cumulative WTMD Disposed for AIT a	Total b = a x $766 ÷ 1 million
2008	0	$0.00
2009	0	$0.00
2010	0	$0.00
2011	0	$0.00
2012	56	$0.04
2013	76	$0.06
2014	86	$0.06
Total		**$0.16**

Note: Totals may not sum exactly due to rounding.

From 2015-2017, TSA projects the baseline cost to be approximately $209,434 undiscounted, $197,470 with three percent discounting, and $183,207 with seven percent discounting. Table 41 presents these costs.

Table 41: Baseline Costs from 2015-2017

(in $millions)

Year	Cumulative WTMD Disposed for AIT a	Total b = a x $766 ÷ 1 million
2015	96	$0.07
2016	96	$0.07
2017	96	$0.07
Total		**$0.21**
Discounted at 3%		**$0.20**
Discounted at 7%		**$0.18**

Note: Totals may not sum exactly due to rounding.

Total Life Cycle Costs

TSA estimates the life cycle costs of AIT by accounting for the acquisition, maintenance, testing and evaluation, PMO, and reallocation costs, and subtracting baseline costs. TSA estimates the total life cycle cost from 2008-2014 as approximately $447.14 million (undiscounted). Table 42 presents these costs.

Table 42: TSA Total Life Cycle Cost of AIT from 2008-2014

(in $millions, undiscounted)

Year	**Acquisition/ Installation/ Integration/ Disposal** a	**Maintenance Cost** b	**Testing and Evaluation Cost** c	**PMO Cost** d	**Reallocation** e	**Baseline Cost** f	**Total Cost** g = a + b + c + d + e - f
2008	$5.40	$16.13	$9.94	$2.58	$0.00	$0.00	$34.04
2009	$0.58	$16.13	$8.72	$2.58	$0.00	$0.00	$28.01
2010	$89.88	$16.67	$9.53	$2.58	$0.00	$0.00	$118.66
2011	$15.05	$16.73	$42.49	$2.58	$0.00	$0.00	$76.86
2012	$66.49	$25.61	$6.95	$2.58	$0.00	$0.04	$101.59
2013	$15.80	$22.31	$3.95	$2.58	$2.13	$0.06	$46.70
2014	$2.12	$30.03	$6.60	$2.58	$0.00	$0.06	$41.28
Total							**$447.14**

Note: Totals may not sum exactly due to rounding.

TSA estimates the total life cycle cost from 2015-2017 as approximately $101.25 million (undiscounted), $96.12 million discounted at three percent, and $89.87 million discounted at seven percent. Table 43 presents these costs.

Table 43: TSA Total Life Cycle Cost of AIT from 2015-2017

(in $millions)

Year	Acquisition/ Installation/ Integration/ Disposal a	Maintenance Cost b	Testing and Evaluation Cost c	PMO Cost d	Reallocation e	Baseline Cost f	Total Cost g = a + b + c + d + e - f
2015	$8.88	$31.96	$6.40	$2.58	$0.00	$0.07	$49.75
2016	$0.03	$22.47	$0.06	$2.58	$0.00	$0.07	$25.06
2017	$0.02	$23.85	$0.06	$2.58	$0.00	$0.07	$26.45
Total							**$101.25**
Discounted at 3%							**$96.12**
Discounted at 7%							**$89.97**

Note: Totals may not sum exactly due to rounding.

Utilities Costs to TSA

TSA incurs increased costs from the added consumption of electricity from AIT at reimbursed airports. Table 44 breaks down the cumulative number of AIT units in reimbursed airports.

Table 44: Cumulative AIT Units In-Service in Reimbursed Airports

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	12	10	0	0	0	**22**
2009	14	10	0	0	0	**24**
2010	177	112	6	0	0	**295**
2011	181	142	18	0	0	**341**
2012	270	188	41	0	0	**499**
2013*	248	160	37	0	0	**445**
2014**	282	162	43	0	0	**487**
2015	303	174	47	0	0	**524**
2016	303	174	47	0	0	**524**
2017	303	174	47	0	0	**524**

Source: TSA Office of Security Capabilities
* Reflects 73 backscatter units removed at the end of 2012 in addition to the units deployed throughout 2013.
** Reflects 174 backscatter units removed at the end May 2013.

The methodology to estimate the increased utilities costs parallels the methodology used for industry costs (described in the Utilities Costs to Airports section). First, TSA multiplies the number of AIT machines in each airport category by the average energy consumption per AIT machine by airport category (shown in Table 19) to calculate the energy consumption in reimbursed airports each year. Table 45 illustrates these calculations.

Table 45: Annual Energy Consumption of AIT in Reimbursed Airports in kilowatts

Year	Cumulative AIT Deployment					Energy Consumed (# of AIT's multiplied by per day consumption x 365.25 days) [141]
	X	I	II	III	IV	
2008	12	10	0	0	0	157,549
2009	14	10	0	0	0	172,014
2010	177	112	6	0	0	2,113,498
2011	181	142	18	0	0	2,436,433
2012	270	188	41	0	0	3,562,222
2013*	248	160	37	0	0	3,234,271*
2014	282	162	43	0	0	3,475,401
2015	303	174	47	0	0	3,740,948
2016	303	174	47	0	0	3,740,948
2017	303	174	47	0	0	3,740,948

Table 46 illustrates how TSA calculates the cost of electricity for AIT using the electricity consumption and prices of electricity (shown in Table 18).

[141] For example, in 2010: ((177 Cat X AITs × 19.80 kW) + (112 Cat I AITs × 19.37 kW) + (6 Cat II AITs × 18.64 kW)) × 365.25 days = 2,113,498 kW.

Table 46: AIT Utilities Cost in Reimbursed Airports

Year	Energy Consumption a	Electricity Price ($ per kWh) b	AIT Utilities Cost c = a x b ÷ $1 million
2008	157,549	$0.1124	$0.018
2009	172,014	$0.1104	$0.019
2010	2,113,498	$0.1094	$0.231
2011	2,436,433	$0.1076	$0.262
2012	3,562,222	$0.1042	$0.371
2013*	3,234,271	$0.1042	$0.337
2014	3,475,401	$0.1074	$0.373
2015	3,740,948	$0.1062	$0.397
2016	3,740,948	$0.1080	$0.404
2017	3,740,948	$0.1087	$0.407

Note: Totals may not sum exactly due to rounding.
*Estimates in 2013 reflect a weighted average based on the removal of backscatter units. (See the Appendix for details).

To account for the net change in utilities costs, TSA subtracts the utilities costs of WTMDs that were removed because of AIT deployment, and then disposed, from AIT utilities costs. Unlike AIT, WTMD consumes the same rate of electricity when it is operational and idle at a rate of 0.04 kWh, or 350.64 kW per year.[142] TSA multiplies the number of WTMDs removed by the energy consumption rate and the price of electricity to estimate the cost of electricity from the removed WTMDs. The following tables illustrate these costs.

[142] 350.64 kW = 0.04 kWh × 24 hours × 365.25 days.

Table 47: Removed WTMDs Utilities Cost from Reimbursed Airports

Year	WTMDs Removed a	WTMD Energy Consumption Rate b	Electricity Price ($ per kWh) c	WTMDs Utilities Cost d =a x b x c
2008	0	350.64	$0.1124	$0.000
2009	0		$0.1104	$0.000
2010	0		$0.1094	$0.000
2011	0		$0.1076	$0.000
2012	21		$0.1042	$0.001
2013	28		$0.1042	$0.001
2014	32		$0.1074	$0.001
2015	35		$0.1062	$0.001
2016	35		$0.1080	$0.001
2017	35		$0.1087	$0.001

TSA estimates the TSA utilities by subtracting the utilities cost from WTMDs from AITs. Illustrates the costs from 2008-2014 as approximately $1.61 million (undiscounted).

Table 48: TSA Utilities Costs from 2008-2014

(in $millions, undiscounted)

Year	AIT Cost from Reimbursed Airports a	WTMD Cost at Reimbursed Airports b	Total Cost c = a - b
2008	$0.018	$0.000	$0.018
2009	$0.019	$0.000	$0.019
2010	$0.231	$0.000	$0.231
2011	$0.262	$0.000	$0.262
2012	$0.371	$0.001	$0.371
2013	$0.337	$0.001	$0.336
2014	$0.373	$0.001	$0.372
Total			**$1.609**

Note: Totals may not sum exactly due to rounding.
*Estimates in 2013 reflect a weighted average based on the removal of backscatter units. (See the Appendix for details).

TSA estimates the TSA utilities costs from 2015-2017 as approximately $1.20 million (undiscounted), $1.14 million with three percent discounting, and $1.05 million with seven percent discounting.

Table 49: TSA Utilities Costs from 2015-2017

(in $millions)

Year	AITs at Reimbursed Airports a	WTMDs at Reimbursed Airports b	Total Cost c = a - b
2015	$0.397	$0.001	$0.396
2016	$0.404	$0.001	$0.403
2017	$0.407	$0.001	$0.405
Total			**$1.204**
Discounted at 3%			**$1.135**
Discounted at 7%			**$1.053**

Note: Totals may not sum exactly due to rounding.

Public Engagement Costs to TSA

TSA met with industry stakeholders, passenger and travel associations, and other parties during the study period to discuss and receive input on AIT deployment and the screening process. TSA has not quantified the time spent within TSA preparing for these meetings and considering and responding to the public input provided at these meetings. TSA expects that the overall cost of this engagement is *de minimis* in comparison to total AIT deployment cost of over $2 billion dollars over ten years.

Removal Costs to Industry

All 247 backscatter units were removed from airports in 2012 and 2013 in order to comply with the statutory requirement to use only AIT equipped with ATR to screen passengers. Both TSA and industry paid for the costs to remove backscatter units. Industry paid for the removal of 174 units in 2013. TSA assumes a per-unit cost of $10,941 to remove a backscatter machine from the airport and, thus, incurs a cost of $1.90 million in 2013. [143]

Total Cost of AIT

TSA estimates that the total historical costs for AIT in the years 2008-2014 as approximately $1,439.32 million (undiscounted). Table 50 reports the total cost by cost category.

Table 50: Cost Summary from 2008 – 2014 by Cost Component

(in $millions, undiscounted)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Industry Costs	Total
			Personnel	Training	Equipment	Utilities	Backscatter Removal	
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	$0.02	$0.01	$12.05	$0.57	$28.01	$0.02	$0.00	$40.69
2010	$0.42	$0.13	$57.20	$33.64	$118.66	$0.23	$0.00	$210.28
2011	$3.17	$0.15	$201.83	$57.06	$76.86	$0.26	$0.00	$339.33
2012	$5.28	$0.28	$219.75	$23.31	$101.59	$0.37	$0.00	$350.58
2013	$4.45	$0.25	$197.77	$14.37	$46.70	$0.34	$1.90	$265.79
2014	$3.05	$0.18	$131.22	$12.21	$41.28	$0.37	$0.00	$188.31
Total	**$16.40**	**$1.02**	**$830.09**	**$141.16**	**$447.14**	**$1.61**	**$1.90**	**$1,439.32**

Note: Totals may not sum exactly due to rounding.

[143] TSA bases the $10,941 removal cost on TSA's Office of Security Capabilities cost estimate assuming an $8,416 removal cost, a $2,314 shipping cost and a $210 warehouse rigging cost as shown in Table 39.

TSA estimates that the total projected costs for AIT in the years 2015-2017 as approximately $706.99 million (undiscounted), $666.47 million with three percent discounting, and $618.18 million with seven percent discounting. Table 51 reports the total cost by cost category.

Table 51: Cost Summary from 2015 – 2017 by Cost Component

(in $millions)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Total
			Personnel	Training	Equipment	Utilities	
2015	$4.12	$0.20	$141.96	$41.25	$49.75	$0.40	$237.68
2016	$4.20	$0.20	$141.96	$54.89	$25.06	$0.40	$226.72
2017	$4.28	$0.20	$141.96	$69.30	$26.45	$0.41	$242.60
Total	**$12.59**	**$0.61**	**$425.89**	**$165.45**	**$101.25**	**$1.20**	**$706.99**
Total (Discounted at 3%)	**$11.87**	**$0.57**	**$401.55**	**$155.22**	**$96.12**	**$1.13**	**$666.47**
Total (Discounted at 7%)	**$11.01**	**$0.53**	**$372.55**	**$143.07**	**$89.97**	**$1.05**	**$618.18**

Note: Totals may not sum exactly due to rounding.

TSA estimates that the total costs for AIT in the years 2008-2017 as approximately $2,146.31 million (undiscounted). Table 52 reports the total cost by cost category.

Table 52: Total Cost Summary from 2008 – 2017 by Cost Component

(in $millions, undiscounted)

Year	Passenger Opportunity Costs	Airport Utilities Costs	TSA Costs				Industry Costs	Total
			Personnel	Training	Equipment	Utilities	Backscatter Removal	
2008	$0.01	$0.01	$10.27	$0.00	$34.04	$0.02	$0.00	$44.34
2009	$0.02	$0.01	$12.05	$0.57	$28.01	$0.02	$0.00	$40.69
2010	$0.42	$0.13	$57.20	$33.64	$118.66	$0.23	$0.00	$210.28
2011	$3.17	$0.15	$201.83	$57.06	$76.86	$0.26	$0.00	$339.33
2012	$5.28	$0.28	$219.75	$23.31	$101.59	$0.37	$0.00	$350.58
2013	$4.45	$0.25	$197.77	$14.37	$46.70	$0.34	$1.90	$265.79
2014	$3.05	$0.18	$131.22	$12.21	$41.28	$0.37	$0.00	$188.31
2015*	$4.12	$0.20	$141.96	$41.25	$49.75	$0.40	$0.00	$237.68
2016*	$4.20	$0.20	$141.96	$54.89	$25.06	$0.40	$0.00	$226.72
2017*	$4.28	$0.20	$141.96	$69.30	$26.45	$0.41	$0.00	$242.60
Total	**$28.99**	**$1.63**	**$1,255.98**	**$306.61**	**$548.39**	**$2.81**	**$1.90**	**$2,146.31**

Note: Totals may not sum exactly due to rounding.
* Estimates in 2015-2017 reflect throughputs that are projected to occur.

Qualitative Impacts

This section describes qualitatively the potential AIT privacy and health impacts and the steps implemented by TSA to address any concerns passengers may have on both issues.

Privacy

TSA enhanced privacy by removing all AIT machines without ATR from its checkpoints. As part of the Federal Aviation Administration Modernization and Reform Act of 2012, Congress mandated that all AIT units must be equipped with ATR by June 1, 2012.[144] As permitted by law, the deadline was extended to June 1, 2013. TSA equipped all of the millimeter wave units with the ATR software. The manufacturer of the backscatter AITs removed all general-use backscatter units without ATR.[145] As of May 16, 2013, TSA only uses AIT equipped with ATR at checkpoints.

Machines equipped with ATR software create a generic outline displayed on a screen located on the AIT equipment viewable by the public. The software auto-detects potential threats concealed on the body. TSOs resolve the identified potential threats through additional screening. The use of the ATR software enhances passenger privacy by eliminating the individual image as well as the need for a TSO to view the image for potential threats. ATR-enabled units deployed at airports have no capability to transmit, store or print the generic outline that will be visible to passengers (for additional discussions on AIT equipment and privacy safeguards see the Final Rule section II subsection S *General Concerns Regarding Privacy*). TSA's website provides examples of the generic outline that the ATR software produces.[146] Even before the development of the ATR software, TSA instituted rigorous safeguards[147] to protect the privacy of individuals screened using AIT. In addition, as noted by the Court in EPIC, the DHS Chief Privacy Officer has conducted several Privacy Impact Assessments (PIAs) on the use of AIT equipment, as required by law. The PIA describes the strict measures TSA uses to protect privacy. The DHS website posts the most recent update to the PIA (http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf). Finally, to give further consideration to the Fair Information Practice Principles, the foundation for privacy policy and

---

[144] P.L. 112-95.
[145] http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract.html
[146] www.tsa.gov
[147] Initially, the images produced by the AIT were viewed in a remote, windowless room by an Image Operator (IO). Because the IO was located away from the checkpoint, the IO was unable to see the passenger being screened. If the IO identified a potential threat, the IO verbally communicated the location of the potential threat via headset to the system operator (SO), who then conducted alarm resolution in accordance with standard operating procedures. The inability of both the AIT machine and the computer used by the IO to store the image provided an additional level of privacy protection.

implementation at DHS, individuals generally may opt-out of the AIT in favor of physical screening. TSA also provides notice of the use of AIT and the opt-out option at the checkpoint so that individuals may exercise an informed judgment on AIT.

TSA further enhanced privacy by removing all AIT machines without ATR from its checkpoint, adopting the use of ATR software in all its new machines, and by providing an "opt-out" measure where passengers generally may decline AIT and opt instead for a pat-down done by a TSO of the same gender. TSA captures the additional time spent in the pat-down in the Passenger Opportunity Cost Section of this RIA.

Health

Prior to procuring and deploying both backscatter and millimeter wave AIT equipment, TSA tested the units to determine whether they would be safe for use in passenger screening. TSA subjected AIT equipment to extensive testing prior to deployment, confirming the equipment met safety standards for individuals being screened, equipment operators, and bystanders. Furthermore, complying with the statutory mandate regarding the ATR software lead to the removal of the backscatter machines that produced the exposure to ionizing x-ray beams. Backscatter machines could not be equipped with ATR software. The millimeter wave machines emit non-ionizing electromagnetic at a level that falls well within the limits allowed under relevant national health and safety standards. Below are descriptions of health certifications and testing for each AIT technology. For discussion on AIT safety see Final Rule section II subsection P *Other Health and Safety Issues*.

1. Millimeter Wave Units

The millimeter wave AIT systems are the only technology deployed at the checkpoint as of May 16, 2013, and use nonionizing radio frequency energy in the millimeter wave spectrum to generate a three-dimensional image based on the energy reflected from the body. Millimeter wave imaging technology meets all known national and international health and safety standards. In fact, the energy emitted by millimeter wave technology is 1,000 times less than the international limits and guidelines. The millimeter wave AIT systems that TSA uses must comply with the 2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety

Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™-2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494-522, published April 1998. TSA's millimeter wave units are also consistent with Federal Communications Commission OET Bulletin 65, Health Canada Safety code 6, and RSS-102 Issue 3 for Canada. The Food and Drug Administration (FDA) also confirmed that millimeter wave security systems that comply with the IEEE Std. C95.1™-2005 cause no known adverse health effects.[148]

2. Backscatter Units

TSA removed all backscatter units by May 16, 2013, in order to comply with the statutory mandate to use only AIT equipped with ATR software. When in use, TSA did not identify health impacts associated with the ionizing radiation emitted by general-use backscatter technology. TSA's procurement specifications required that the backscatter units must conform to American National Standards Institute/Health Physics Society (ANSI/HPS) N43.17, a consensus radiation safety standard approved by ANSI and HPS for the design and operation of security screening systems that use ionizing radiation.[149] The ANSI/HPS N43.17 standard was first published in 2002 and revised in 2009.[150] The National Council on Radiation Protection and Measurements in Report 116, "Limitations of Exposure to Ionizing Radiation," bases the annual dose limits in ANSI/HPS N43.17 on dose limit recommendations for the general public.[151] The

---

148 FDA, "Products for Security Screening of People," available at http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm

149 American National Standards Institute is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system. The Institute oversees the development and use of voluntary consensus standards by providing neutral, third-party accreditation of the procedures used by standards developing organizations, and approving their documents as American National Standards. Health Physics Society (HPS) is a scientific organization of professionals who specialize in radiation safety. Its mission is to support its members and to promote excellence in the science and practice of radiation safety. As an independent nonprofit scientific organization, HPS is not affiliated with any government or industrial organization or private entity.

150 American National Standard. "Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation," ANSI/HPS N43.17 (2009); Health Physics Society; McLean, VA. Copies can be ordered at: http://webstore.ansi.org/faq.aspx#resellers.

151 The National Council on Radiation Protection and Measurements was founded in 1964 by Congress to cooperate with the International Commission on Radiological Protection, the Federal Radiation Council, the International Commission on Radiation Units and Measurements, and other national and international organizations, both governmental and private, concerned with radiation quantities, units, and measurements as well as radiation protection. The report is available at www.ncrponline.org.

National Council on Radiation sets the dose limits with consideration given to individuals, such as pregnant women, children and persons who receive radiation treatments, and who may be more susceptible to radiation health effects. Further, the standard also takes into consideration the continuous exposure to ionizing radiation from the environment. The ANSI/HPS N43.17 sets the maximum permissible dose of ionizing radiation from a general-use system per security screening at 0.25 microsieverts.[152] The standard also requires that individuals should not receive 250 microsieverts or more from a general-use x-ray security screening system in a year.

The FDA's Center for Devices and Radiological Health (CDRH), the National Institute for Standards and Technology, and the Johns Hopkins University Applied Physics Laboratory (APL) independently tested the radiation dose (effective dose) a passenger receives from a general-use backscatter AIT screening. All results affirmed that the effective dose for individuals being screened, operators, and bystanders fell well below the dose limits specified by ANSI.[153] The DHS Office of Inspector General (OIG) confirmed these results in a report issued in February 2012.[154] The OIG report found that the independent surveys show that backscatter radiation levels fall below the established limits and that TSA complied with ANSI radiation safety requirements.

Typical doses from backscatter machines amount to no more than 0.05 microsieverts per screening, well below the ANSI/HPS N43.17 maximum dosage of 0.25 microsieverts per screening. An individual would have to have been screened by the Backscatter Secure 1000 more than 13 times daily for 365 consecutive days before exceeding the ANSI/HPS standard.

By comparison, a traveler would have to be screened 2,000 times to equal the dosage received in a single chest x-ray, which delivers 100 microsieverts of ionizing radiation. A typical bite-wing dental x-ray of 5 microsieverts would be equivalent to 100 screenings, and a two-view

---

[152] The biological effect of radiation is measured in sieverts (Sv). One sievert equals 1,000 millisieverts and one millisievert equals 1,000 microsieverts.
[153] TSA's website at www.tsa.gov contains many articles and studies that discuss AIT safety, including a description of the built-in safety features of the backscatter AITs, an Archives of Internal Medicine report on the risks of imaging technology, the FDA evaluation of backscatter technology, and other independent safety assessments of AIT.
[154] Department of Homeland Security, Office of Inspector General, "Transportation Security Administration's Use of Backscatter Units," OIG-12-38, February 2012.

mammogram that delivers 360 microsieverts would be equivalent to 7,200 screenings.[155] A passenger on a one-way trip from New York to Los Angeles is exposed to approximately four microsieverts of ionizing radiation per hour of flight.[156]

ANSI/HPS also reflects the standard for a negligible individual dose of radiation established by the National Council on Radiation Protection and Measurements at 10 microsieverts per year. Efforts to reduce radiation exposure below the negligible individual dose are not warranted because the risks associated with that level of exposure are so small as to be indistinguishable from the risks attendant to environmental radiation that individuals are exposed to every day.[157] The level of radiation issued by the backscatter AIT is so low that most passengers would not have exceeded even the negligible individual dose. In fact, an individual would have to be screened more than 200 times a year by a backscatter AIT before they would exceed the negligible individual dose and, even then, would be below the ANSI/HPS N43.17 standard.

The European Commission released a report conducted by the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) on the risks related to the use of security scanners for passenger screening that use ionizing radiation such as the general-use backscatter AIT machines.[158] The committee found that, "The health effects of ionizing radiation include short-term effects occurring as tissue damage. Such deterministic effects cannot result from the doses delivered by security scanners."[159] In the long term, it found that the potential cancer risk cannot be estimated but, likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources and background risk due to other factors.

---

[155] HPS Fact Sheet: Radiation Exposure from Medical Exams and Procedures, January 2010, http://www.hps.org/documents/Medical_Exposures_Fact_Sheet.pdf.
[156] http://www.radiationanswers.org/radiation-sources-uses/natural-radiation.html
[157] The World Health Organization estimates that each person is exposed, on average, to 2.4 millisieverts (i.e., 2400 microsieverts) of ionizing radiation each year from natural sources. www.who.int/ionizing_radiation/about/what_is_ir/en/index2.html.
[158] The SCENIHR is an independent committee that provides the European Commission with the scientific advice it needs when preparing policy and proposals relating to consumer safety, public health, and the environment. The committee is made up of external experts. The report can be found at http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf.
[159] Ibid. pg. 8.

The ANSI/HPS N43.17 standard also requires that any general-use backscatter machine have safety interlocks to terminate emission of x-rays in the event of any system problem that could result in abnormal or unintended radiation emission. The backscatter AIT had three such features.[160] First, the manufacturer designed the unit to cease x-ray emission once the programmed scan motion ends. This feature could be adjusted. Second, the manufacturer programed the unit to terminate emission once the requisite number of lines of data necessary to create an image was received. Both of these automatic features reduced the possibility that emissions could continue if the unit malfunctions. Finally, the unit had an emergency stop button that would terminate x-ray emission.

Upon installation, TSA conducted a radiation emission survey on each backscatter AIT to ensure the unit operated properly. TSA performed preventive maintenance checks, including radiation safety surveys, at least once every 6 months and after any maintenance that affected the radiation shielding, shutter mechanism, or x-ray production components, after any incident where damage was suspected, or after a unit was moved. The U.S. Army Public Health Command also conducted an independent radiation survey on deployed systems. These surveys measured the radiation levels that passengers and bystanders would be exposed to when a system performed a scan. The report confirmed that the general-use backscatter units tested were well within applicable national safety standards.[161]

The DHS Office of the Chief Procurement Officer requested the National Academy of Sciences to convene a committee to review previous studies as well as current processes used by DHS and equipment manufacturers to estimate radiation exposure resulting from backscatter x-ray advanced imaging technology (AIT) systems used in screening air travelers and provide a report with findings and recommendations on: (1) whether exposures comply with applicable health and safety standards for public and occupational exposures to ionizing radiation, and (2) whether system design (e.g., safety interlocks), operating procedures, and maintenance procedures are

---

[160] TSA's website contains a link to the backscatter's safety features.
[161] U.S. Army Institute of Public Health. "Rapiscan Secure 1000 Single Pose dosimetry study". January 2012.

appropriate to prevent over exposures of travelers and operators to ionizing radiation.[162] That study was released in October 2015 and confirms that radiation doses did not exceed the ANSI/HPS standard.[163]

TSA does not include economic costs to the public associated with the use of the AIT machines because radiation exposure and doses received from ionizing and non-ionizing rays are negligible and do not attribute any significant risk as a result of their use in screening. In addition, while TSA and independent tests determined that AIT pose an extremely low radiation risk from x-ray screening, passengers generally may decline AIT and opt instead for a pat-down.

[162] Backscatter X-Ray Machines Committee, National Materials and Manufacturing Board. http://sites.nationalacademies.org/DEPS/NMMB/DEPS_084944.htm.

[163] National Academies of Sciences, Engineering, and Medicine. Airport Passenger Screening Using Backscatter X-Ray Machines: Compliance with Standards (2015), available at http://www.nap.edu/21710.

CHAPTER 3: ANALYSIS OF ALTERNATIVES

OMB Circular A-4 requires TSA to consider alternatives. The subsequent sections analyze the costs of each alternative and also discuss the rationale for rejecting the alternatives.

Consideration of Regulatory Alternatives

In order to mitigate a vulnerability of existing aviation security, TSA sought to identify a means to detect non-metallic items concealed underneath the clothing of passengers traveling on commercial aircrafts. Through analysis, laboratory testing, and field testing, TSA identified several solutions capable of detecting non-metallic items. In Table 53, TSA presents a description of each alternative**.** Of all the alternatives considered, only Alternative 2 – WTMDs and Pat-Down – offers similar levels of screening as AIT by detecting both metallic and non-metallic potential threats. Alternatives 3 and 4 do not offer the same level of security and risk reduction as AIT and are not viable screening alternatives to AIT, without accepting a considerable amount of vulnerability to non-metallic potential threats. For this reason, TSA did not prepare a break-even analysis for these alternatives.

Table 53: Descriptive Summary of Regulatory Alternatives

Regulatory Alternative	Type	Description
1	WTMDs Only	The passenger screening environment remains the same as it was prior to 2008. TSA continues to use WTMDs as the primary passenger screening technology and resolve alarms with a pat-down.[164]
2	WTMD as Primary, Randomized Pat-Down as Secondary	TSA continues to use WTMDs as the primary passenger screening technology. Alarms would be resolved by a pat-down. In addition, TSA supplements the WTMD screening by conducting a pat-down on a randomly selected portion of passengers after screening by a WTMD (even if the person did not alarm in the WTMD).
3	WTMD as Primary, Randomized Explosive Trace Detection as Secondary Screening	TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.
4	WTMD as Primary, Randomized AIT as Secondary Screening	TSA continues to use WTMDs as the primary screening technology. TSA supplements the WTMD screening by conducting AIT screening on a randomly selected portion of passengers after screening by a WTMD.

[164] This pat-down is different from the one performed after an AIT is alarmed. AIT secondary screening pat-down are targeted toward a specific area while a pat-down resulting from an alarmed WTMD requires a full-body pat-down that will likely take longer.

Regulatory Alternative	Type	Description
5	AIT as Primary Screening (Preferred)	TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down. This is TSA's preferred alternative.

Regulatory Alternative 1 – WTMDs Only

Under this alternative, TSA imposes no change to the passenger screening environment pre-2008. TSA continues to use WTMDs as the primary passenger screening technology and resolves alarms with a pat-down. Due to the reliance on WTMDs, this alternative does not result in passengers being screened specifically for non-metallic items. While a pat-down may detect a non-metallic threat, this alternative uses a pat-down to resolve an alarm triggered by metallic objects.

Recent events highlight the need for a technology or process capable of detecting non-metallic threats concealed on passengers. In addition, this alternative fails to meet the instruction provided in the Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack, issued January 7, 2010.[165] This alternative also fails to meet the statutory requirements in 49 USC 44925. While this alternative imposes no additional cost burden, it falls short in addressing or mitigating the threat to aviation security posed by non-metallic explosives and weapons. For this reason, TSA rejected this alternative in favor of deploying AIT to screening checkpoints. This alternative represents the baseline screening scenario and therefore TSA did not perform a cost analysis or break-even analysis.

Regulatory Alternative 2 – Pat-Down

Under this regulatory alternative, TSA continues to use the WTMD as the primary passenger screening technology and supplements WTMD screening with a pat-down. In this alternative, TSA would conduct a pat-down on a high volume of randomly selected passengers[166]—meaning more passengers would be subject to physical touching while undergoing a pat-down. This pat-down consists of a thorough physical inspection capable of detecting non-metallic items concealed under passengers' clothing undetected by the WTMD. Performing pat-downs on a high volume of randomly selected passengers after primary screening by the WTMD addresses the threats of metallic and non-metallic weapons and explosives for a random sample of passengers.

The main advantage of this alternative involves the use of currently deployed WTMD technology. This alternative imposes minimal technology acquisition costs to TSA. Although TSA still needs to replace WTMDs after their useful life, this alternative avoids the resource cost to test and evaluate a new technology, the upfront cost of acquiring a new technology, and the cost to deploy and integrate the new technology into checkpoints.

[165] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack
[166] TSA believes 80 percent of the AIT-eligible screening population would be a minimum sufficient level of random screening to maintain an acceptable level of risk-reduction.

The main disadvantages with this alternative are the increasing the number of pat-downs performed on passengers and a reduction in passenger throughput due to the length of time required to perform a pat-down. Based on field tests, TSA estimates the pat-down procedure takes 80 seconds to perform.[167] Therefore, performing pat-downs on a significant number of passengers necessitates a substantial increase in staffing levels to maintain the current passenger throughput level (approximately 150 passengers per hour per lane). Without a staffing increase, passenger wait times and the associated opportunity costs would increase.

Additionally, as AIT represents a machine-based methodology, a screening environment centered on AIT provides a more consistent outcome over time. Further, TSA anticipates future advancements to AIT in detection capability, throughput, and privacy protection. Due to the reasons outlined above, TSA opted to reject implementing a random pat-down on a high volume of passengers to supplement WTMD screening for non-metallic explosives and weapons.

Cost Analysis

In order to estimate the potential cost of Alternative 2, TSA conducted an analysis using its staffing allocation model (SAM) to estimate the FTEs required to perform pat-downs on 80 percent of the AIT-eligible passenger throughput population based on 2015 data. TSA estimated that an additional 6,246 FTEs over the preferred alternative (AITs as the primary screening technology) would be needed to perform the pat-downs. TSA adjusted this additional FTE requirement in each year of the study period based on the estimated throughput for any given year. TSA multiplied FTEs by a TSO's average annual full compensation costs ($60,986) to calculate the personnel cost from this additional labor. TSA added to this subtotal the estimated AIT personnel cost (see the Personnel Cost to TSA section on page 68 for more detail on this cost) to calculate the full incremental personnel cost of Alternative 2 from the baseline (WTMDs as the primary screening technology). TSA also uses the AIT-eligible passenger throughput to estimate opportunity cost on the 80 percent who receives a pat-down. TSA multiplies the estimated passenger value of time ($45.14) by the time it takes to perform a pat-down (80

[167] This estimate excludes the 70 seconds estimated to wait for a same-gender TSO because under this alternative, TSA would increase its staff so there will always be both male and female TSOs available to perform a pat-down.

seconds) to estimate the opportunity cost of $1.00 per passenger. TSA estimates that the total cost for this alternative in the years 2008-2017 as approximately $5,542.04 million (undiscounted), $5,411.24 million discounted at 3 percent, and $5,255.37 million discounted at 7 percent. These costs represent a rough estimate due to the fact that TSA does not have enough information at this time to model all potential additional costs related to the implementation of this alternative such as potential additional training. Table 54 illustrates the calculation of costs for Alternative 2.

Table 54: Estimated Total Cost for Alternative 2

(in $ millions)

Year	Estimated FTEs	Annual FTE Compen-sation	AIT Personnel Cost	Alternative 2 Personnel Cost	AIT Throughput	Percent Receiving SPD	Opportunity Cost per Passenger	Alternative 2 Opportunity Cost	Total Alternative 2 Cost
	a	b	c	d = (a x b) ÷ $1 million + c	e	f	g	h = e × f × g ÷ $1 million	i = d + h
1	15	$60,986	$10.27	$11.19	682,155	80%	$1.00	$0.55	$11.74
2	63		$12.05	$15.90	2,832,564			$2.27	$18.18
3	570		$57.20	$91.93	25,555,844			$20.51	$112.44
4	3,001		$201.83	$384.82	134,645,029			$108.06	$492.87
5	6,502		$219.75	$616.30	291,776,221			$234.16	$850.45
6	7,975		$197.77	$684.14	357,874,438			$287.20	$971.35
7	6,965		$131.22	$555.99	312,542,888			$250.82	$806.81
8	6,246		$141.96	$522.88	280,280,076			$224.93	$747.81
9	6,365		$141.96	$530.12	285,605,397			$229.21	$759.32
10	6,486		$141.96	$537.49	291,031,900			$233.56	$771.05
Total									**$5,542.04**
Discounted at 3%									**$5,411.24**
Discounted at 7%									**$5,255.37**

Note: Totals may not sum exactly due to rounding.

Compared to the AIT alternative, this alternative is cost prohibitive and would represent an additional cost $5.54 billion (undiscounted) over a period of ten years. Additionally, this alternative may create negative reaction from the public subjected to a pat-down.

Break-Even Analysis

TSA performed a break-even analysis on the estimated costs of Alternative 2 against five scenarios of successful attacks on commercial aviation. Details about these scenarios, including the cost methodology, can be found on page 131 in Chapter 4. The costs of these consequences are divided by the annualized cost of Alternative 2 using a 7 percent discount rate ($497.03 million) to estimate the frequency of averted attacks that would have to occur for the benefits of Alternative 2 to meet its costs. Table 55 displays the results of the break-even analysis for Alternative 2.

Table 55: Frequency of Attacks Averted to Break-Even for Alternative 2 (Pat-Downs) ($ millions)

Aircrafts	Replacement & Emergency Response Costs a	Total Passengers + Crew b	Load Factor c	Total Consequence d = a + (b × c × VSL)	Attacks Averted by AIT to Break-Even: Total Consequence / $497.03M e = d ÷ $497.03M
High Capacity					
Airbus A380	$428.9	557	86%	$4,811	1 attack per 9.68 yrs
Boeing 777-200	$305.9	326	84%	$2,791	1 attack per 5.61 yrs
Medium Capacity					
Boeing 737-700/700LR	$79.2	138	80%	$1,075	1 attack per 2.16 yrs
Boeing 737-800	$94.2	176	84%	$1,434	1 attack per 2.89 yrs
Airbus Industries A320-100/200	$97.9	156	85%	$1,305	1 attack per 2.63 yrs

Note: Totals may not sum exactly due to rounding.

Regulatory Alternative 3 – Explosives Trace Detection Screening

Under this regulatory alternative, TSA continues to use the WTMD as the primary passenger screening technology and performs an ETD screening on a randomly selected population of passengers after WTMD screening. ETD screening involves swabbing a surface or individual and then testing the swab for traces of explosives. TSA found that additional ETD screening somewhat addresses the threat of non-metallic explosives but did not provide the same level of security effectiveness as AIT due to the more limited detection capability of ETD.

TSA identified a number of disadvantages to this alternative. First, although ETDs would help reduce the risk of non-metallic explosives being taken through the checkpoint, ETDs cannot detect other dangerous items such as weapons and IED components made of ceramics or plastics, whereas AIT detects metallic and non-metallic anomalies concealed under clothing.

Second, incorporating ETD screening into the current checkpoint screening process can negatively impact the passenger's screening experience. An ETD screening—from swab to test results—takes approximately 20-30 seconds. The mid-point of this range (25 seconds) would slow passenger throughput to levels below the current rate of 150 passengers per hour per lane, thereby possibly increasing passenger wait times and the associated opportunity cost.

Third, while EDTs experience low mechanical issues, throughput depends on the reliability and mechanical consistency of these machines. In the rare instance where an ETD may experience a mechanical issue, throughput may slow down for an extended period of time. Additionally, alarms can and do occur from some innocuous products that may contain trace amounts of chemicals found in explosive materials, which may also impede throughput until the alarm is resolved. Finally, this alternative requires an increase in ETD consumables, including swabs and gloves.

TSA rejected this alternative in favor or deployment of AIT due to the logistical concerns of implementing this alternative, in addition to the limited capability of ETD screening to detect other non-explosive threats. Because of this limited capability, TSA did not consider Alternative 3 a viable alternative to AIT and therefore did not perform a break-even analysis.

Regulatory Alternative 4 – Advanced Imaging Technology as Secondary Screening Option

Under this regulatory alternative, TSA continues to use the WTMD as the primary passenger screening technology and performs AIT screening on a randomly selected population of passengers after WTMD screening.

TSA identified a number of disadvantages to this alternative. First, it imposes little change to the passenger screening environment pre-2008. TSA continues to use WTMDs as the primary passenger screening technology and resolves alarms with a pat-down. AIT is only used on a random basis and does not screen a majority of passengers for non-metallic items. While a pat-down may detect a non-metallic threat, this alternative uses a pat-down to resolve an alarm triggered by metallic objects. Second, this alternative also relies on the correct use of random selection to prevent individuals from exploiting a pattern or loophole in AIT screening.

Incorporating AIT screening as secondary screening would have all the disadvantages of AIT including the cost and complexity of testing and evaluating new technology, acquiring the technology, and integrating the technology into checkpoint configurations and standard operating procedures. In addition, AIT screening results in an increase in staffing over WTMD levels and includes costs to train TSOs to operate AIT.

TSA rejected this alternative in favor or deployment of AIT as the primary screening technology due to the limited effectiveness of AIT as secondary screening would add because it does not screen the majority of the passengers for non-metallic items. Because of this limited capability, TSA did not consider Alternative 4 a viable alternative to AIT and therefore did not perform a break-even analysis.

Regulatory Alternative 5 – Advanced Imaging Technology (NPRM)

TSA determined that the deployment and use of AIT as a means of screening passengers is the preferred alternative. TSA began deploying AIT machines to screening checkpoints in 2008. Currently, TSA deploys WTMDs and AIT machines as passenger screening technologies. Of these, only AIT is capable of detecting both metallic and non-metallic threats.

AIT safely screens passengers for metallic and non-metallic threats, including weapons, explosives, and other prohibited objects concealed under layers of clothing. AIT not only enhances security, it reduces the need for a pat-down among individuals with medical implants such as a pacemaker or a metal knee replacement. A passenger can be screened by an AIT machine in 12 seconds, as opposed to 150 seconds needed for a pat-down. TSA, however, maintains the option of AIT screening for all passengers. Passengers generally may decline AIT and opt instead for a pat-down to ensure an equivalent level of security.

AIT has a number of advantages over the other alternatives. AIT maintains a lower personnel cost and a higher passenger throughput rate than either the random pat-down of a high volume of passengers or ETD screening (Alternatives 2 and 3). ATR software development shifts potential threat detection from human image interpretation to an automated system. AIT systems with ATR alleviate passenger privacy concerns by eliminating observation of an individual's image. Further, TSA can upgrade the ATR software platform, which leaves the opportunity open for future advancement towards faster processing times and enhanced aviation security.

The disadvantages of AIT include the cost and complexity of testing and evaluating a new technology, acquiring the technology, and integrating the technology into checkpoint configurations and standard operating procedures. In addition, AIT screening resulted in an increase in staffing over baseline (Alternative 1) levels. Finally, costs to train TSOs to operate AIT exceed what would have been imposed on TSA under some of the other alternatives considered.

Lastly, there exists potential for negative public perception of the health impacts from the use of backscatter AIT machines. Although TSA no longer uses backscatter machines at the screening checkpoints, this technology has been independently evaluated by CDRH, NIST, and the Johns Hopkins University APL, and all results confirm that the radiation doses for the individuals being screened, operators, and bystanders are well below the dose limits specified by the American National Standards Institute.[168] While TSA ensures the impact of backscatter and millimeter wave technologies are within industry standards, it may not be accepted by a portion of the flying public, increasing passenger opportunity costs as a result of opting out of the AIT screening in favor of a pat-down. TSA's PMIS reports that the opt-out rate peaked in December 2010 at 1.6 percent but steadily declined to 0.9 percent as of January 2013.

---

[168] ANSI/HPS N43.17 – 2002, American National Standard Radiation Safety for Personnel Screening Systems Using X-rays, ANSI/HPS N43.17 – 2009 Final for Publication, American National Standard Radiation Safety for Personnel Screening Systems Using X-ray or Gamma Radiation, 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]).

Chapter 2 of this RIA contains a comprehensive cost analysis of this preferred alternative and Table 57 presents the break-even analysis.

Table 56 summarizes the four alternatives along with the advantages and disadvantages of each. After weighing the advantages and disadvantages of each alternative, TSA elected to deploy AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats.

Table 56: Advantages and Disadvantages of Regulatory Alternatives

Regulatory Alternative	Name	Description	Advantages	Disadvantages
1	WTMDs Only	The passenger screening environment remains unchanged. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.	• No additional cost burden. • No additional perceived privacy concerns.	• Fails to meet the January 7, 2010 Presidential Memorandum and statutory requirement in 49 USC 44926.[169] • Does not mitigate the non-metallic threat to aviation security.
2	Pat-Down	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by with a pat-down on a randomly selected portion of passengers.	• Thorough physical inspection of metallic and non-metallic items. • Uses currently deployed WTMD technology. • Minimal technology acquisition costs.	• Employs a substantial amount of human resources. • Increase in number of passengers subject to a pat-down. • Increased wait times.

[169] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack

Regulatory Alternative	Name	Description	Advantages	Disadvantages
3	ETD Screening	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses the threat of non-metallic explosive threats.	• Does not detect non-explosive non-metallic potential threats. • Increased wait times and associated passenger opportunity cost of time. • Increase in ETD consumable costs.
4	AIT as Secondary Screening	TSA continues to use WTMDs as the primary screening technology. TSA supplements the WTMD screening by conducting AIT screening on a randomly selected portion of passengers after screening by a WTMD	• Somewhat addresses non-metallic explosive threats.	• Primary screening does not detect non-metallic weapons or explosives • Incremental cost of deployment of AIT.

Regulatory Alternative	**Name**	**Description**	**Advantages**	**Disadvantages**
5	AIT	TSA uses AIT as a passenger screening technology. Alarms resolved through a pat-down.	• Addresses the threat of non-metallic explosives hidden on the body by safely screening passengers for metallic and non-metallic threats. • Maintains lower personnel cost and higher throughput rates than the other alternatives. • Adds potential deterrence value—the effect of would be attackers becoming discouraged because the increased security of AIT would result in a reduction of the likelihood of a successful attack.	• Incremental cost of acquisition to TSA. • Incremental personnel cost to TSA. • Incremental training cost to TSA.

CHAPTER 4: AIT DEPLOYMENT BENEFITS

The background section (Chapter 1) of this document and the rule preamble present a thorough discussion of the need for AIT and the qualitative benefits of the technology. This chapter summarizes monetized passenger time-savings benefits, presents a break-even analysis to frame the relationship between the potential benefits of the rulemaking and the costs of implementing the rule, and presents a qualitative discussion of other related benefits from AIT.

How AIT Increases Security

The primary benefit from AIT is the enhanced security it provides to passengers, aircraft operators, and commercial aviation as a whole. AIT is the most effective technology available that detects non-metallic potential threats concealed under clothing and is an essential component of TSA's comprehensive approach to providing security to commercial aviation.[170] Since TSA began using AIT, TSA has detected many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the WTMD. Specifically, since January 2010, this technology has helped TSA officers detect hundreds of prohibited, dangerous, or illegal items concealed on passengers.[171] TSA's procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of potential threats concealed under an individual's clothing. While TSA keeps the detection requirements of AIT classified, the procurement specifications require that any approved system be sensitive enough to detect small items.

TSA's experience confirmed that AIT will detect metallic and non-metallic items, including material that could be in various forms concealed under an individual's clothing. Instances of non-metallic items found using AIT have been discussed on TSA's blog.[172] For example, TSA

---

[170] TSA bases this claim on comparative analysis conducted by TSA's Office of Security Capabilities in lab and field tests on AIT and alternative methods.
[171] Remarks of TSA Administrator John S. Pistole, Homeland Security Policy Institute, George Washington University, November 10, 2011.
[172] http://blog.tsa.gov

discovered a non-metallic martial arts weapon called a "Tactical Spike" in the sock of a passenger in Pensacola, Florida after being screened by AIT.[173]

AIT proves to be very effective at detecting objects intentionally hidden by passengers, which could pose a threat.[174] [175] Some of the items discovered concealed on passengers during AIT screening are small items, such as weapons made of composite, non-metallic materials, including a three-inch pocket knife hidden on a passenger's back; little packets of powder, including a packet the size of a thumbprint; and a syringe full of liquid hidden in a passenger's underwear.[176] AIT detected a plastic dagger hidden in the hemline of a passenger's shirt[177] and a plastic dagger concealed inside a comb in a passenger's pocket.[178] AIT's capability to identify these small items is important because, in addition to weapons and explosive materials, TSA also searches for improvised explosive device components, such as timers, initiators, switches, and power sources. Such items may be very small. AIT enhances TSA's ability to find these small items and further assists TSA in detecting threats.

AIT is also effective in detecting metallic items. In December 2011, AIT discovered a loaded .38 caliber firearm in an ankle holster at Detroit Metropolitan Airport.[179] The versatility of AIT in detecting both metallic and non-metallic concealed items makes it more effective and efficient than WTMDs as a tool to protect transportation security. In addition, TSA risk reduction

---

[173] "TSA Week In Review: Non Metallic Martial Arts Weapon Found with Body Scanner," http://blog.tsa.gov/2011/12/tsa-week-in-review-non-metallic-martial.html.

[174] The Inspector General of DHS recently conducted covert testing of TSA aviation security screening and the Secretary has directed TSA to undertake a number of steps to enhance security capabilities and techniques. See, e.g., Statement by Secretary Jeh C. Johnson On Inspector General Findings on TSA Security Screening, Press Release, June 1, 2015. TSA's response to the Inspector General's findings and the changes TSA has implemented to address those findings were discussed in the testimony of TSA Administrator Peter V. Neffenger before the Senate Committee on Appropriations, Subcommittee on Homeland Security on September 29, 2015. See https://www.tsa.gov/news/testimony/2015/09/29/testimony-tsa-efforts-address-oig-findings.

[175] DHS Office of the Inspector General, "DHS OIG Highlights: Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints", September 22, 2015, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG-15-150-Sep15.pdf

[176] "Advanced Imaging Off To a Great Start," April 20, 2010, at http://blog.tsa.gov/2010/04/advanced-imaging-technology-off-to.html and "Advanced Imaging Technology – Yes, It's Worth It," March 31, 2010, at http://blog.tsa.gov/2010/03/advanced-imaging-technology-yes-its.html.

[177] "TSA Week in Review: Plastic Dagger Found With Body Scanner," May 4, 2012, at http://blog.tsa.gov/2012/05/tsa-week-in-review-plastic-dagger-found.html.

[178] "TSA Week in Review: Comb Dagger Discovered With Body Scanner, 28 Loaded Guns, and More," August 17, 2012 at http://blog.tsa.gov/2012/08/tsa-week-in-review-comb-dagger.html.

[179] http://blog.tsa.gov/2011/12/loaded-380-found-strapped-to-passengers.html.

analysis shows that the chance of a successful terrorist attack on aviation targets generally decreases as deployment of AIT increases.

TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. Devices have been, and will continue to be, constructed and intentionally hidden on parts of the body in an effort to defeat current security protocols. Since 2001, the use of non-metallic bombs highlights the adaptive nature of terrorists. Terrorists attempt to evade detection, and as historical evidence shows, develop weapons not detectable by WTMDs. AIT enhances the passenger screening environment in two distinct ways: AIT can detect non-metallic items as well as detect items concealed on sensitive parts of the body. AIT represents TSA's best available security measure against these emerging and changing threats.

TSA also considered the added benefit of deterrence—the effect of would-be attackers becoming discouraged as a result of increased security measures—from AIT. Morral and Jackson (2009) stated that "Deterrence is also a major factor in the cost effectiveness of many security programs. For instance, even if a radiation-detection system at ports never actually encounters weapon material, if it deters would be attackers from trying to smuggle such material into the country, it could easily be cost-effective even if associated program costs are very high."[180] Given the demonstrated ability of AIT to detect concealed metallic and non-metallic objects, it is reasonable to assume that AIT acts as deterrence to attacks involving the smuggling of a metallic or non-metallic weapon or explosive on board a commercial airplane. As an essential component in airports' layered security approach that can detect a non-metallic weapon or explosive concealed under a person's clothing, AIT plays a vital role in decreasing the vulnerability of commercial air travel to a terrorist attack. However, TSA was unable to quantify the value of deterrence from AIT.

Break-even Analysis

TSA includes a break-even analysis to compare the potential security benefits of AIT with the net costs of implementing it as a response to the public comments (please see the final rule

---

[180] Andrew R. Morral, Brian A. Jackson. "Understanding the Role of Deterrence in Counterterrorism Security." 2009. Rand Homeland Security Program. http://www.rand.org/content/dam/rand/pubs/occasional_papers/2009/RAND_OP281.pdf

section *II. Public Comments on the NPRM and TSA Responses*). When it is not possible to quantify or monetize the incremental security benefits of a regulation, OMB recommends conducting a threshold, or break-even, analysis. According to OMB Circular No. A–4, ''Regulatory Analysis,'' such an analysis answers the question, ''How small could the value of the non-quantified benefits be (or how large would the value of the nonquantified costs need to be) before the rule would yield zero net benefits?''[181] This analysis compares the net cost of AIT with the major direct consequences incurred by the types of terrorist attacks that could potentially be averted with AIT screening.

Ideally, quantifying and monetizing the security effects of AIT would be a two-step process. First, TSA would estimate the reduction in the probability of a successful terrorist attack, along with the fully quantified consequences of an attack averted by the deployment and use of AIT. These two estimates compose the total risk associated with a potential terrorist attack. Second, TSA would estimate the willingness of individuals to pay for this incremental risk reduction and apply that to the population experiencing the benefit. Willingness to pay measures the amount of money people would be willing to spend for a good or service, and is therefore a proxy for the contribution of that good or service to their well-being. Economists commonly seek to measure willingness to pay to estimate the benefits of a good or service to consumers. However, the process of measuring willingness to pay relies on critical data that are not available in order to complete this process. TSA therefore uses a break-even analysis to compare program costs with the major direct costs from a range of potential attack scenarios.

In the break-even analysis, TSA compares the estimated net costs to deploy and operate AIT against the estimated direct consequences of a successful terrorist attack. By generating a ratio between these two sets of costs, TSA estimates how small the value of non-quantified benefits would need to be for the deployment of AIT to yield zero net benefits.[182] TSA bases the costs of

---

[181] http://www.whitehouse.gov/omb/circulars_a004_a-4/

[182] The benefits used in this rule's break-even analysis are the avoidance of the major direct costs associated with a successful terrorist attack. The break-even analysis does not include the difficult to quantify indirect costs of an attack.

direct consequences from a terrorist attack from the number of fatalities and the replacement value for the aircraft destroyed in the attack.

In order to compare direct costs with direct benefits, TSA considers major direct costs of the attack scenarios. The analysis does not account for possible macroeconomic consequences of terrorist attacks, specifically the indirect benefits (in terms of avoided indirect costs), from preventing a successful terrorist attack. Given this omission, the associated costs from the attacks scenarios, and likewise the full benefits of AIT screening are underestimated in this break-even analysis. In addition to the direct impacts of a terrorist attack in terms of lost life and property, there are other more indirect impacts, particularly on aviation based terrorist attacks, that are difficult to measure. For example, one study estimates the 9/11 attacks as causing a .5 percentage decrease in GDP growth (or $60 billion dollars) and an upper bound estimate of twice that or $125 billion (in 2006 dollars).[183] Also, as noted by Cass Sunstein in the Laws of Fear, "…fear is a real social cost, and it is likely to lead to other social costs. If, for example, people are afraid to fly, the economy will suffer in multiple ways…"[184] In addition, Ackerman and Heinzerling state "…terrorism 'works' through the fear and demoralization caused by uncontrollable uncertainty. Efforts to offset this fear by attaching necessarily arbitrary numbers to the probabilities of being harmed by a terrorist seem, especially in a post-September 11 world, ridiculous."[185] Further, Pidgeon, Kasperson and Slovic state the 9/11 attacks had consequences that spanned "a range of behavioral, economic, and social impacts…"[186] Another study estimates at least 1,200 additional driving deaths were attributable to the effect of 9/11 as people substituted less-safe surface transportation for safer air transportation, as noted by these authors "Our results show that the public response to terrorist threats can create unintended consequences that rival the attacks themselves in severity."[187] In conclusion, as devastating as the direct impacts of a successful terrorist attack can be in terms of the immediate loss of life and

---

[183] S. Brock Blomberg and Gregory D. Hess, "*Estimating the Macroeconomic Consequence of 9/11*," Peace Economics, Peace Science and Public Policy, Volume 15 Issue 2 Article 7, 2009.
[184] Cass R. Sunstein, "Laws of Fear" p.127, 2005.
[185] Frank Ackerman and Lisa Heinzerling, "Priceless On Knowing the Price of Everything and the Value of Nothing," p.136-137, 2004
[186] Nick Pidgeon, Roger E. Kasperson, and Paul Slovic, "The Social Amplification of Risk," p.16, 2003
[187] Blalock et al, "*The Impact of 9/11 on Road Fatalities: The Other Lives Lost to Terrorism*" February 2, 2005. Abstract and page 1. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=677549

property, avoiding the impacts of the more difficult to measure indirect effects are also substantial benefits of preventing a terrorist attack.

Scenarios

TSA used five types of aircrafts to represent five different scenarios where an attacker detonates a body-bomb on a domestic passenger aircraft, the type of attack AIT is meant to mitigate. The five types of aircraft fall into two assigned categories: high-capacity, long range aircrafts typically used for international travel; and a medium-capacity and -range aircrafts typically used for cross-country travel or popular routes. TSA used the Bureau of Transportation Statistics' T-100 domestic segment data from 2014 to determine the most popular aircraft models for each of the categories of aircrafts. [188] The most popular aircraft models of 2014 are defined as the aircraft that had the most departures performed and carried the most passengers.[189] TSA also selected the Airbus A380 and the Boeing 777-200 for this analysis because they are likely targets due to their higher seat capacity. TSA used the T-100 from 2014 to determine the average load factor for each aircraft type. [190] The load factor for each aircraft type is found by dividing the total sum of passengers by the sum of available seats for each aircraft type.

These aircrafts were used in the break-even analysis and are listed below along with their specifications:

High Capacity

- Airbus A380 – Airbus' long-range aircraft with a 544 seat capacity[191] and an average crew size of 13 (557 occupancy total)[192] with a market value of $428.0 million[193].

[188] U.S. Department of Transportation, Bureau of Transportation Statistics. "T-100 Domestic Segment (All carriers) Data bank". http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air. Selected fields: DepPerformed, Aircraft Type, and Year = 2014, All months.
[189] Boeing 737-700/700LR, Boeing 737-800, and Airbus A320-100/200 are the first-, fourth-, and fifth-most often-used aircrafts in 2014, respectively.
[190] U.S. Department of Transportation, Bureau of Transportation Statistics. "T-100 Domestic Segment (All carriers) Data bank". http://www.transtats.bts.gov/DL_SelectFields.asp?Table_ID=311&DB_Short_Name=Air. Selected fields: Seats, Passengers, Aircraft Type, and Year = 2014, All months.
[191] Airbus.com. "A380 Dimensions & Key Data". Accessed August 12, 2015. http://www.airbus.com/aircraftfamilies/passengeraircraft/a380family/specifications/

- Boeing 777-200LR – Boeing's long-range aircraft with 317 seat capacity[194] and an average crew size of 9 (323 occupancy total)[195] and a market value of $305.0 million[196].

Medium Capacity

- Boeing 737-700/700LR – A medium-range aircraft with a seating capacity range between 126 and 149 (median of 138 used to represent passengers and crew)[197] and a market value of $78.3 million[198].
- Boeing 737-800 – A medium-range aircraft with a seating capacity range between 162 and 189 (median of 176 used to represent passengers and crew)[199] and a market value of $93.3 million[200].
- Airbus A320-100/200 – A medium-range aircraft with a 150 seat capacity[201] and crew size of 6 (156 occupancy total)[202] and a market value of $97.0 million[203].

To conduct the break-even analysis, TSA estimated the direct costs for these attack scenarios. Preventing these direct costs from being incurred by society is a proxy of the potential benefits of using AIT to avoid such attack. TSA assumed 100 percent fatality[204] and used the value of

---

[192] Estimated thirteen crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and ten flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391 which state there must be at least one flight attendant per 50 passenger seats.
[193] Airbus.com. "New Airbus aircraft list prices for 2015". http://www.airbus.com/newsevents/news-events-single/detail/new-airbus-aircraft-list-prices-for-2015/
[194] Boeing.com. "777-200/-200ER Technical Characteristics". Accessed August 12, 2015. http://www.boeing.com/boeing/commercial/777family/pf/pf_200product.page
[195] Estimated nine crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and six flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391 which state there must be at least one flight attendant per 50 passenger seats.
[196] Boeing.com. "Commercial Airplanes Jet Prices". http://www.boeing.com/boeing/commercial/prices/
[197] Boeing.com. "737-700 Technical Characteristics". Accessed August 12, 2015. http://www.boeing.com/boeing/commercial/737family/pf/pf_700tech.page
[198] Boeing.com. "Commercial Airplanes Jet Prices". http://www.boeing.com/boeing/commercial/prices/
[199] Boeing.com. "737-800 Technical Characteristics". Accessed August 12, 2015. http://www.boeing.com/boeing/commercial/737family/pf/pf_800tech.page?
[200] Boeing.com. "Commercial Airplanes Jet Prices". http://www.boeing.com/boeing/commercial/prices/
[201] Airbus.com "A320 Setting single aisle standards, Dimensions & Key Data". Accessed August 12, 2015. http://www.airbus.com/aircraftfamilies/passengeraircraft/a320family/a320/specifications/.
[202] Estimated six crew members is a TSA assumption. This estimate is based on the crew consisting of a pilot, copilot, flight engineer, and three flight attendants. The number of flight attendants is based on the minimum requirements from 14 CFR 121.391 which state there must be at least one flight attendant per 50 passenger seats.
[203] Airbus.com. "New Airbus aircraft list prices for 2015". http://www.airbus.com/newsevents/news-events-single/detail/new-airbus-aircraft-list-prices-for-2015/
[204] TSA does not include for the possibility that there are fatalities on the ground or secondary and tertiary economic effects.

statistical life (VSL) of $9.1 million per fatality, as adopted by the U.S. Department of Transportation (DOT)[205], to monetize the consequences from fatalities. TSA emphasizes that the VSL is a statistical value used only for regulatory comparison and does not suggest that the actual value of a life can be stated in dollar terms. Although it is possible for an attacker to detonate an explosive on an airplane without downing the airplane, only causing immediate casualties to those sitting near the attacker, there are examples of airplanes being downed from an explosion. TSA is unable to precisely quantify the resiliency of aircraft to all types of attacks taking into account the various factors that may occur in an explosion (e.g. where the attacker is seated, how much and type of explosives). Terrorists are also conscious opponents in that they are seeking to down the airplane and will likely target vulnerable areas of the aircraft to detonate their explosives. Given the imprecise nature of quantifying these factors and their associated risk, along with the fact that terrorists are constantly changing strategies to seek the most vulnerable area of an aircraft, TSA uses the break-even analysis. A break-even analysis squarely focuses on measuring the threshold of successful attacks—those that meet the terrorist goal of downing the aircraft—that need to be averted for the cost of AIT to equal its quantified benefits and does not attempt to measure the precise decrease in risk .

The replacement cost of the aircraft and emergency response costs[206] [207] are added to the loss of life to sum up the total direct cost of each attack scenario. TSA then calculates the ratio between the estimated cost of a successful attack and the annualized cost of AIT using a seven percent discount rate.[208] By generating a ratio between these costs, TSA estimates how small the value of non-quantified benefits would need to be for the deployment of AIT to yield zero net benefits.

---

[205] U.S. Department of Transportation. "Guidance on Treatment of Economic Value of a Statistical Life in U.S. Department of Transportation Analyses". http://www.dot.gov/sites/dot.dev/files/docs/VSL%20Guidance%202013.pdf.

[206] TSA uses a proxy estimate of $869,552 (inflated from $800,000 in 2009 dollars) from a lawsuit filed by The County of Erie, New York to recuperate emergency response costs from Colgan Air, Inc. in response to the Colgan Air Flight 3407 crash. These costs include overtime, removal of human remains, cleanup of the aircraft and chemical substances, counseling for the surviving family members, and acquiring special equipment.

[207] McGrory, Michael, "Airlines Not Liable for Colgan Air Crash Clean-Up Costs", *SmithAmunden Aerospace Report*, March 20, 2013, http://www.salawus.com/insights-alerts-70.html

[208] TSA estimates the annualized net cost of AIT deployment to be $204.57 million using a seven percent discount rate.

Break-even Analysis Results for AIT

TSA makes the comparison between the estimated consequence and the annualized cost of AIT using a seven percent discount rate. Table 57 presents the number of attacks averted (expressed as a number of years between attacks) which comes as a result of comparing the annualized cost of the deployment of AIT to all five attack scenarios.

Table 57: Frequency of Attacks Averted to Break-Even for AIT (in $millions)

Aircrafts	Replacement & Emergency Response Costs a	Total Passengers + Crew b	Load Factor c	Total Consequence d = a + (b × c × VSL)	Attacks Averted by AIT to Break-Even: Total Consequence / $204.57M e = d ÷ $204.57M
High Capacity					
Airbus A380	$428.9	557	86%	$4,811	1 attack per 23.52 yrs
Boeing 777-200	$305.9	326	84%	$2,791	1 attack per 13.64 yrs
Medium Capacity					
Boeing 737-700/700LR	$79.2	138	80%	$1,075	1 attack per 5.25 yrs
Boeing 737-800	$94.2	176	84%	$1,434	1 attack per 7.01 yrs
Airbus Industries A320-100/200	$97.9	156	85%	$1,305	1 attack per 6.38 yrs

Note: Totals may not sum exactly due to rounding.

CHAPTER 5: NPRM AND FINAL RULE COMPARISON

The regulatory impact analyses accompanying both the NPRM and the final rule estimate costs from the same baseline—the airport screening environment prior to the deployment of AIT. TSA made changes to the NPRM RIA based on public comments on newly available data. This chapter highlights the changes made and their impact to estimated costs and benefits of AIT deployment.

TSA modified or updated many population projections, data, and assumptions from the regulatory impact analysis that accompanied the NPRM. TSA made some of these updates, such as those for initial populations and compensation rates, to reflect more recently available data. TSA received updated information from TSA's OSC regarding the deployment and life cycle cost of AIT. TSA revised the AIT deployment schedule from its original estimate in the NPRM, which includes revising estimates from the previous years (2008-2014) and projected years (2015-2017) with respect to the number of AIT machines deployed and the category of airport to which they were deployed. TSA's passenger screening program is a dynamic endeavor and TSA continually seeks to improve its process. Some of the revisions to the NPRM are due to exogenous factors—for example an AIT was deployed to an airport in 2008 that was category II at the time but has since been reclassified as Category I—while some revisions were corrections revealed in TSA's continually improving data management process. Additionally, AITs can be relocated to other airports within the same year or taken out service and not return to a checkpoint until the following year. This makes it difficult for TSA to provide annual numbers as it ignores the fluidity of the AIT program.

TSA's OTD provided more detailed information on personnel training on AIT for both historical and projected years. Further, TSA updated the federalized airport population to include 460 airports regulated under 49 CFR part 1542 within the period of this analysis. Other changes, such as the inclusion of the monetized passenger benefits and a break-even analysis in the benefits chapter, were in response to public comments received after the publication of the NPRM.

In summary, TSA's changes in the RIA from the NPRM are:

- Revising the airport listings to include 460 airports instead of 448. The updated airport list includes new, previous, and former airports that operated AIT units and are regulated under 49 CFR part 1542;
- Updating the AIT life cycle and period of analysis from 8 to 10 years based on a recent life cycle cost estimate (LCCE) report[209] from OSC. Using the information from this report, TSA also revised its previous assumption about the share of Passenger Screening Program (PSP) expenditures spent on AIT technology;
- Revising the number of AIT units to be deployed from 821 to 793 based on new data;[210]
- Revising the total wait time for passenger that opts-out from 80 to 150 seconds to include passenger time spent waiting for a same gender TSO to perform the pat-down;
- Revising the calculation of utilities costs to incorporate new data on the hours of AIT operation from the TSA's Performance Management Information System (PMIS) database;
- Refining the calculation of personnel costs by using information on specific labor hours dedicated to AIT operation in response to new data on hours of AIT operation;
- Revising the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs;
- Including a break-even analysis to estimate how small the value of non-quantified benefits would need to be for the deployment of AIT to yield zero net benefits; and
- Revised language within the RIA and final rule to state that passengers "may generally opt-out of AIT screening" to reflect current DHS policy issued at in December 2015.[211]

The revisions listed above are a result of public comments, acquirement of more complete data, and revisions to previous estimates since TSA published the NPRM. Table 58 presents a summary of the effects these changes from the NPRM to the final rule had on the costs and

---

[209] TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" March 10, 2014. This is a TSA internal acquisition sensitive information report based on OSC technology assessments.
[210] The number of AIT machines in the field is a dynamic estimate. TSA may add or remove AIT machines abruptly for the purpose of addressing security risks or increasing efficiency in its passenger screening program.
[211] https://www.dhs.gov/sites/default/files/publications/privacy-tsa-pia-32-d-ait.pdf

benefits in the RIA. In the table, NPRM and final rule costs have been annualized due to the different periods of analysis.

Table 58: Changes in AIT Estimates from the NPRM to the Final Rule (Annualized at a 7% Discount Rate in 2014 dollars)

Variables	NPRM and FR Comparison			Description of Changes
	NPRM	Final Rule	Difference	
Annualized Industry Costs ($millions)				
Airport Utilities Cost	$0.19	$0.15	-$0.04	This estimate decreased due to incorporation of newly available historical data on AIT hours of operation from the TSA's PMIS database.
Backscatter AIT Removal	$0.21	$0.18	-$0.03	Total cost in constant dollars remained the same, but annualized cost decreased because of the different periods of analysis between NPRM and final rule.
Annualized Passenger Costs ($millions)				
Opportunity Costs (Delay Costs)	$2.08	$2.60	$0.52	This estimate increased because the estimated duration of a pat-down increased from 80 to 150 seconds to include passenger wait time to be handed off to a same gender TSO.
Annualized TSA Costs ($millions)				

Variables	NPRM and FR Comparison			Description of Changes
	NPRM	Final Rule	Difference	
Personnel	$216.40	$117.17	-$99.22	TSA refined this estimate to account for labor hours dedicated to AIT operation. TSA used AIT operational hours recorded in PMIS as a basis for this estimate.
Training	$5.81	$27.68	$21.87	TSA revised the calculation of training costs to incorporate newly available historical data on the hours of participation for each training course required for AIT operation and new training and development costs.
Equipment	$70.62	$56.53	-$14.08	TSA revised its cost estimates in 2014 -2017 to reflect the most recent LCCE document by OSC. TSA also revised some assumptions for cost estimates from 2008-2013 based on the recent LCCE.

Variables	NPRM and FR Comparison			Description of Changes
	NPRM	Final Rule	Difference	
TSA Utilities Cost	$0.25	$0.26	$0.01	This change reflects the revised estimate on AIT operation time and an increase of airport enrollment in TSAs utilities reimbursement program.
Total Costs	**$295.56**[212]	**$204.57**	-$90.99	The total cost decreased from the NPRM, primarily from the reduction in personnel costs.
Benefits				
Break-Even Analysis	Prevent 1 attack per 5.25 to 23.52 years considering only the major direct costs of an averted attack			Per public comment, TSA has included a break-even analysis in the RIA.

[212] There was a calculation error in the NPRM's presentation of annualized costs. TSA has resolved this error and presented the correct annualized amounts in Tables 1 and 58 of this RIA. The calculation error in annualized costs did not affect any other cost estimates in the NPRM, including the estimated total cost of the rule and the estimated itemized costs presented in the NPRM.
.

CHAPTER 6: FINAL REGULATORY FLEXIBILITY ANALYSIS

Summary of the NPRM IRFA

The Transportation Security Administration (TSA) performed an initial regulatory flexibility analysis (IRFA) on the impacts on small entities in the NPRM. TSA performed this assessment using the cost information discussed in Chapter 2 of the Initial RIA. TSA determined that AIT would not result in a significant economic impact on a substantial number of small entities under section 605(b) of the Regulatory Flexibility Act. TSA's Final Regulatory Flexibility Analysis suggests that this rule would not have a significant economic impact on a substantial number of small entities under section 605 (b) of the RFA. Below is a summary of the IRFA findings:

- TSA estimated that there are 446 U.S. airports affected by the AIT deployment, of which 97 are considered small. Of the 97 small airports, 96 are owned by small governmental jurisdiction with population of less than 50,000, and one is a small privately-owned airport.
- These small entities incur additional utilities costs as a result of increased power consumption from AIT operations. The estimated average additional utilities costs ranged from $723 to $1446 per year.
- TSA estimated that the costs of AIT deployment resulted in less than 1 percent impact on revenue for 100 percent of the small entities.

Changes from the NPRM IRFA

Since the IRFA, the number of federalized airports increased from 446 to 460, and the expected number of small entities affected by the deployment of AIT decreased from 97 to 7. This is due to the changes in procurement and allocation of AIT in smaller airports. As a result 90 of the original 97 small entities are no longer projected to incur costs as a result of the deployment of AIT.

Final Regulatory Flexibility Analysis (FRFA)

The Regulatory Flexibility Act of 1980 (Public Law 96-354) establishes "as a principle of regulatory issuance that agencies shall endeavor, consistent with the objectives of the rule and of applicable statutes, to fit regulatory and informational requirements to the scale of the businesses, organizations, and governmental jurisdictions subject to regulation. To achieve this principle, agencies are required to solicit and consider flexible regulatory proposals and to explain the rationale for their actions to assure that such proposals are given serious consideration."

When an agency promulgates a final rule under 5 U.S.C. 553, after being required by that section or any other law to publish a general notice of proposed rulemaking, or promulgates a final interpretative rule involving the internal revenue laws of the United States as described in section 603(a), the agency must prepare a final regulatory flexibility analysis (FRFA) or have the head of the agency certify pursuant to RFA section 605(b) that the rule will not, if promulgated, have a significant economic impact on a substantial number of small entities. The RFA prescribes the content of the FRFA in section 604(a), which is discussed below.

(1) a statement of the need for, and objectives of, the rule;

By Federal regulation, "no individual may enter a sterile area or board an aircraft without submitting to the screening and inspection of his or her person and accessible property in accordance with the procedures being applied to control access to that area or aircraft…" 49 C.F.R. 1540.107(a). The final rule amends this regulation to specify that the screening and inspection of a person may include the use of AIT.

In addition, Federal law requires that AIT used to screen passengers must be equipped with and employ automatic targeting recognition (ATR) software (49 U.S.C. 44901(l)). The final rule adopts the statutory definition of both AIT and ATR and requires that any AIT equipment used to screen passengers be equipped with and employs ATR software.

TSA adopted the final rule to comply with a ruling of the United States Court of Appeals for the District of Columbia Circuit. In Electronic Privacy Information Center (EPIC) v. U.S. Department of Homeland Security (DHS), 653 F.3d 1 (D.C. Cir. 2011), the court directed TSA to conduct notice-and-comment rulemaking on the use of AIT to screen passengers. TSA published a notice of proposed rulemaking (NPRM) on March 26, 2013, to obtain public comment on its proposal to revise civil aviation security regulations to codify that TSA may use AIT for passenger screening (78 FR 18287). The final rule defines AIT, states that AIT may be used to screen passengers, and requires that AIT be equipped with and employ the use of ATR software.

(2) a statement of the significant issues raised by the public comments in response to the initial regulatory flexibility analysis, a statement of the assessment of the agency of such issues, and a statement of any changes made in the proposed rule as a result of such comments;

On March 26, 2013, TSA published the Notice or Proposed Rulemaking (NPRM) entitled Passenger Screening Using Advanced Imaging Technology in the Federal Register (78 FR 18287). TSA summarized these comments in the final rule section *II. Public Comments on the NPRM and TSA Responses*. TSA reviewed comments raised by the public in response to the IRFA. Two commenters recommended that the analysis estimate the costs incurred by small business entities, such as sole proprietors. The commenters claimed that the impacts on small entities would include time lost as well as lost revenue from tourists (e.g., fewer air travelers, both foreign and domestic). An advocacy group suggested that the NPRM erroneously excludes individuals from the definition of "small entities." The commenter argues that TSA must publish and allow comment on a new RFA analysis that takes into consideration the impact of the proposed rule on individuals in their capacity as "small entities". The commenter stated that many individual travelers are self-employed individuals and sole proprietors that qualify as small entities. The commenter estimated that the impact on "small entities" is at least $1.8 billion per year.

TSA was unable to find evidence that air travel is reduced due to AIT. Further, TSA notes that since it began using AIT to screen passengers, only one percent of passengers requested a pat-down over AIT.[213]

TSA also did not include individuals as "small entities" because they are not considered as such according to the definition of small entities in the Regulatory Flexibility Act (5 U.S.C. § 601). Nevertheless, TSA considered the impact to individuals in Chapter 2 of the RIA and determined that the main impact on a person traveling would be the extended wait time if that person opts out of AIT screening and undergoes a pat-down. As stated in the RIA, AIT does not increase wait time for the general traveling public. TSA measured the ratio of individuals who opt-out of AIT to be approximately one percent of the total volume of passengers screened. Additionally, the pat-down for individuals who opt-out is estimated to be 150 additional seconds per screening, and would not reflect a significant opportunity cost impact ($1.88 per screening).

(3) the response of the agency to any comments filed by the Chief Counsel for Advocacy of the Small Business Administration in response to the proposed rule, and a detailed statement of any change made to the proposed rule in the final rule as a results of the comments.[214]

The Small Business Administration did not submit any comments during the comment period for the NPRM.

(4) a description of and an estimate of the number of small entities to which the rule will apply or an explanation of why no such estimate is available;

TSA's FRFA suggests that this rulemaking would not have a significant economic impact on a substantial number of small entities under section 605(b) of the RFA. The SBA defines a government-owned airport as a small entity if the owning government entity has a population of less than 50,000 people. Similarly, the SBA defines a privately-owned airport as a small entity if

---

[213] Elliott, Christopher. "Speak out no on the TSA's full-body scanners. "*Chicago Tribune*. April 23, 2013. http://articles.chicagotribune.com/2013-04-23/lifestyle/sns-201304230000--tms--traveltrctntt-b20130423-20130423_1_tsa-agents-body-scanners-advanced-imaging-technology
[214] This section of 604(a) has been added by the Small Business Jobs Act of 2010.

annual revenue amounts to less than $30 million. Privately-owned airports are classified in NAICS code 488119. TSA finds that seven airports run by governments, and are considered small entities, incur additional utilities costs.

The RIA also includes additional costs to industry (i.e., costs incurred by the manufacturer of the backscatter AITs). However, TSA does not consider this manufacturer to be a small entity based on employment size of their parent company which is classified as NAICS code "Semiconductor and Related Devices Manufacturing" (334413). The parent company reports having 4,000 employees, which exceeds the 500 employee threshold to be considered small under SBA size standards for that industry.[215]

TSA uses FAA data to identify the affected airports, owners, or owning entity. TSA determined the population served by each airport owner primarily using U.S. Census data (for counties and cities). Revenue data for counties and cities with populations above 25,000 are based on 2007 U.S. Census City and County Data book.[216] For those jurisdictions where revenue figures could not be found in the Census City and County data books, TSA used revenue data from one of the following sources:

- The city's annual financial report (CAFR), when available online.
- www.city-data.com, a web site that compiles data from various government databases.
- The owner's annual financial report to the FAA.[217]

TSA presents all revenue data to 2013 dollars. To avoid double-counting the population, for airports that are owned by both a county and one or more cities within that county, TSA used county population and revenue from both the county and the city.[218]

Of the 460 airports regulated under 49 CFR part 1542, TSA identified a total of 106 small entities; seven of which are currently incurring additional utilities costs due to this rule. Small

---

[215] http://files.shareholder.com/downloads/OSIS/2340310712x0x611139/7CC050BD-4B0D-4756-B76A-150EED5FBA20/OSI_Systems_Annual_Report_2012.pdf, Page 8 lists the approximate number of employees.
[216] The 2007 Census City and County Data book states revenue data in constant 2002 dollars. TSA uses a 2002 GDP factor of 1.230 to convert all revenue data to constant 2011 dollars. https://www.census.gov/prod/2008pubs/07ccdb/ccdb-07.pdf.
[217] The FAA financial data cover only airport revenues and, therefore, understate the financial resources of the owning government.
[218] TSA does not use county populations when cities and counties are geographically independent.

governmental jurisdictions comprise 105 of the 106 small entities. TSA also identified one privately owned business. However, TSA was unable to determine from publically available data if this business is a small entity. To be conservative, TSA assumes this privately owned airport is a small business. Of the 105 small governmental jurisdictions, TSA reimburses the cost of utilities for eight of them. Of the 106 small entities, seven currently have AITs deployed and are not reimbursed for their utilities. Consequently, TSA estimates seven small entities or 1.5 percent of all airports (7/460) incur additional direct costs in the period of this analysis. Table 59 displays the number of airports and the number of small airports by category.

Table 59: Description of Affected Small Entities

FAA Category	Number of Airports	Number of Small Entities	Number of Small Entities Reimbursed	Number of Small Entities with AIT	Number of Small Entities with AIT and Reimbursed
X	28	0	0	0	0
I	56	0	0	0	0
II	78	7	2	7	0
III	131	19	1	0	0
IV	167	80	5	0	0
Total	**460**	**106**	**8**	**7**	**0**

(5) a description of the projected reporting, recordkeeping and other compliance requirements of the rule, including an estimate of the classes of small entities which will be subject to the requirement and the type of professional skills necessary for preparation of the report or record; and

The final rule imposes no recordkeeping and reporting requirements.

Estimated Cost and Impact as a Percentage of Revenue

In this FRFA, TSA includes the additional utilities costs incurred by airport operators. To estimate the costs that the deployment of AIT has on the seven small entities that are currently incurring costs, TSA uses the average kilowatt hour (kWh) consumed per unit using data available from the U.S. Energy Information Administration,[219] the number of hours these AITs are in operation, and the number of AITs deployed at these airports on an annual basis to derive a per-unit daily cost of $2.01 to operate AIT at a small airport.[220] The $2.01 per-unit daily cost only takes into account the hours of operation at small entity airports, instead of all airports, therefore the per-unit cost differs from that as illustrated in the utilities sections in Chapter 2 of this RIA. TSA multiplies the daily cost ($2.01) by the number of AITs at any small entity airport by the number of days in a calendar year (365.25).

TSA estimates the average additional utilities costs to range by airport from $290 to $921 per year while the average annual revenue for these small entities ranges from $8.4 million to $212.3 million per year.[221] To be conservative TSA assumes that these small entities incur additional utilities costs throughout the entire duration of this analysis. Consequently, TSA estimates that the cost for the deployment of AIT on small entities ranges from 0.0003 percent to 0.0087 percent of their annual revenue. Table 60 summarizes the additional utilities cost for the seven small entities that have had AIT deployed at their airports during the 10-year period of this analysis and summarizes the impacts of AIT deployment as a percentage of their revenue. TSA opts to withhold the seven small entities' identities from the public for privacy reasons.

---

[219] TSA uses historical information for years 2008-2014 for the commercial sector as reported by the U.S. Energy Information Administration. EIA, "Short-Term Energy Outlook", Table 7c: U.S. Regional Electricity Prices (Cents per Kilowatthour), Annual Frequency, 2008-2016, Commercial Sector – U.S. Average, https://www.eia.gov/forecasts/steo/tables/?tableNumber=21#startcode=2008 . For years 2015-2017, TSA uses the projected growth rate from the U.S. Energy Information found in Table C3. Electricity price for the commercial sector. http://www.eia.gov/forecasts/aeo/pdf/0383(2015).pdf.

[220] TSA calculates the per-unit utilities cost per day average power used to perform a scan and the power used when idle. TSA estimates the average daily operation time of 5.76 hours at category II airports from years 2009-2013 with data available from PMIS. TSA estimates18.24 hours of idle time by subtracting the average daily operation time of 5.76 hours from 24 hours. TSA estimates the average kW used per hour by taking the sum of the power consumption when the system is in operation (1.02) multiplied by in the hours in operation (5.76) and the power consumption when the system is idle (0.70) multiplied by the idle hours (18.24 hours). This calculation results in an average kWh per day of 18.64 = (1.02 x 5.76) + (0.70 x (18.24). TSA then multiplies this average number of kWh per day by the ten year average cost per kWh to obtain a per-unit utilities cost per day.

[221] TSA has changed the way that utilities costs were calculated from the NPRM in order to match the operating time of an AIT with its associated cost for additional utilities consumption. The change in the revenue range for small entities from the NPRM is due to the population of airports which has been adjusted to include all airports that have entered CFR 49 Part 1542 since publication of the NPRM.

Table 60: Utilities Cost for Small Entities

(in $millions, undiscounted)

Airport		Cat	AITs	Annual Utilities Cost	Annual Revenue	Percentage of Revenue
			a	b = a x $2.01 x 365.25 ÷ 1 million	c	d = b ÷ c
SAP	Small Airport	II	1	$0.00073	$212.31	0.0003%
SAP	Small Airport	II	1	$0.00073	$123.06	0.0006%
SAP	Small Airport	II	2	$0.00147	$162.05	0.0009%
SAP	Small Airport	II	2	$0.00147	$141.30	0.0010%
SAP	Small Airport	II	2	$0.00147	$112.16	0.0013%
SAP	Small Airport	II	2	$0.00147	$76.66	0.0019%
SAP	Small Airport	II	1	$0.00073	$8.41	0.0087%
Total			11	$0.00807	$835.87	

(6) a description of the steps the agency has taken to minimize the significant economic impact on small entities consistent with the stated objectives of applicable statutes, including a statement of the factual, policy, and legal reasons for selecting the alternative adopted in the final rule and why each one of the other significant alternatives to the rule considered by the agency which affect the impact on small entities was rejected.

TSA examined four additional options as alternatives to the preferred regulatory option that could potentially reduce the burden of the rule on small entities. Chapter 3 of this RIA explains these alternatives in more detail. The alternatives considered include a continuation of the current screening environment (WTMDs only), increased use of physical pat-down searches that supplements primary screening with WTMDs, AIT use as secondary screening (with WTMD as primary), and increased use of ETD screening that supplements primary screening with WTMDs.

Without a staffing increase, passenger wait times and the associated opportunity cost increases. ETD would generate both utilities cost for small entities and a large amount of consumables for TSA. Finally, ETDs cannot detect dangerous items such as weapons and IED components made of ceramics or plastics whereas AIT is capable of detecting potential threats concealed under clothing.

After weighing the advantages and disadvantages of each alternative, TSA elected to deploy AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats.

CHAPTER 7: INTERNATIONAL TRADE IMPACT ASSESSMENT

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. The Trade Agreement Act does not consider legitimate domestic objectives, such as safety, unnecessary obstacles. The statute also requires that international standards be considered and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this final rule and has determined that it would not have an adverse impact on international trade.

CHAPTER 8: UNFUNDED MANDATES REFORM ACT ANALYSIS

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), Public Law 104–4, establishes requirements for Federal Agencies to assess the effects of their regulatory actions on State, local, and tribal governments and the private sector. Under section 202 of the UMRA, TSA generally must prepare a written statement, including a cost-benefit analysis, for proposed and final rules with ''Federal mandates'' that may result in expenditures by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million (adjusted for inflation) or more in any one year. Before TSA promulgates a rule for which a written statement is needed, section 205 of the UMRA generally requires TSA to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost effective, or least burdensome alternative that achieves the objectives of the rule. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows TSA to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the Administrator publishes with the final rule an explanation why that alternative was not adopted. Before TSA establishes any regulatory requirements that may significantly or uniquely affect small governments, including tribal governments, it must develop under section 203 of the UMRA a small government agency plan. The plan must provide for notifying potentially affected small governments, enabling officials of affected small governments to have meaningful and timely input in the development of TSA regulatory proposals with significant Federal intergovernmental mandates, and informing, educating, and advising small governments on compliance with the regulatory requirements.

TSA has determined that this rule does not contain a Federal mandate that may result in expenditures of $146 million or more in any one year (when adjusted for inflation) in 2013 dollars for either State, local, and tribal governments in the aggregate, or by the private sector.

APPENDIX: COST ESTIMATE EXPLANATION OF 2013 BACKSCATTER TECHNOLOGY REMOVAL

All general-use backscatter units that were deployed at TSA checkpoints were removed from operation by the end of May 2013. TSA removed all remaining backscatter units: 94 units in Category X, 68 in Category I, 8 in Category II, and 4 in Category III. For the purpose of this analysis, TSA assumes that these 174 backscatter machines were simultaneously removed at the end of May 2013. TSA uses weighted averages to estimate the costs given the mid-year removal and replacement of backscatters. TSA only applies the weighted average to cost categories dependent on the number of active AIT units in the field. These categories include airport utilities[222] and personnel costs.

Airport Utilities Cost

To estimate the airport utilities cost in 2013, TSA calculated a weighted average costs using two scenarios: "with backscatter units" and "without backscatter units". TSA bases airport utilities costs on the number of AIT units in non-reimbursed airports. At the end of 2013, there were 278 AITs at non-reimbursed airports. TSA counts 155 of the 174 backscatter units removed in 2013 came from non-reimbursed airports. TSA adds these AIT units to end-of-the-year in-service AITs in 2013 to estimate that there were 433 AIT units (278 + 155) in non-reimbursed airports in early 2013. TSA uses the ratio of AITs in non-reimbursed airport at the beginning of 2013 to the end of 2013 (443:278) to inflate the original estimate of AIT hours in 2013 in Table 17. Table A2 calculates the streams of utilities costs for AIT for the full year in 2013 under both scenarios—with backscatter units (443 AITs) and without backscatter units (278 AIT units)—and takes the weighted average of both to calculate the airport utilities costs for 2013.

[222] Utilities cost to TSA from AITs in reimbursed airports are based upon new, updated data after 2013. These numbers take into account the changes from in mid-2013 and therefore do not require any adjustments. TSA bases the utilities costs to industry on their calculation of AITs from deployment data and AITs in reimbursed airports. TSA uses a weighted average to account for the change in backscatter units in non-reimbursed airports.

Table A1: Airport Utilities Costs for AIT in 2013

(in $millions, undiscounted)

Scenario	**AITs**		**Total Cost**
	Energy Consumption (kWs)	**Per Unit Cost ($ per kWh)**	
	a	b	c = a × b ÷ $1 million
with backscatter	3,067,186[223]	$0.1042	$0.32
w/o backscatter	1,969,232		$0.21
Weighted Average	**2,426,713**		**$0.25**[224]

TSA Utilities Cost

At the end of 2013, there were 445 AITs at reimbursed airports. TSA counts 19 of the 174 backscatter units came from reimbursed airports. TSA adds these AIT units to end-of-the-year in-service AITs to estimate that there were 464 AIT units (445 + 19) in reimbursed airports in early 2013. TSA uses the ratio of AITs in reimbursed airport at the beginning of 2013 to the end of 2013 (464:445) to inflate the original estimate of AIT hours in 2013 in Table 45. Table A2 calculates the streams of utilities costs for AIT in the full year in 2013 under both scenarios—with backscatter units (464 AITs) and without backscatter units (445 AIT units)—and takes the weighted average of both to calculate the airport utilities costs for 2013.

[223] 3,067,186 hours = (433 AIT units / 278 AIT units) × 1,969,232 hours.
[224] 0.25 = 0.32 × (5 months /12 months) + 0.20 × (7 months / 12 months).

Table A3: TSA Utilities Costs for AIT in 2013

(in $millions, undiscounted)

Scenario	AITs		Total Cost
	Energy Consumption (kWs)	Per Unit Cost ($ per kWh)	
	a	b	c = a × b ÷ $1 million
with backscatter	3,313,417[225]	$0.1042	$0.35
w/o backscatter	3,177,738		$0.33
Weighted Average	**3,234,271**		**$0.34**[226]

Personnel Cost

To estimate the personnel cost in 2013, TSA again calculates a weighted average costs from both scenarios. TSA bases personnel costs on the number of AIT lanes for each AIT (IO and ATR). Because backscatter only has IO technology, the number of lanes using ATR remains unchanged in both scenarios. In order to calculate the number lanes with IO technology, TSA applies the average lanes per AIT in each airport category found in Table 28 to the 94 backscatter units in Category X airports, 68 in Category I, 8 in Category II, and 4 in Category III to calculate approximately 297[227] lanes with IO technology in the first five months of 2013. Because all backscatter units are removed after May, there are zero lanes with IO technology in the last seven months of 2013. Table A4 shows the calculation of costs in both scenarios and weighted average — which is used to estimate personnel costs in Chapter 2 Table 29.

---

[225] 3,313,417 = (464 AIT units / 445 AIT units) × 3,177,738.
[226] 0.34 = 0.35 × (5 months /12 months) + 0.33 × (7 months / 12 months).
[227] 297 lanes = (94 Cat X backscatters x 1.71 lanes per AIT in Cat X) + (68 Cat I backscatters x 1.73 lanes per AIT in Cat I) + (8 Cat II backscatters x 1.75 lanes per AIT in Cat II) + (4 Cat III backscatters x 1.26 lanes per AIT in Cat III).

Table A4: Personnel Cost in 2013

(in $millions, undiscounted)

Scenario	Lanes with IO	Hours		Lanes with ATR	Hours		Total Hours	Hourly Comp	Total
	a	b = a x Avg Hrs per AIT w/IO	c = b x 1.5 TSO per lane	d	e = d x Avg Hrs per AIT w/ATR	f = e x 1 TSO per lane	g = c + f	h	i = g x h ÷ 1 million
with backscatter	297	1,379,098	2,068,646	1,238	5,741,952	5,741,952	7,810,598	$29.95[228]	$233.91
w/o backscatter	0	0	0	1,238	5,741,952	5,741,952	5,741,952	$29.95	$171.96
Weighted Avg	**124**	**574,624**	**861,936**	**1,238**	**5,741,952**	**5,741,952**	**6,603,888**	**$29.95**	**$197.77**

[228] Fully loaded wage rate for TSOs. Estimates come from the Office of Finance of Administration.

Privacy Impact Assessment
for

TSA Whole Body Imaging

January 2, 2008

Contact Point
Mike Golden
Assistant Administrator
Operational Process & Technology
Mike.Golden@dhs.gov

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

Hugo Teufel III
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.

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

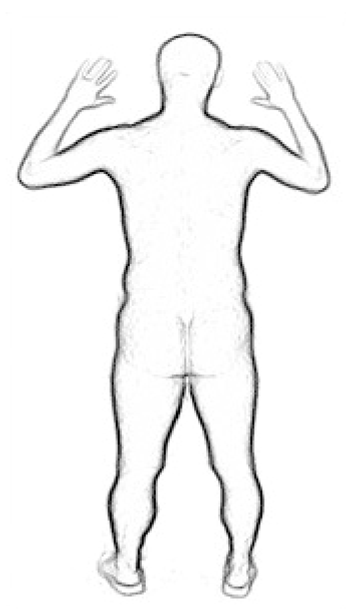
[1] "Sterile area" is defined in 49 CFR 1540.5 and generally means an area of an airport with access limited to persons who have undergone security screening by TSA.
[2] TSA additionally requested that the National Research Council study "technologies to protect the nation's air transportation system from attacks by terrorists and others of like mind." The study, *Assessment of Millitmeter-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.

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 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).
- 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).

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 a blur appears 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. If there is a red light, 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. 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.

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 select a WBI 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 brochures that explain the technology and show 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 FIPs.

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 Page

Original signed and on file with the DHS Privacy Office

Hugo Teufel III
Chief Privacy Officer
Department of Homeland Security

The TSA Blog

http://blog.tsa.gov

FRIDAY, FEBRUARY 20, 2009

Pilot Program Tests Millimeter Wave for Primary Passenger Screening

This week, TSA began testing MMW technology in the place of a metal detector at Tulsa International Airport to assess passenger throughput and acceptance.

Currently, 18 airports have millimeter wave equipment installed at checkpoints in a "secondary" screening configuration, which means that metal detectors are still the primary method of screening passengers. At these airports, randomly selected passengers and those requiring secondary screening can be screened by millimeter wave technology as a non-invasive alternative to a pat-down from an officer.

In Tulsa, instead of walking through the metal detector, passengers will go directly through the millimeter wave machine. A passenger can opt not to go through the unit, but will go through the metal detector and get a pat-down instead. Signage at the checkpoint informs travelers about the technology and lets them know that using it is voluntary. We've included one of the signs below.

So far the pilot seems to be going well, as noted in an article in USA Today. In the first three days of primary MMW at Tulsa, 3,780 passengers have been screened using the technology and only 8 people have opted for the metal detector and a pat-down.

In addition to the security benefit of whole body imaging – it can detect metallic and non-metallic threat items – the technology also reduces the need to pat-down passengers with hip replacements, prosthetics and other surgical implants. At airports without Whole Body Image machines, when passengers alarm the metal detector, the alarm must be resolved through a hand-held metal detector and a pat down. This often takes two to four minutes as opposed to about 15 seconds with millimeter wave.

For every person who is hesitant to go through the millimeter wave portal for whatever reason, there are 100 people with metallic surgical implants that are rejoicing. Here is a quote from Thomas Frank's USA Today Article:

"For passengers with metallic hips or knees, the scanners were a relief from metal detectors, which invariably sound alarms that lead to pat-downs. 'I walked through, raised my arms and was done,' said a beaming Larry Brenden, 43, of Albuquerque. 'I was like, what, no pat-down?"

And yes, whenever we talk about whole body imaging we get lots of comments and questions about privacy. We suggest checking out 60 Minutes correspondent Leslie Stahl's commentary on millimeter wave or this article by the producer of Ms. Stahl's segment. For anyone just hearing about millimeter wave and wanting to know more, please read Blogger Bob's two previous MMW posts: [link 1] [link 2]. The short version: the technology is completely safe, WBI images are never transmitted, printed or stored, the officer at the machine cannot see the image and the officer viewing the image cannot see the passenger.

ABOUT THIS BLOG

The purpose of this blog is to communicate with the public about all things TSA related. Check in regularly for "TSA Travel Tips" and our end of week "TSA Week in Review" posts on Fridays.

Google™ Custom Sear | Search

BLOG LINKS

- Comment Policy
- Contact the TSA Blog Team
- Meet Our Bloggers
- Please Post Off Topic Comments Here
- Privacy & Website Policies
- Blog Home

POPULAR POSTS FOR THE LAST 30 DAYS

Let's Talk Turkey: TSA Thanksgiving 2016 Travel Tips

Safety Razors and Disposable Razors

TSA Travel Tips Tuesday – Can You Fly Without an ID?

TSA Travel Tips Tuesday - Traveling With Alcoholic Beverages

Travel Tips Tuesday: Safely Packing Batteries for Your Trip

BLOG ARCHIVE

In the next two months, the pilot program will expand to San Francisco, Las Vegas, Miami, Albuquerque, and Salt Lake City.

If you have the chance to go through a millimeter wave machine – in primary or secondary – please share your thoughts here on the blog.

- Poster Paul

EoS Blog Team

**Update:

***Addendum:

Including the above, three signs will be on display at the security checkpoint for airports participating in the Primary MMW pilot. See the other two below. All three are currently on display at Tulsa.

Posted by Blogger Paul, EoS Blog Team at 2/20/2009 05:43:00 PM 172 comments

G+1 Recommend this on Google Links to this post

Labels: millimeter wave, Paul, Screening Technology, technology

Newer Posts Home Older Posts

Subscribe to: Posts (Atom)

▶ June (5)
▶ May (8)
▶ April (11)
▶ March (9)
▼ February (4)
▶ Feb 25 (1)
▼ Feb 20 (1)
Pilot Program Tests Millimeter Wave for Primary Pa...
▶ Feb 18 (1)
▶ Feb 09 (1)
▶ January (7)
▶ 2008 (126)

EMAIL UPDATES

To sign up for updates or to access your subscriber preferences, please enter your contact information below.

Email Address

Submit

SUBSCRIBE TO

Posts

All Comments

Powered by Blogger.

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

Transportation Security Administration

FEB 27 2009

ACTION

MEMORANDUM FOR: Janet Napolitano
Secretary

FROM: Gale D. Rossides Gale D. Rossides
Acting Administrator

SUBJECT: Whole Body Imagery Primary Deployment Evaluation

Purpose

To document in writing your decision to approve the Transportation Security Administration's (TSA) Whole Body Imager Primary Deployment Evaluation at Albuquerque International Airport (ABQ), McCarran International Airport (LAS), Miami International Airport (MIA), Salt Lake City International Airport (SLC), San Francisco International Airport (SFO), and Tulsa International Airport (TUL).

Background

Whole Body Imagery (WBI) is a general term for the technologies that scan an individual and create a computer image of the person's body. In addition to metal objects, WBI technologies are capable of detecting a variety of items, such as explosives and other non-metallic threat items that would not be detected by traditional metal-detection equipment or physical pat-down searches. A specially-trained screening officer remotely reviews the computer image for anomalies that may represent concealed weapons or explosives on the body and then communicates the result back to the checkpoint.

The purpose of the WBI Primary Deployment Evaluation is to assess the consequences of replacing the standard walk-through metal detector (WTMD) at an airport with the millimeter wave (MMW) WBI. For this operational evaluation, TSA deployed the MMW WBIs in primary configurations at Tulsa International Airport (TUL) (February 17 – March 3), Albuquerque International Airport (ABQ) (February 26 – March 12), and San Francisco International Airport (SFO) (March 2 – March 16). TSA will also deploy WBI in primary at Salt Lake City International Airport (SLC) (March 9 – March 23), McCarran International Airport (LAS) (March 16 – March 30), and Miami International Airport (MIA) (March 23 – April 6).

Deployment of the WBI in a primary screening configuration accords with TSA's broad statutory authority for ensuring the security of all modes of transportation and for development and use of new technologies in all of those environments. See 49 U.S.C. §§ 114(d), (f). Congress has also encouraged TSA to use the WBI for the purpose of ensuring aviation security. See S. Rep. No 110-396 (2008). TSA's use of the WBI at screening checkpoints additionally comports with Fourth Amendment requirements.

Discussion

In 2007, TSA began piloting WBI units at airport checkpoints as a tool for conducting additional screening; that is, as an optional method for screening selectees and other individuals requiring additional screening. Currently, a total of 40 WBI units are deployed at 19 airports.

TSA's strategy for the operational evaluation is to determine the viability of deploying MMW WBI units collocated with WTMDs at airport checkpoints as primary screening devices. The proposed operational evaluation is the first step in achieving TSA's long-term strategy of incorporating WBI technology at the screening checkpoint in a primary screening configuration. Upon completion of this evaluation, TSA will review the throughput and detection capabilities of the WBI units, the impact on airport security operations, and other factors to determine the feasibility and desirability of further deployment. TSA will provide a briefing to update you on the results of that evaluation.

TSA has been diligent to ensure privacy protections are addressed in the program. WBI privacy protections are the same for operations in both primary and secondary mode. Specifically, TSA preserves anonymity by preventing the Transportation Security Officer (TSO) viewing the image from seeing the individual undergoing screening, and by not saving the image of the passenger, and furthers choice by allowing individuals to choose a physical pat-down as an alternative to WBI. A Privacy Impact Assessment was conducted and approved by DHS Privacy.

TSA developed and is executing a robust outreach strategy for this effort. TSA's Office of Strategic Communication and Public Affairs developed a targeted media strategy that includes the posting of a blog, press release, and information on the website. TSA advanced the story to selected media outlets on Friday, February 13, 2009. TSA also notified key Congressional committees, including the House Committee on Homeland Security, and Congressional representatives of areas where the equipment is being rolled out, including Senators Coburn, Hatch, Reid, and Feinstein. Congressional notification was finalized on Monday, February 16, 2009.

Recommendation:

I recommend you sign below to acknowledge your approval of the Whole Body Imagery Primary Deployment Evaluation.

Approved: ______________________ Disapproved: ____________________

Requires More Discussion: __________ Date: _________________________

May 31, 2009

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Dear Secretary Napolitano,

We the undersigned privacy, consumer rights, and civil rights organizations are writing to you regarding the Transportation Security Administration's announced plan to deploy Whole Body Imaging as the primary means of screening airline passengers in the United States. We strongly object to this change in policy and urge you to suspend the program until the privacy and security risks are fully evaluated.

Whole Body Imaging systems, such as backscatter x-ray and millimeter wave, capture a detailed image of the subject stripped naked. In this particular application, your agency will be capturing the naked photographs of millions of American air travelers suspected of no wrongdoing.

Moreover, the privacy problems with these devices have still not been adequately resolved. Even though a "chalk line" image is displayed to an operator in a remote location and even though the TSA undertook a Privacy Impact Assessment and said that the image-recording feature would be disabled, it is obvious that the devices are designed to capture, record, and store detailed images of individuals undressed.

If the public understood this, they would be outraged -- many on religious grounds -- by the use of these devices by the US government on US citizens. "The desire to shield one's unclothed figure from view of strangers, and particularly strangers of the opposite sex, in impelled by elementary self-respect and personal dignity," said the U.S. Ninth Circuit Court of Appeals in 1958. The law of privacy, according to a federal judge in California in 1976, "encompasses the individual's regard for his own dignity; his resistance to humiliation and embarrassment; his privilege against unwanted exposure of his nude body and bodily functions." Both courts were discussing dignity in prisons, even though other rights of privacy are not accorded inmates.

Further, the TSA repeatedly stated that these systems would only be used for secondary screening of passengers and only as a voluntary alternative to a pat-down search. The fact that the TSA reversed itself on the central question of whether these systems would be voluntary makes obvious the risk that the TSA will later reverse itself on the retention of images.

More must be known about the use of these devices. The American public is directly impacted by the planned use of these systems and should be given an opportunity to express its views.

We ask that the use of "Whole Body Imaging" technology undergo a 90-day formal public rulemaking process to receive public input on the agency's use of "Whole Body Imaging" technologies.

In the interim, the agency should suspend the use of Whole Body Imaging to screen all travelers. Individuals who are asked to undergo secondary screening must be fully informed of their right to alternative secondary screening options. Not native English speaking passengers must be informed via multi-lingual oral and written formats that include an image comparable to the size of the image that will be produced by the Whole Body Image technology. Passengers should also have alternatives to the Whole Body Imaging option for secondary screening such as a pat down, or physical search of carry-on bags.

The TSA should also investigate less invasive means of screening airline passengers. The expense of the technology to taxpayers should be considered in light of other less costly means of creating a secure air travel experience.

Finally, we seek a full investigation of the medical and health implications of repeated exposure to Whole Body Imaging technology. The frequency of air travel, medical conditions such as pregnancy, and chronic health conditions, and repeated exposure of TSA and airport personnel stationed in the vicinity of the technology should be assessed. Age, gender, pre-existing medical conditions, and other factors should be evaluated and medical recommendations developed regarding the use of any Whole Body Imaging system.

Sincerely,

American Association of Small Property Owners
American Civil Liberties Union
Americans for Democratic Action
Calegislation
Center for Democracy and Technology
Center for Digital Democracy
Center for Financial Privacy and Human Rights
Constitution Project
Consumer Action
Consumer Federation of America
Consumer Travel Alliance
Consumer Watchdog
Cyber Privacy Project
Discrimination and National Security Initiative
Electronic Privacy Information Center
Fairfax County Privacy Council
Feminists for Free Expression
Gun Owners of America
Identity Project (PapersPlease.org)
Liberty Coalition
National Center for Transgender Equality
National Workrights Institute
Pain Relief Network

Patient Privacy Rights
Privacy Activism
Privacy Journal
Privacy Rights Clearinghouse
Privacy Times
The Multiracial Activist
The Rutherford Institute
Transgender Law Center
U.S. Bill of Rights Foundation
Woodhull Freedom Foundation
World Privacy Forum

Office of the Assistant Secretary

U.S. Department of Homeland Security
601 South 12th Street
Arlington, VA 22202-4220

JUN 19 2009

Transportation
Security
Administration

Ms. Lillie Coney
Electronic Privacy Information Center (EPIC)
1718 Connecticut Ave, NW
Suite 200
Washington, DC 20009

Dear Ms. Coney:

Thank you for your letter of May 31, 2009, to Secretary Janet Napolitano on behalf of 24 groups regarding privacy concerns associated with the Transportation Security Administration (TSA) Whole Body Imaging (WBI) program. I would like to take this opportunity update you on TSA's WBI program and the privacy protections that are accompanying the deployment of WBI equipment.

As you know, whole body imaging is an umbrella term used to describe a number of technologies that enable TSA to detect prohibited items that may be concealed under clothing without a physical search of a passenger. WBI is a key component of TSA efforts to address evolving security threats, including non-metallic threat items. To date, 19 airports across the nation are using WBI technology, and at six of those airports, WBI is being used in primary screening. At all locations, individuals who do not want to go through WBI screening may decline in favor of a pat-down, whether in primary or secondary screening.

TSA is committed to preserving privacy in its security programs and believes strongly that the WBI program accomplishes that through a screening protocol that ensures complete anonymity for the individual undergoing the WBI scan. This is achieved by physically separating the officer viewing the image from the person undergoing the scan. This officer sits in a windowless room that is separated from the checkpoint. The WBI scanned images cannot be stored or retained, pursuant to a factory setting that cannot be changed by the operator. Cameras and cell phones are not allowed in the viewing room under any circumstances. Further anonymity protection is achieved by a filter on the scanned image that blurs the face of the individual who was scanned. TSA has not deviated from these operational protocols, first published in the Privacy Impact Assessment for WBI in January 2008 prior to the first devices being operated in the WBI pilot. While we believe that these privacy protections are robust, we also believe that improvements in WBI technology will allow us to add even more privacy protections in the future while continuing to maintain the effectiveness of these systems to detect threat items.

From the outset of the WBI program, TSA has worked to inform the public on WBI screening and to listen to public reaction to the technology. These efforts are not static:

we continue to listen to the public, and we constantly look for ways to improve our outreach and education. TSA outreach has included briefings to the Privacy Coalition in March 2007 and again in December 2008. Indeed, it was a comment specifically from you at the March 2007 meeting that prompted signage being placed directly on the WBI devices instead of only being made available in a brochure. Recently, we improved the signage at the entrance to the passenger screening queue. In the near future, we also will be adding WBI information on the video screens at checkpoints with WBI screening. In October 2007, TSA offered demonstrations of the technology to news organizations and to privacy groups, including three groups that signed your letter (American Civil Liberties Union, EPIC, and Center for Democracy and Technology). The TSA web site has information on WBI screening at www.tsa.gov/approach/tech/body_imaging.shtm. The TSA blog, one of the most heavily trafficked blogs in the Federal government (third behind only the White House and the Congressional Budget Office blogs), has made repeated posts on the WBI program, and TSA considered views expressed in several hundred comments to the posts as well as reaction to articles in the news and travel media. TSA also considered international reaction to the deployment of WBI by other governments at foreign airports.

Finally, with respect to health concerns, the energy (both x-ray and millimeter wave) generated by the WBI devices are only a small fraction of the energy that individuals are exposed to every day. The x-ray energy is equivalent to 2 minutes of flight at altitude, or the energy that every living thing is exposed to in a single day at ground level, while the millimeter wave energy is equivalent to 1/100,000 of the energy permitted by the FCC for cell phones.

We appreciate hearing the concerns expressed in your letter and hope this information is helpful. If you need additional assistance, please contact Peter Pietra, Director, Privacy Policy & Compliance, at TSAprivacy@dhs.gov.

Sincerely yours,

Gale D. Rossides
Acting Administrator

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.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Daniel K. Akaka

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

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 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.

Post-Hearing Questions for the Record
Submitted to the Honorable Janet A. Napolitano
From Senator Tom Coburn

"Intelligence Reform: The Lessons and Implications of the Christmas Day Attack"
January 20, 2010

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

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)

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. 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.

VerDate Nov 24 2008 09:31 Oct 05, 2011 Jkt 056838 PO 00000 Frm 00281 Fmt 6601 Sfmt 6601 P:\DOCS\56838.TXT SAFFAIRS PsN: PAT

56838.088

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.

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.

EPIC v. Napolitano
AR 31 2008
TSA-100122-0022

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.

EPIC v. Napolitano
AR 081.007

April 21, 2010

Secretary Janet Napolitano
Department of Homeland Security
U.S. Department of Homeland Security
Washington, DC 20528

Chief Privacy Officer Mary Ellen Callahan
The Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

Re: Petition for Suspension of TSA Full Body Scanner Program

Dear Secretary Napolitano and Ms. Callahan,

We the undersigned privacy, consumer rights, and civil rights organizations hereby petition[1] the Department of Homeland Security ("DHS") and its component, the Transportation Security Administration ("TSA") to suspend the ongoing deployment of the TSA's Full Body Scanner ("FBS") program. The TSA program uses FBS devices (also called "whole body imaging" machines) to screen air travelers in the United States.

We strongly object to the TSA's use of full body scanners as primary, mandatory screening at security checkpoints. On May 31, 2009, twenty-four privacy and civil liberties groups[2] wrote to the DHS requesting, *inter alia*, that the DHS conduct "a 90-day formal public rulemaking process to receive public input on the agency's use of 'Whole Body Imaging' technologies."[3] The DHS failed to initiate a rulemaking. Instead, the TSA recently announced its intent to deploy approximately one thousand additional FBS devices to American airports.[4] Although the TSA failed to conduct a formal rulemaking, it is clear that the TSA has established a rule mandating the use of body scanners at airport checkpoints as primary screening. EPIC petitions the TSA to repeal that rule, and suspend the Full Body Scanner program.

The deployment of Full Body Scanners in US airports, as currently proposed, violates the U.S. Constitution, the Religious Freedom Restoration Act ("RFRA"), the Privacy Act of 1974 ("Privacy Act"), and the Administrative Procedures Act ("APA"). As described below, the FBS program effectively subjects all air travelers to unconstitutionally intrusive searches that are disproportionate and for which the TSA lacks any suspicion of wrongdoing. The FBS Program also violates the RFRA because it requires those of sincerely held religious beliefs to be subject

[1] The undersigned file this petition pursuant to 5 U.S.C. § 553(e), which requires that "[e]ach agency shall give an interested person the right to petition for the issuance, amendment, or repeal of a rule."
[2] The May 31, 2009 letter signatories include many of the undersigned groups.
[3] Letter from EPIC and thirty-three organizations to Secretary Janet Napolitano, U.S. Dep't. of Homeland Security (May 31, 2009), *available at* epic.org/privacy/airtravel/backscatter/Napolitano_ltr-wbi-6-09.pdf.
[4] U.S. Government Accountability Office, Testimony Before the House Subcommittee on Transportation Security and Infrastructure Protection, *TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Other Areas of Aviation Security Remain*, Mar. 17, 2010 at 1 *available at* http://www.gao.gov/new.items/d10484t.pdf.

to offensive intrusions by government officials. The program violates the Privacy Act because the system gathers personally identifiable information—a detailed and unique image of the human body easily associated with a particular airline ticket—yet the TSA failed to publish a System of Records Notice. The TSA Chief Privacy Office violated its statutory obligations to ensure that new technologies "sustain and do not erode" the privacy of Americans when it effectively approved the program.

Further, substantial questions have been raised about the effectiveness of the devices, including whether they could detect powdered explosives—the very type of weapon used in the December 25, 2009 attempted airliner bombing. The full body scanning program is enormously expensive, costing taxpayers at least $2.4 billion dollars. There are less intrusive and less costly techniques available to address the risk of concealed explosives on aircrafts. For example, last week, U.S. Senators asked the DHS to evaluate alternative technologies that could "address many of the privacy concerns raised by the scanners DHS is currently testing."[5]

I. The Agency is Undertaking an Aggressive Plan to Deploy Full Body Scanners in US Airports without regard to Effectiveness, Traveler Complaints, Privacy Risks, or Religious Objections

A) The Plan to Deploy Approximately One Thousand Full Body Scanners to American Airports

The TSA operates Full Body Scanners at airports throughout the United States.[6] The TSA uses two types of FBS devices: backscatter x-ray and millimeter wave.[7] Both types of FBS devices can capture, store, and transfer[8] detailed, three-dimensional images of individuals' naked bodies.[9] Experts have described full body scans as "digital strip searches."[10] The images captured by FBS devices can uniquely identify individual air travelers. The TSA uses FBS devices to search air travelers as they pass through the TSA's airport security checkpoints.[11]

FBS devices are currently deployed at: Albuquerque International Sunport Airport, Boston Logan International Airport, Chicago O'Hare International Airport, Cincinnati/Northern Kentucky International Airport, Hartsfield-Jackson Atlanta International Airport, Baltimore/Washington International Thurgood Marshall Airport, Denver International Airport,

---

[5] Letter from Sen. Susan Collins, Sen. Saxby Chambliss, and Sen. Jon Kyl to Secretary Janet Napolitano, U.S. Dep't. of Homeland Security (Apr. 12, 2010) *available at* http://hsgac.senate.gov/public/index.cfm?FuseAction=Press.MinorityNews&ContentRecord_id=f8689ee7-5056-8059-767f-091debe8eae4.

[6] TSA, *TSA: Imaging Technology*, http://www.tsa.gov/approach/tech/imaging_technology.shtm (last visited Apr. 15, 2010).

[7] *Id.*

[8] TSA Office of Security Technology System Planning and Evaluation, *Procurement Specification for Whole Body Imager Devices for Checkpoint Operations*, Sept. 23, 2008 ("TSA Procurement Specifications Document") at 5, *available at* http://epic.org/open_gov/foia/TSA_Procurement_Specs.pdf (stating "When in Test Mode, the WBI: shall allow exporting of image data in real time; … shall provide a secure means for high-speed transfer of image data; [and] shall allow exporting of image data (raw and reconstructed)").

[9] *E.g.* Wikipedia, Backscatter X-ray, http://en.wikipedia.org/wiki/Backscatter_X-ray; L3, L3 Composite, http://www.sds.l-3com.com/products/i/L-3%20composite%20300dpi.jpg.

[10] Privacy Coalition, *Stop Digital Strip Searches*, http://www.stopdigitalstripsearches.org/.

[11] *Supra* note 5.

Dallas/Fort Worth International Airport, Detroit Metro Airport, Indianapolis International Airport, Jacksonville International Airport, Kansas City 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, and Tulsa International Airport.[12]

In March 2010, the TSA began deploying additional FBS devices in American airports.[13] In March 2010, the TSA announced its decision to further deploy approximately one thousand additional FBS devices to American airports.[14] As a matter of pattern, practice and policy, the TSA requires air travelers to submit to FBS searches once they have entered the security zone in airports equipped with FBS devices.[15] As a matter of pattern, practice and policy, the TSA employs FBS searches as a primary search of air travelers in airports equipped with FBS devices.[16] As a matter of pattern, practice and policy, the TSA does not offer air travelers a meaningful alternative to FBS searches in airports equipped with FBS devices.[17] As a matter of pattern, practice and policy, the TSA does not offer air travelers with religious objections to Full Body Scanning a meaningful alternative to FBS searches in airports equipped with FBS devices.[18]

B) The TSA's Full Body Scanner Program Collects and Retains Detailed Personal Information About Air Travelers

The TSA requires air travelers to disclose their full name, birth date, and gender when purchasing a ticket.[19] The TSA obtains additional information about air travelers from airlines, government agencies, and other third parties. The TSA collects and stores this information, linking it to air travelers' itineraries. The TSA requires air travelers to submit to searches of their

[12] *Supra* note 5.
[13] U.S. Government Accountability Office, Testimony Before the House Subcommittee on Transportation Security and Infrastructure Protection, *TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Other Areas of Aviation Security Remain*, Mar. 17, 2010 at 1 *available at* http://www.gao.gov/new.items/d10484t.pdf.
[14] *Id*.
[15] Air Traveler Complaints to the TSA at 45, http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf (air traveler stated that "when he requested an alternative screening, the TSA screeners interrogated and laughed at him."); at 53 (air traveler "was told to go in this machine and … was not told that this machine would do a full body scan. I did not know what I went thru[*sic*] until today, when I read the article on line.").
[16] *Id*. at 67 ("I am outraged and angry that what was supposed to be a 'pilot' for the millimeter scan machines has now become MANDATORY at SFO. I have transited through the International A terminal boarding area several times over the past few months and TSA has shut down all lanes other than the scanner.") (emphasis in original).
[17] *Id*. at 62, ("I was picked to go through the new body scanner machine … When I looked around, I noticed that there were only women who were 'told' to go through this machine, there were no men. I would have refused, but didn't realize that I could until I read up on the scanner."); at 65 ("I was asked/forced into this [body scanner] at BWi airport on 6/30/09"); at 69 ("the TSA guard sent my wife and I through the new X-Ray machine … A guard did not give us a choice."); at 69 ("I am 70 years old. [At BWI, I] went through the metal detector … with apparently no problems, I proceeded to collect my belongings … but was stopped [for a body scan]. I was never told why I had to do this, had no idea what was being done."); at 72 ("[I] decided to opt out [of a FBS scan]. My family and I were then subjected to a punitive pat-down search (they went over me three times) that would have been considered sexual assault in any other context.").
[18] *Id*. at 92 (describing mandatory body scan and subsequent patdown of devout Muslim air traveler).
[19] TSA, *Secure Flight Update*, Jul. 15, 2009, http://www.tsa.gov/blog/2009/07/secure-flight-update.html

bodies and carry-on luggage at TSA airport security checkpoints.[20] The TSA requires that air travelers present a boarding pass and government-issued photo identification card at airport security checkpoints.[21] The boarding pass displays air travelers' full names, travel itineraries, and bar codes containing machine-readable versions of travelers' personal information.[22] As a matter of pattern, practice and policy, the TSA visually matches air travelers' photo ID cards with their boarding passes when travelers pass through airport security checkpoints.[23] As a matter of pattern, practice and policy, the TSA scans air traveler's boarding passes, collecting air travelers' personal information, when travelers pass through airport security checkpoints that are equipped with paperless boarding pass scanners.[24]

As described above, the TSA employs full body scanners to search air travelers at airport security checkpoints.[25] As described above, FBS devices can capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies.[26] As a matter of pattern, practice, and policy, the TSA requires air travelers to possess and often display boarding passes contemporaneous with FBS searches. The TSA is therefore able to associate a specific FBS image with the full name, birth date, gender, and travel itinerary of the scanned traveler. The TSA failed to publish a "system of records notice" concerning the FBS Program in the Federal Register.

C) The TSA Misrepresents the Full Body Scan Program

The TSA claims that FBS devices cannot capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies.[27] In fact, the FBS devices employed by the TSA can capture, store, and transfer detailed, three-dimensional images of individuals' naked bodies, as per the TSA's own requirements.[28] The TSA claims that FBS searches are "optional."[29] In fact, as a matter of pattern, practice and policy, the TSA does not offer air travelers a meaningful alternative to FBS searches in airports equipped with FBS devices.[30]

---

[20] TSA, *TSA Travel Assistant*, http://www.tsa.gov/travelers/airtravel/screening/index.shtm; TSA, *3-1-1 on Air Travel*, http://www.tsa.gov/311/index.shtm.
[21] TSA, *The Screening Experience*, http://www.tsa.gov/travelers/airtravel/assistant/editorial_1044.shtm.
[22] Wikipedia, *Boarding Pass*, http://en.wikipedia.org/wiki/Boarding_pass; *see also* Wikipedia, *Bar Coded Boarding Pass*, http://en.wikipedia.org/wiki/Bar_Coded_Boarding_Pass
[23] TSA, *TSA Announces Enhancements to Airport ID Requirements to Increase Safety*, Jun. 23, 2008, http://www.tsa.gov/press/happenings/enhance_id_requirements.shtm.
[24] TSA, *Paperless Boarding Pass Pilot*, http://www.tsa.gov/approach/tech/paperless_boarding_pass_expansion.shtm.
[25] *Supra* note 5.
[26] *Supra* notes 7-8.
[27] *Supra* note 5 (claiming "The image cannot be stored, transmitted or printed, and is deleted immediately once viewed.").
[28] *Supra* notes 7-8.
[29] *Supra* note 5 (claiming "Advanced imaging technology screening is **optional for all passengers**."[emphasis in original]).
[30] *Supra* note 16; *see also supra* note 5 (stating "passengers who do not wish to utilize this screening will receive an equal level of screening, including a physical pat-down.").

In 2007, the TSA stated that FBS searches would not be mandatory for passengers, but rather "a voluntary alternative to a pat-down during secondary screening."[31] In fact, as a matter of pattern, practice and policy, the TSA employs FBS searches as a primary search of air travelers in airports equipped with FBS devices.[32] The TSA has claimed that "a security algorithm will be applied to the image to mask the face of each passenger."[33] In fact, the FBS devices employed by the TSA can capture images without any security algorithm and without masking the face of each passenger.[34]

The TSA claims that air travelers prefer FBS searches.[35] In fact, hundreds of air travelers have lodged objections with the TSA, alleging a host of law and policy violations arising from the TSA's FBS searches.[36] Air travelers object to the invasiveness of the FBS searches.[37] Air travelers state that they are not informed when they undergo a FBS search, or of a pat-down alternative.[38] Air travelers object to the use of FBS devices to search vulnerable individuals, including children and pregnant women.[39] Pregnant air travelers objected to the TSA's FBS search after the TSA scanned them without identifying the machine or informing them of how it operates.[40]

D) Full Body Scanner Technology is Flawed

The FBS devices employed by the TSA are not designed to detect powdered explosives.[41] The FBS devices employed by the TSA are not designed to detect powdered pentaerythritol

[31] *TSA Tests Second Passenger Imaging Technology at Phoenix Sky Harbor Airport*, Transportation Security Administration, October 11, 2007 *available at* http://www.tsa.gov/press/releases/2007/press_release_10112007.shtm; *see also X-Ray Backscatter Technology and Your Personal Privacy*, http://web.archive.org/web/20080112014635/http://www.tsa.gov/research/privacy/backscatter.shtm (archived January 12, 2008) (stating "Backscatter is a voluntary option for passengers undergoing secondary screening as an alternative to the physical pat down procedures").
[32] *Supra* note 15.
[33] TSA, *TSA Tests Second Passenger Imaging Technology at Phoenix Sky Harbor Airport*, Oct. 11, 2007, http://www.tsa.gov/press/releases/2007/press_release_10112007.shtm.
[34] TSA Systems Engineering Branch, *Operational Requirements Document, Whole Body Imager Aviation Applications*, July 2006, ("TSA Operational Requirements Document") at 8 *available at* http://epic.org/open_gov/foia/TSA_Ops_Requirements.pdf (stating "the WBI shall provide ten selectable levels of privacy."); TSA Procurement Specifications Document at 5 (Enabling and disabling of image filtering shall be modifiable by users as defined in the User Access Levels and Capabilities appendix).
[35] *Supra* note 5 (claiming "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.").
[36] Air Traveler Complaints to the TSA *available at* http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf, http://epic.org/privacy/airtravel/backscatter/EPIC2.pdf, http://epic.org/privacy/airtravel/backscatter/EPIC3.pdf, http://epic.org/privacy/airtravel/backscatter/EPIC4.pdf, http://epic.org/privacy/airtravel/backscatter/EPIC5.pdf.
[37] Air Traveler Complaints to the TSA at 19, 24, 27, 28, 37 *available at* http://epic.org/privacy/airtravel/backscatter/EPIC1.pdf (complaints stating that body scanners are "a disgusting violation of civil liberties and privacy," "for a bunch of peeping toms," "unconstitutional," "intrusive and ridiculous" and "a joke.").
[38] *Supra* note 16.
[39] *E.g.* TSA Traveler Complaints at 14, 21, 25, 85.
[40] TSA Traveler Complaints at 159; TSA Traveler Complaints at 11-12, *available at* http://epic.org/privacy/airtravel/backscatter/EPIC2.pdf.
[41] TSA Procurement Specifications Document at 4 (requiring body scanners to detect liquid, but not powdered, material.); *see also* Jane Merrick, *Are Planned Airport Scanners Just a Scam?*, The Independent (UK), Jan. 3 2010

tetranitrate ("PETN")—the explosive used in the attempted December 25, 2009 bombing of Northwest Airlines flight 253.[42] The FBS devices employed by the TSA have profound technical flaws that allow the machines to be breached and create the risk that sensitive traveler images could be leaked.

The FBS devices employed by the TSA run Windows XPe, which contains security vulnerabilities.[43] The FBS devices employed by the TSA are designed to transfer information via highly transportable and easily concealable USB devices.[44] The FBS devices employed by the TSA are equipped with Ethernet network interfacing capabilities that are vulnerable to security threats.[45] The FBS devices employed by the TSA permit TSA employees to disable built-in "privacy safeguards."[46]

II. The Plan to Deploy Full Body Scanners is Widely Opposed, Violates the Fourth Amendment, and Several Federal Acts, including the Religious Freedom and Restoration Act, The Administrative Procedures Act, and the Privacy Act

A) Religious Leaders Object to Full Body Scanners

On February 20, 2010, Pope Benedict XVI objected to FBS searches because they fail to preserve the integrity of individuals.[47] Agudath Israel, an Orthodox Jewish umbrella group, objects to FBS searches, calling the devices "offensive, demeaning, and far short of acceptable norms of modesty" within Judaism and other faiths.[48] On February 9, 2010, The Fiqh Council of North America objected to body scanners, announcing that "general and public use of such

---

available at http://www.independent.co.uk/news/uk/home-news/are-planned-airport-scanners-just-a-scam-1856175.html (noting that body-scanners "have been touted as a solution to the problem of detecting … liquids, chemicals or plastic explosive. But Ben Wallace, the Conservative MP, who was formerly involved in a project by a leading British defence research firm to develop the scanners for airport use, said trials had shown that such low-density materials went undetected.").

[42] *Id*; *see also* Kenneth Chang, *Explosive on Flight 253 Is Among Most Powerful*, N.Y. Times, Dec. 27, 2009 *available at* http://www.nytimes.com/2009/12/28/us/28explosives.html?_r=1.

[43] TSA Contract HSTS04-06-R-CTO046 with L3 ("TSA Contract with L3") at 27 *available at* http://epic.org/open_gov/foia/TSA_Millwave_Contract.pdf; *See* Konstantin Morozov, White Paper, *Best Practices for Protecting Windows XP Embedded Devices* at 4, *available at* http://www.dsta.com.au/DSTeupload/protectingxpedevices.pdf ("In general, malware does not affect Windows Mobile devices, such as Smartphone and Pocket PCs, and other devices based on Windows CE, as much as it impacts devices running Windows XP Embedded. This is because Windows XP Embedded is based on the same feature binaries as Windows XP Professional and thus has similar vulnerabilities that can be exploited."); Brian Krebs, *Windows Security Flaw is 'Severe*,' Washington Post, Dec. 29, 2005, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2005/12/29/AR2005122901456.html.

[44] TSA Procurement Specifications Document at 10 ("the WBI shall provide capabilities for data transfers via USB devices.").

[45] TSA Procurement Specifications Document at 7; TSA Operational Requirements Document at 10-11.

[46] TSA Procurement Specifications Document at 5 (Enabling and disabling of image filtering shall be modifiable by users as defined in the User Access Levels and Capabilities appendix).

[47] Catholic News Agency, *Benedict XVI Urges Airports to Protect Integrity of Travelers*, Feb. 20, 2010, http://www.catholicnewsagency.com/news/benedict_xvi_calls_for_airports_to_protect_integrity_of_travelers/.

[48] Omar Sacirbey, *Jews, Muslims Worry Body Scanners Violate Religious Laws*, Mar. 3, 2010, http://www.religionnews.com/index.php?/rnstext/jews_muslims_say_body_scanners_violate_religious_laws/.

scanners is against the teachings of Islam, natural law and all religions and cultures that stand for decency and modesty."[49]

American air travelers have filed objections with the TSA on religious grounds.[50] On February 19, 2010, two Muslim women refused to submit to a body scan at the Manchester Airport, forfeiting their tickets to Pakistan rather than undergo the scan.[51] In March 2010, a six-member Pakistani parliamentary delegation from the Federally Administered Tribal Areas refused to submit to full body scanning at the Washington Dulles International Airport, stating it was an insult to parliamentarians of a sovereign country.[52] Instead, they ended their visit to the US and returned to Pakistan.[53]

B) The TSA's Full Body Scanner Program Violates the Fourth Amendment and the RFRA

The TSA's FBS program subjects air travelers to unreasonable searches. The program requires air travelers to submit to a uniquely invasive search without any suspicion that particular individuals have engaged in wrongdoing. Courts have upheld some invasive airport checkpoint searches, but typically on the basis that the searches are part of a progressively escalating series of screenings.[54] Full Body Scanners are part of no such program. Instead, they employ the intrusive, degrading digital strip search as mandatory, primary screening.

The TSA program particularly burdens devout air travelers. As noted above, many religious leaders condemn digital strip searches as incompatible with religious tenets. Yet the TSA's practice of requiring Full Body Scans as mandatory, primary screening leaves religious travelers without a meaningful alternative. The program violates RFRA because the TSA's interest in conducting a Full Body Scan is limited, particularly given that the scanners' are not designed to detect powdered explosives. Further, Full Body Scanners are not the least restrictive means of furthering the TSA's interest in safeguarding air travel.[55]

---

[49] Fiqh Council of North America, *Home*, http://www.fiqhcouncil.org/ (last visited April 15, 2010) (stating "a general and public use of such scanners is against the teachings of Islam, natural law and all religions and cultures that stand for decency and modesty.").
[50] *E.g.* Air Traveler Complaints to the TSA *available at* http://epic.org/privacy/airtravel/backscatter/3-2_Interim_Response.pdf.
[51] Will Pavia, *Muslim Woman Refuses Body Scan at Airport*, Mar. 3, 2010, The Times (UK) *available at* http://www.timesonline.co.uk/tol/travel/news/article7048576.ece.
[52] Press TV, *Pakistan MPs End US Visit to Protest Body Scanners*, Mar. 7, 2010 http://www.presstv.ir/detail.aspx?id=120286&sectionid=351020401.
[53] *Id*.
[54] *E.g. United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2006) (finding airport searches reasonable because they "were well-tailored to protect personal privacy, escalating in invasiveness only after a lower level of screening disclosed a reason to conduct a more probing search. The search began when Hartwell simply passed through a magnetometer. … Only after Hartwell set off the metal detector was he screened with a wand. … And only after the wand detected something solid on his person, and after repeated requests that he produce the item, did the TSA agents … reach into his pocket.").
[55] *Supra* note 5 (observing that passive scanners "incorporate auto-detection technology that addresses many of the privacy concerns raised by the scanners DHS is currently testing, while also appearing to provide a highly effective scan.")

C) The TSA's Full Body Scanner Program Violates the Privacy Act

As described above, the TSA's Full Body Scanner Program creates a group of records containing air travelers' personally-identifiable information. The group of records is under the control of the TSA, and the TSA can retrieve information about air travelers by name or by some identifying number, symbol, or other identifying particular assigned to the individual. The TSA's FBS program has created and/or revised a "system of records" under the Privacy Act. The TSA unlawfully failed to publish a "system of records notice" in the Federal Register, and otherwise failed to comply with its Privacy Act obligations concerning the FBS Program.

D) The TSA's Full Body Scanner Program Violates the Administrative Procedures Act

The DHS Chief Privacy Officer has a statutory obligation to "assur[e] that the use of technologies sustain, and do not erode, privacy protections relating to the use, collection, and disclosure of personal information."[56] The DHS Chief Privacy Officer has a statutory obligation to "assur[e] that personal information contained in Privacy Act systems of records is handled in full compliance with fair information practices as set out in the Privacy Act of 1974."[57] The DHS Chief Privacy Officer has a statutory obligation to "conduct[] a privacy impact assessment of proposed rules of the Department or that of the Department on the privacy of personal information, including the type of personal information collected and the number of people affected."[58]

The DHS Chief Privacy Office prepared an inadequate Privacy Impact Assessment of the TSA's FBS test program.[59] The inadequate assessment, which was subsequently revealed through Freedom of Information Act litigation, failed to identify numerous privacy risks to air travelers. The DHS Chief Privacy Office failed to prepare any Privacy Impact Assessment concerning the TSA's current FBS program. The TSA's current FBS program is materially different from the TSA's FBS test program. The TSA's use of full body scanners fails to comply with the Privacy Act. The program erodes, and does not sustain, privacy protections relating to the use, collection, and disclosure of air traveler's personal information.

III. Petition for Relief: Suspend Purchase, Deployment, and Operation of Full Body Scanners

The undersigned hereby request and petition the DHS and TSA for relief. As set forth above, the TSA's Full Body Scanner program violates the Fourth Amendment, the RFRA, the Privacy Act, and the APA. We request that the DHS and TSA immediately suspend purchase and deployment of Full Body Scanners to American airports. In addition, we request that the DHS and TSA cease operation of already-deployed Full Body Scanners as primary screening.

---

[56] 6 U.S.C. § 142(1) (2009).
[57] 6 U.S.C. § 142(2) (2009).
[58] 6 U.S.C. § 142(4) (2009).
[59] DHS, *Privacy Impact Assessment for TSA Whole Body Imaging* (Oct. 17, 2008) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbi.pdf; *see also* DHS, *Privacy Impact Assessment Update for TSA Whole Body Imaging* (Jul. 23, 2009) *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf.

Sincerely,

Electronic Privacy Information Center
American Civil Liberties Union
American Policy Center
Asian American Legal Education and Defense Fund
Bill of Rights Defense Committee
Calegislation
Campaign for Liberty
Center for Financial Privacy and Human Rights
Center for the Study of Responsive Law
Citizen Outreach
Consumer Federation of America
Consumer Travel Alliance
Consumer Watchdog
Council on American Islamic Relations
Cyber Privacy Project
Essential Information
Government Accountability Project
The Identity Project
Liberty Coalition
Muslim Legal Fund of America
National Center for Transgender Equality
National Workrights Institute
Patient Privacy Rights
Privacy Activism
Privacy Rights Clearinghouse
Public Citizen Litigation Group
Republican Liberty Caucus
Rutherford Institute
U.S. Bill of Rights Foundation
World Privacy Forum

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

Homeland Security

April 27, 2010

The Honorable Susan Collins
United States Senate
Washington, DC 20510

Dear Senator Collins:

Thank you for your April 12, 2010 letter regarding the imaging technology demonstrated at Amsterdam's Schiphol International Airport.

Transportation Security Administration (TSA) officials have had extensive discussions with their Dutch counterparts related to the current and future state of Advanced Imaging Technology (AIT) systems and the available automated target recognition (ATR) functionality. TSA representatives have made several visits to Schiphol to discuss the capabilities, operational effectiveness, and suitability of AIT systems—both with and without currently available ATR functionality. The Dutch have also shared testing results with us, including detection and false alarm rates for the currently deployed ATR-enabled AIT systems, and TSA has used the lessons learned from Schiphol to evaluate the use of the AIT in primary screening and determine ATR requirements for U.S. nationwide deployment. Our discussion and technical evaluation sessions with the Dutch about the current and future possibilities for ATR are ongoing,

To give you further insight, the AIT system *without* ATR functionality that is in use at Schiphol is listed on TSA's AIT Qualified Products List, and the AIT system *with* ATR functionality that is in use at Schiphol will be evaluated in a pilot. TSA has provided ATR requirements to manufacturers; once their systems are fully tested and proven to meet these requirements, TSA plans to upgrade all currently deployed systems with this new functionality.

Thank you again for your letter. I value your views on these emerging technologies, and I look forward to working with you on this and other homeland security issues. Senators Kyl and Chambliss, who co-signed your letter, will receive separate, identical responses. Should you need additional assistance, please do not hesitate to contact me at (202) 282-8203.

Yours very truly,

Janet Napolitano

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

Transportation
Security
Administration

MAY 28 2010

Electronic Privacy Information Center, *et al.*
c/o Mr. Mark Rotenberg
1718 Connecticut Avenue, N.W., Suite 200
Washington, D.C. 20009

Dear Mr. Rotenberg:

Thank you for the letter of April 21, 2010, to Department of Homeland Security (DHS) Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan from 30 organizations regarding the Transportation Security Administration's (TSA's) use of advanced imaging technology (AIT) to screen passengers for security purposes at our Nation's airports.[1] I am responding on behalf of Secretary Napolitano and Chief Privacy Officer Callahan, and request that you forward this letter to the other organizations who signed the April 21 letter. We appreciate the opportunity to address the important issues the 30 organizations have raised regarding AIT.

Statutory Mandate. In your letter, you question TSA's authority to install and operate AIT machines for passenger screening at airports absent the initiation of a formal public rulemaking process under the Administrative Procedure Act (APA). However, 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.[2]

Moreover, since 9/11, Congress has mandated that TSA invest in technologies to strengthen the efficiency and security of aviation. The emphasis on developing new technologies to address transportation security is codified at 49 U.S.C. § 44925(a):

> The Secretary of Homeland Security shall 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. The Secretary shall ensure that the equipment alone, or as part of an integrated system, can detect under realistic operating

[1] While you footnote that your letter is a Petition for Rulemaking under 5 U.S.C. §553, the relief actually sought is specified instead to be the immediate suspension of the AIT program. Accordingly, TSA does not interpret your letter to seek a rulemaking or to constitute a petition under 5 U.S.C. §553.

[2] *See* 49 CFR 1540.105(a)(2) and 1540.107.

conditions the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.

The Secretary also is required under 49 U.S.C. § 44925(b) to develop a strategic plan for deploying explosive detection equipment, such as AIT machines, at airport screening checkpoints.

AIT equipment addresses this Congressional and national security mandate by safely screening airline passengers for both metallic and nonmetallic threats, including weapons, explosives and other objects concealed under layers of clothing. TSA, DHS, the White House, and the Congress are pursuing AIT for airport checkpoint security because it is a key component of TSA's layered approach to security that addresses the evolving threats faced by airline travelers. As Secretary Napolitano stated in January 2010:

> 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. . . . [AIT is] 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. . . . [A]ll of these things have a role to play.[3]

Beyond the general mandate from Congress to deploy technology capable of screening airline passengers for nonmetallic and other evolving threats, DHS has communicated to and discussed with the Congress TSA's specific AIT deployment plans. For example, Secretary Napolitano recently announced deployments of AIT units purchased with American Recovery and Reinvestment Act (ARRA) funds to 28 additional airports, which will increase to 44 the number of airports with AIT equipment.[4] In addition, over the past several months, Secretary Napolitano and TSA Acting Administrator Gale Rossides have testified at Congressional hearings about AIT deployment plans and requests for funding for additional AIT deployment.

- "The . . . Recovery Act funds provided to TSA for checkpoint . . . screening technology have enabled TSA to greatly . . . 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

[3] Hearing on "The State of Aviation Security - Is Our Current System Capable of Meeting the Threat?," before the Senate Committee on Commerce, Science, and Transportation, January 20, 2010.

[4] *See* "Secretary Napolitano Announces Additional Deployments of Recovery Act-Funded Advanced Imaging Technology," May 14, 2010, at www.dhs.gov/ynews/releases/pr_1273850925050.shtm. *See also* Secretary Napolitano's March 5, 2010 announcement of 11 airports that will receive AIT units using ARRA funds at www.dhs.gov/ynews/releases/pr_1267803703134.shtm.

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."[5]

- The President's FY 2011 funding request will result in "total AIT coverage at 75 percent of Category X airports and 60 percent of the total lanes at Category X through II airports."[6]
- "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. . . . The President's FY 2011 budget requests . . . an additional 500 AIT units at checkpoints, . . . [and a]n additional . . . 5,355 TSO positions to operate these AIT machines at their accelerated deployment pace."[7]

As this discussion illustrates, TSA not only has ample, clear authority to install and operate AIT machines for passenger screening at airports, but has been directed by the Congress to pursue screening technology solutions that are capable of detecting nonmetallic and other dangerous devices under realistic operating conditions. DHS and TSA have communicated regularly with the Congress on TSA's AIT deployment efforts and recommendations. AIT machines offer the best current option for meeting these statutory directives and security imperatives.

AIT Screening is Optional. Your letter also states that AIT screening subjects all air travelers to intrusive searches that are disproportionate and for which TSA lacks any suspicion of wrongdoing. Your letter, however, misstates the facts.

TSA has made clear from its earliest AIT deployment that **use of AIT screening is optional for all passengers**,[8] and TSA makes every effort to address any AIT complaints or concerns.

---

[5] Written statement of Secretary Janet Napolitano for a hearing entitled "The State of Aviation Security - Is Our Current System Capable of Meeting the Threat?," before the Senate Committee on Commerce, Science, and Transportation, January 20, 2010.

[6] Written statement of Secretary Napolitano for a hearing on the DHS Budget Submission for FY 2011, before the Senate Committee on Homeland Security and Governmental Affairs, February 24, 2010, and before the House Homeland Security Committee, February 25, 2010.

[7] Written statement of TSA Acting Administrator Gale Rossides for a hearing on the TSA FY 2011 Budget before the House Appropriations Subcommittee on Homeland Security, March 4, 2010. *See also* Department of Homeland Security, Transportation Security Administration, Fiscal Year 2011 Congressional Justification for Aviation Security, pages AS-4, AS-13, and AS-22, and the written statement of Acting Administrator Rossides for a hearing entitled "The Lessons and Implications of the Christmas Day Attack: Watchlisting and Pre-Screening," before the Senate Committee on Homeland Security and Governmental Affairs, Wednesday, March 10, 2010.

[8] *See* www.tsa.gov/approach/tech/imaging_technology.shtm.

For those passengers who express concerns or decline AIT screening, TSA employs alternative screening techniques, such as use of a hand-held metal detector coupled with a pat down. The notion of alternative screening methods is consistent with TSA's screening practices over the years and is not a new feature that was introduced with the implementation of AIT. For example, TSA offers the pat down option to passengers who elect not to undergo screening by a walk-through metal detector (WTMD), and offers screening guidance for airline passengers with certain medical devices who may not wish to be screened by WTMD.[9] Not surprisingly, passengers with implanted knee and hip joints have welcomed AIT screening; these passengers alarm a WTMD and require a pat-down to resolve the alarm, but are able to use the AIT without alarming it.[10]

Similarly, options for alternative screening also are offered to those passengers for whom there are religious or cultural considerations. These passengers also may request an alternative personal search (pat-down inspection) performed by an officer of the same gender, and in private.[11]

In addition to being optional, AIT screening is widely accepted by the traveling public. For example, a *USA Today*/Gallup poll found that 78 percent of U.S. air travelers approve of the use of AIT screening in U.S. airports as a measure to prevent terrorists from smuggling explosives or other dangerous objects onto airplanes.[12] This result is consistent with TSA's experience with passenger acceptance rates for AIT machines at airport checkpoints. Only a small fraction of the millions of passengers screened using AIT, approximately 600 individuals, have expressed complaints or concerns about AIT since the inception of the program. This small number equates to less than .015 percent of the millions of airline passengers screened with AIT.

Effectiveness of AIT Screening. In your letter, you also express concern about the effectiveness of AIT devices, including whether they are capable of exposing the emerging threats to aviation such as powdered explosives, and state that there are less intrusive and costly techniques to address the risk of concealed explosives on aircraft. TSA continually searches for effective technologies and methods to detect explosives to meet the constantly evolving threats to transportation security. Clearly, walk-through metal detectors are not effective in detecting the kind of powdered explosive that you identified, and TSA's experience is that AIT provides the best, current tool for detecting this and other non-metallic threats. TSA's web site includes

---

[9] *See* www.tsa.gov/travelers/airtravel/specialneeds/editorial_1374.shtm#1. For example, for passengers with pacemakers, TSA recommends that individuals ask the TSO to conduct a pat-down inspection rather than using the walk-through the metal detector. TSA also recommends that passengers advise the Transportation Security Officer (TSO) if they have implanted pacemakers or other medical devices and where that implant is located so that a private screening can be offered. *Id.*

[10] *See* www.tsa.gov/approach/tech/imaging_technology.shtm.

[11] See www.tsa.gov/travelers/airtravel/assistant/editorial_1037.shtm.

[12] *See* "In U.S., Air Travelers Take Body Scans in Stride," Jan. 11, 2010, found at www.gallup.com/poll/125018/Air-Travelers-Body-Scans-Stride.aspx.

examples of the kind of materials that have been uncovered using AIT machines at U.S. airports, including bags of powder.[13]

Your letter also references a letter from Senator Collins and others to Secretary Napolitano about the use of AIT with automated target recognition (ATR) capabilities. Some machines with this feature currently are in use at Schiphol International Airport in Amsterdam. As the Secretary's response states,[14] TSA has worked closely with Dutch authorities and AIT manufacturers to evaluate ATR capabilities, and has established ATR requirements and provided them to AIT manufacturers. TSA is evaluating the effectiveness of ATR with respect to improved threat detection capabilities; should our evaluation show that ATR is effective in high-volume U.S. airport environments, TSA will seek to deploy this technology on AIT machines at U.S. airports.

TSA's experience, and that of other governments, clearly supports the effectiveness of AIT machines in exposing emerging threats to aviation, and this capability may be enhanced in the future by ATR, which TSA has been evaluating for some time. Your letter offers no other suggestions for alternative devices or practices that are less intrusive and less costly, yet equally effective, in addressing the risks to aviation security.

AIT Screening and Health Concerns. Your letter cited concerns about health issues related to AIT use involving children and pregnant women. TSA has relied on independent studies to address health concerns related to this technology to ensure the technology conforms to national consensus standards. Current AIT machines deployed by TSA use two different technologies: backscatter x-ray machines use ionizing radiation, and millimeter-wave machines use radio frequency energy.

AIT backscatter scanners use a narrow, low-level x-ray beam that scans the surface of the body at a high speed. The machines then generate an image resembling a chalk etching with a privacy filter applied to the entire body. Unlike a traditional x-ray machine that relies on the transmission of x-ray through the object material, backscatter x-ray detects the radiation that reflects back from the object to form an image

Over the past several years, various backscatter scanners have been independently evaluated by the Food and Drug Administration (FDA) Center for Devices and Radiological Health (CDRH), and by the National Institute for Standards and Technology (NIST) on behalf of TSA. The backscatter scanner deployed by TSA, the Rapiscan Secure 1000 Single Pose, was independently evaluated by the Johns Hopkins University Applied Physics Laboratory (APL). The APL results confirm that radiation doses to the general public are well below those limits specified by standards established by the American National Standards Institute and through the Health

[13] See http://blog.tsa.gov/2009/07/blog-post-archives.html It is unclear how you conclude that AIT cannot detect explosives in powder form The TSA acquisition documents you cite to specify that AIT detects explosives, including liquids, solids, and powders

[14] *See* Secretary Napolitano's April 27, 2010 letter to Senator Collins, attached to this letter (identical letters were sent to Senators Kyl and Chambliss).

Physics Society (ANSI/HPS) and published in ANSI/HPS N43.17-2009, entitled "Radiation Safety for Personnel Security Screening Systems Using X-ray or Gamma Radiation." The dose limits were set with the understanding that the general public includes individuals who may be more susceptible to radiation-induced health effects, such as pregnant and potentially pregnant women, children, and persons receiving radiation treatment for medical conditions. The amount of radiation from the backscatter screening equipment currently deployed by TSA is less than ten microrem, or the amount of radiation dose one would receive in less than two minutes of flight time on an airplane at flight altitude, or during one hour standing on the earth with normal exposure to naturally-occurring background radiation at sea level.

Millimeter wave AIT scanners use radio frequency energy in the millimeter wave spectrum to generate a three-dimensional computer image of the body based on the energy reflected from the body. The energy projected by millimeter wave technology is thousands of times less than the energy projected from a cell phone transmission, 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).[15] 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.

In summary, AIT scanning has been assessed by independent scientific entities that have found the technology conforms to national consensus standards.

Constitutional and Legal Issues. The deployment of AIT machines responds to the Congressional and national security mandate to screen airline passengers for both metallic and nonmetallic threats. Despite widespread public acceptance of AIT screening, TSA also provides alternative screening methods. AIT screening has proven effective, and numerous independent studies have addressed health concerns related to AIT screening.

In addition to this objective, factual support for the use of AIT screening, TSA has carefully considered the important Constitutional and statutory concerns raised in your letter as it developed AIT deployment plans. We disagree with your assertions that TSA's deployment of AIT equipment violates the Constitution and various laws, as addressed below.

The Fourth Amendment. TSA strongly disagrees with the statements in your letter that TSA's deployment of AIT machines violates the Fourth Amendment and subjects air travelers to unreasonable searches. Case law supports TSA's analysis.

TSA screening protocols at airport checkpoints have been upheld by the courts as "special needs searches" or "administrative searches" under the Fourth Amendment. *See, e.g., United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007) (*en banc*); *United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2006) (Alito, J.); and *Torbet v. United Airlines*, 298 F.3d 1087 (9th Cir. 2002). A lawful special

---

[15] 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.

needs search requires no warrant and no suspicion of wrongdoing. As long as the search serves a special public need beyond law enforcement and is conducted in a reasonable fashion, it will be found to be permissible under the Fourth Amendment. As stated by the Supreme Court:

> Our precedents have settled that, in certain limited circumstances, the Government's need to discover such latent or hidden conditions, or to prevent their development, is sufficiently compelling to justify the intrusion on privacy entailed by conducting such searches without any measure of individualized suspicion. *NTEU v. Von Raab*, 489 U.S. 656, 668 (1989).

Although the Supreme Court has not had occasion to rule directly on airport security screening, it has referenced security screening favorably in several cases:

> The point is well illustrated also by the Federal Government's practice of requiring the search of all passengers seeking to board commercial airliners, as well as the search of their carry-on luggage, without any basis for suspecting any particular passenger of an untoward motive… When the Government's interest lies in deterring highly hazardous conduct, a low incidence of such conduct, far from impugning the validity of the scheme for implementing this interest, is more logically viewed as a hallmark of its success. *Von Raab*, 489 U.S. at 675, n.3.

> We reiterate, too, that where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as "reasonable" – for example, searches now routine at airports and at entrances to courts and other official buildings. *Chandler v. Miller*, 520 U.S. 305, 323 (1997).

The Federal appellate courts that have directly considered the lawfulness of airport security screening have had little difficulty concluding that screening is a special needs search that serves a compelling public interest:

> When the risk is the jeopardy to hundreds of human lives and millions of dollars of property inherent in the pirating or blowing up of a large airplane, the danger alone meets the test of reasonableness, so long as the search is conducted in good faith for the purpose of preventing hijacking or like damage and with reasonable scope and the passenger has been given advance notice…so that he can avoid it by choosing not to travel by air. *U.S. v. Edwards*, 498 F.2d 496, 500 (2d Cir. 1974).

> First, there can be no doubt that preventing terrorist attacks on airplanes is of paramount importance. Second, airport checkpoints also "advance[] the public interest" …As this Court has held, "absent a search, there is no effective means of detecting which airline passengers are reasonably likely to hijack an airplane." *U.S. v. Hartwell*, 436 F.3d at 179-80.

Because airport security screening serves the compelling public interest of aviation security, it is a valid special needs search and a particular screening method will be lawful as long as it is reasonable.

> A particular airport security screening search is constitutionally reasonable provided that it is "no more extensive or intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives [] [and] that it is confined in good faith to that purpose." (citation omitted)…The search procedures used in this case were neither more extensive nor more intensive than necessary to rule out the presence of weapons or explosives. *Aukai*, 497 F.3d at 962.

In assessing the lawfulness of a particular search, it is important to note that the standard is whether it is reasonable, not whether it is the "least restrictive means:"

> [T]he choice among such reasonable alternatives remains with the governmental officials who have the responsibility for limited public resources. ("[T]he effectiveness inquiry involves only the question of whether the [search] is a 'reasonable method of deterring the prohibited conduct;' the test does not require that the [search] be 'the most effective measure.'")…Thus, our task is to determine not whether LCT's ASP [the screening plan at issue] was optimally effective, but whether it was reasonably so. (citations omitted) *Cassidy v. Chertoff*, 471 F.3d 67, 85 (2d Cir. 2006) (Sotomayor, J.) (upholding screening of ferry passengers).

Turning to the use of AIT, it is clear from the case law that this screening process is a lawful special needs search that strikes the appropriate balance between the interests of aviation security and individual privacy. As made clear by the attempted attack on December 25, 2009, the threat of nonmetallic explosives is real. Also, the nonmetallic threat is not limited to explosives. It is essential for aviation security to have screening methods in use that are capable of detecting threats in the form of powders, liquids, and other nonmetallic materials. The need for AIT also is illustrated by the fact that Congress has mandated TSA to deploy screening methods that are capable of detecting explosives and other nonmetallic threats. See 49 U.S.C. § 44925(a), quoted above. When compared to the substantial risk presented by the threat of terrorist acts against aviation, the impact on individual privacy of AIT screening is minimal. AIT screening has been appropriately tailored to minimize the impact on individual privacy while still providing an effective means of detecting concealed nonmetallic threats. Given the nature of the threats we face today, AIT screening is "no more extensive or intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives." *Aukai*, 497 F.3d at 962.

The Privacy Act. Contrary to your assertions, TSA has not violated the Privacy Act in its AIT deployment. The Privacy Act applies to systems of records in which the records are retrieved by the name or personal identifier of the individual. 5 U.S.C. §552a(a)(5). All Privacy Act requirements, including publication of a system of records, are linked to the agency maintaining a system of records. AIT does not collect and retrieve information by a passenger's name or other identifying information assigned to that individual, nor do we link any AIT images to any personally identifying information about the individual, such as name or date of birth. Indeed, images are not retained and all images are immediately deleted after AIT screening is complete. Consequently, since TSA does not maintain a system of records by using AIT, none of the obligations outlined under section 552a(e), "Agency requirements," apply to TSA.

TSA and DHS, including the DHS Chief Privacy Officer, evaluated the privacy considerations associated with AIT very carefully before TSA deployed the technology. As a result, TSA incorporated robust privacy protections into the program. These protections are reflected in the publicly available Privacy Impact Assessment (PIA), which was published two years ago under the authority given to the Chief Privacy Officer to assess the impacts of technology on privacy, in advance of the deployment of AIT at airports.[16] The PIA outlines a number of measures that TSA has implemented to ensure passenger privacy, and reflects extensive consideration of informal comments from a wide variety of sources, including some of the groups that have signed your letter. Relevant operating protocols include:

- The TSO viewing the images is located remotely from the individual being screened to preserve anonymity and modesty.
- To resolve an anomaly, the TSO viewing the image communicates via radio to direct the TSO at the checkpoint to the location on the individual's body where a threat item is suspected.
- The images are immediately deleted once AIT screening of the individual is complete.
- The image storage functions are disabled by the manufacturer before the AIT equipment is placed in an airport. This function cannot be activated by the TSOs operating the equipment. Your claims regarding storage of images by AIT used in TSA test facilities are irrelevant to the operation of the devices in the airports. As stated in the AIT PIA, "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 cannot be downloaded in operating mode, and the equipment is not networked.
- TSOs are prohibited from bringing any cameras, cell phones, or other recording devices into the image viewing rooms.
- Passengers may opt out of AIT screening and undergo alternate screening procedures.
- Signs at TSA screening checkpoints that utilize AIT advise individuals that AIT screening is optional and that they may request alternate screening.

These operating protocols, coupled with the fact that TSA does not retain or in any way link AIT images to passenger records, provide ample support of TSA's compliance with both the letter and the spirit of the Privacy Act.

Religious Freedom Restoration Act (RFRA). TSA's use of AIT does not violate the RFRA.[17] As an initial matter, TSA's decision to employ AIT would not implicate the RFRA unless it is deemed to substantially burden an individual's exercise of religion.[18] But the very fact that

[16] See Privacy Impact Assessment - http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_tsa_wbiupdate.pdf (July 23, 2009), updating the original PIA dated October 17, 2008.

[17] 42 U.S.C. § 2000bb, *et seq.*

[18] *See, e.g.*, *Navajo Nation v. U.S. Forest Svc.*, 535 F.3d 1058, 1068 (9th Cir. 2008).

passengers are not required to undergo AIT screening – as noted above – necessarily means that its use at airports does not constitute a substantial burden under the RFRA.[19] Because passengers may request a pat-down as an alternative to AIT screening, TSA's use of the technology does not "force[] them to engage in conduct that their religion forbids or . . . prevent[] them from engaging in conduct their religion requires."[20] Indeed, some of the very authorities cited in your letter note that while some religious organizations have expressed concern about AIT, they also acknowledge TSA's effort to accommodate that concern by providing the option for a pat-down.[21]

Courts have long recognized that the government has a compelling interest in maintaining national security and public safety.[22] When requirements predicated on concerns of this type (*e.g.*, prison grooming requirements prohibiting long hair or beards that may facilitate smuggling of contraband, gang identity, etc., and thereby undermine prison security) are pitted against religious precepts (such as the prohibition in Rastafarian or Sunni Muslim traditions that prohibit the cutting of hair or beards), courts have consistently concluded that the requirement may in appropriate circumstances be upheld as the least restrictive means of achieving the compelling government interest.[23]

In light of these considerations, TSA's use of AIT—which serves a compelling governmental interest in security—does not implicate the RFRA. TSA's web site provides further information about how the agency addresses religious and cultural needs at the checkpoint, including the ability of travelers to request alternative, private screening by a TSO of the same gender.[24]

* * * * *

AIT machines, coupled with TSA's layered approach to security, respond to the statutory mandate and the national security imperative to screen airline passengers for both metallic and nonmetallic threats. There is widespread public acceptance of AIT screening, and TSA also provides alternative screening methods. AIT screening has proven effective in addressing ever-

---

[19] *See id.*, at 1069-70.

[20] *Henderson v. Kennedy*, 253 F.3d 12, 16 (D.C. Cir. 2001) (collecting cases).

[21] *E.g.*, your letter at notes 48 and 49.

[22] *Gillette v. United States*, 401 U.S. 437, 462 (1971); *Prince v. Massachusetts*, 321 U.S. 158, 165 (1944); *see also United States v. Acevedo-Delgado*, 167 F. Supp. 2d 477, 481 (D. Puerto Rico 2001) (noting that, in an era in which "the relative peace enjoyed by all citizens of the United States is being challenged more and more frequently by our enemies and terrorists alike," courts considering RFRA challenges "cannot simply zoom in on the concerns of [one person or group(s) of United States citizens] but it must pan back and keep the larger picture in focus [taking into account the concerns of] ALL United States citizens, citizens who are entitled to a well-trained military and national security" (internal quotations omitted)).

[23] *Jackson v. District of Columbia*, 89 F. Supp. 2d 48 (D.D.C. Mar 21, 2000) (collecting authority), *overruled on other grounds*, 254 F.3d 262 (D.C. Cir. 2001).

[24] *See* www.tsa.gov/travelers/airtravel/assistant/editorial_1037.shtm.

changing security threats, and numerous independent studies have addressed health concerns related to AIT screening. TSA has carefully considered the important Constitutional, statutory, and privacy issues associated with the deployment of AIT systems, and has taken numerous steps to address those issues in a manner that protects the rights of travelers.

We appreciate hearing the concerns expressed in your letter and hope this information is helpful.

Sincerely yours,

Francine J. Kerner

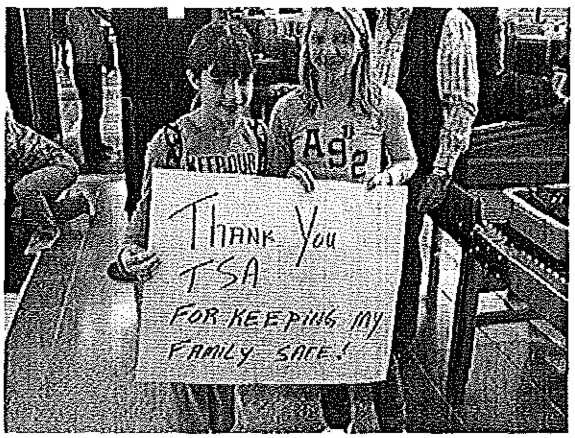
Francine J. Kerner
Chief Counsel

Attachment

11.24.2010

Opt Out Turns Into Opt In

What some protesters threatened as an opt out day has turned into a TSA



appreciation day.

As reports continue to come with normal or below-normal wait times, this will be our final update of this post today.

Though volume was around expected levels, our preparations for today kept wait times at such a minimum that some airports are closing screening lanes due to a lack of passenger throughput.

In addition to our operational updates from the field, we've rounded up news coverage from across the country about today's airport travel experience:

The Dallas Morning News: TSA "outrage": There's no "there" there

New York Times: Travelers' Reports: Better Than Expected

Washington Post: Airport travel starts smoothly, with no sign of delays from scanner protests

CNN: Opt-outs largely no-shows at airports

TalktoTSA Click Here »

Search

Blog Home

Archives

Comment Policy

Contact The TSA Blog Team

Meet Our Bloggers

Please Post Off Topic Comments Here

Previous Posts

- Airport Travel Time Status Updates for 11/24/2010
- Administrator Pistole Reaches Out to Passenger for...
- Check out Our Holiday Travel Tips
- Response to "Young Boy Strip Searched by TSA"
- Airports Who Opt out of TSA Screening are Still Re...
- TSA Myth or Fact: Leaked Images, Handcuffed Hosts,...
- TSA has not, will not and our Advanced Imaging Tec...
- Opting-out of Advanced Imaging Technology and the ...
- CBS News Poll: 4 in 5 Support Full-Body Airport Sc...
- Response to "Female radio host cuffed to chair, ti...

Links

- TSA.gov
- @TSABlogTeam on Twitter
- The Blog @ Homeland Security

Reuters: "Don't touch my junk" airport patdown protests fizzle

Denver Post: DIA: Smooth day at Denver airport

Boston Herald: Terrorism risks trivialized by media

Bloomberg: New York, Chicago Airports Report No Scanner Logjams

Philadelphia Inquirer: Smooth traveling at airport

Pittsburgh Post Gazette: Pittsburgh travelers unfazed by new pat-downs, scanners

NYDN: Thanksgiving travelers opt out of National Opt-Out Day protest, TSA says no delays over body scans

Mercury News: So far, no delays due to security procedures or protests at Oakland International

The Plain Dealer: Smooth, protest-free traffic at Cleveland Hopkins International Airport

CBS: Airport Scanners and 12 Must-Know Radiation "Risks"

Baltimore Sun: BWI traffic moves briskly despite plans for protest

Gizmodo: National Opt-Out Day Is A Bust, Says TSA

Albany Times Union: Lines move smoothly at Albany Int'l Airport, rail, bus stations

KC Star: Passengers moving smoothly through airports

Wired: Air Travelers Opting Out of Opting Out

Seattle King 5 News: Sea-Tac Airport lines move smoothly despite threat of protest

The Dallas Morning News: Security lines moving smoothly at D/FW Airport

Indy Star: Passengers not fussing at Indy airport checkpoints

SF Chron: Smooth sailing at Bay Area airports

Star Ledger: Sen. Robert Menendez says he supports use of full-body scanners, pat-downs

Toronto Star: Travellers opt out of Opt-Out Day

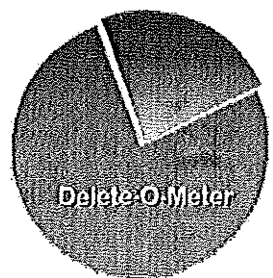
Richmond Times Dispatch: RIC passengers move smoothly through security

The Beacon - USCIS
The Coast Guard Compass
FEMA Blog
The White House Blog

2010 BRONZE ANVIL AWARDS

Download
Acrobat Reader

Subscribe in a reader



Click here to see what type of things cause comments to be deleted.

Email Updates
To sign up for updates or to access your subscriber preferences, please enter your contact information below.

*Email Address

Submit

Transportation Security Administration

USA Today: Fliers facing minimal airport delays, despite protest threats

LA Times: No unusual airport screening delays seen yet, but officials brace for possible 'opt out' protests

Chicago Sun Times: Despite security, few delays at O'Hare--so far

AP: Airport lines move smoothly despite warnings

Orlando Sentinel: Big crowds, but small lines, at Orlando International Airport today

Atlanta Journal-Constitution: No crowds, protests at Hartsfield

FOX: Many Opting Out of "National Opt Out Day"

Dayton Daily News: Dayton airport lines moving quickly; no delays reported

Additional Recent Clips, Op-Eds and Editorials

The Daily Beast: The Media's Pat-Down Frenzy

New York Times: Politicizing Airport Security

Washington Post: Don't Touch My Junk? Grow Up, America.

NYDN: Mayor Bloomberg To Passengers Outraged By Intrusive TSA Checks: Get Over It, It's To 'Keep You Safe'

USAT: Airports Say Security Checks Going Smoothly

USAT: Pistole: Why We Need TSA's Security Measures

Operational Updates as of 5 p.m. EST:

Dallas/Fort Worth: One Advanced Imaging Technology (AIT) opt-out today, and wait times consistently under 12 minutes.

Dallas Love Field: Wait times under 3 minutes.

Salt Lake City: Wait times no more than 5 minutes at both checkpoints one and two; when open, checkpoint 3 has a 2-minute wait time. Across the airport, we have all lanes open and 6 AITs in operation.

Atlanta: 39 total AIT opt outs today (again, out of 47,000 fliers). All were screened and continued to their flights.

Newark: Average wait times today by terminal were 6 minutes for A and C, 11 minutes for B.

New Orleans: The longest reported wait time was approximately 13 minutes. Six passengers opted out of AIT screening. All were screened and continued to their flights.

Iowa and Kansas: No disruptions, no wait times greater than 10 minutes. According to federal security director, lots of passenger compliments.

Denver: Current wait times are 3-4 minutes per checkpoint.

Colorado Springs: 5-minute average wait time, and no AIT opt-outs.

Minneapolis: Wait times are currently 5-10 mins. No incidents.

Detroit: No wait time over 20 minutes all day.

Green Bay: Wait time is 3 minutes.

Indianapolis: 24-minute peak this morning at 6 a.m. Nothing near since.

Louisville: 5-10 minute wait times.

Los Angeles: Los Angeles: 113 AIT opt outs across LAX's 8 terminals, which is less than 1 percent of the approximately 50,000 travelers screened at LAX today. All AIT opt-outs were screened and continued to their flights.

Charlotte: 18,000 passengers screened so far today, and estimated 24,000 will be screened by end of day. 1 AIT opt out today.

Cincinnati: The peak wait time was 10 minutes, and average is 5 minutes.

Chicago O'Hare: The longest wait was 15 minutes at one checkpoint, and has been under 10 minutes airport-wide for the most part.

Cleveland: Under 20 minutes for wait times all day, with a 10-minute average. Current wait times are less than 5 minutes. 0.66 percent opt out rate today.

Boston: Approximately 56,000 passengers screened with 300 AIT opt outs, which is less than 1 percent of all travelers and less than a normal day at the airport's 17 AITs. All were screened and continued to their flights. The longest wait time all day was 12 minutes in terminal A in very early morning, and it was very short lived given all lanes were open.

Detroit: 25,000 passengers screened today, and 57 AIT opt-outs. All were screened and continued to their flights.

Blogger Bob
TSA Blog Team

Labels: Blogger Bob, Holiday Travel, Wait Times

Digg This! • Save to del.icio.us (2 saves, tagged: privacy tsa via:packrati.us) • Technorati Links • Share on Facebook

Posted By Blogger Bob At 5:25 PM

196 Comments:

Anonymous **Anonymous Said...**

Well there you have it. A handful of terrorists have forced America to transform into a scared, quivering mass. Congratulations Osama!

November 24, 2010 5:29 PM

Anonymous **Anonymous Said...**

Huzzah! Huzzah for the Stakhonovites of the state security apparatus! Lubyanska security checkpoint exceeds all production quotas!

My guess: people aren't opting out because they don't want to be inconvenienced by the TSA anymore than they already are, and they don't want to inconvenience others. I doubt very much that this is a broad vote of approval for a child-groping, granny-scanning counterterrorist agency that has never caught a single terrorist.

November 24, 2010 5:31 PM

Anonymous **Anonymous Said...**

Your boss asked us not to cause a disruption. We listened.

Will the TSA?

November 24, 2010 5:32 PM

Anonymous **Anonymous Said...**

The relative lack of opt outs is not a glowing commendation on the TSA, in fact, the media coverage that ensued is more proof that the distaste is still fresh on everybody's minds. This will an ill-timed effort, in that many fliers no doubt were concerned with retaliatory detainments, and the wrath of their family if they dared to miss Thanksgiving. Just because nobody is staging a mass protest on the eve of Thanksgiving doesn't mean you can assume your love by travelers. We still despise what you have done to cancer patients, people with steel implants in their hips, people with colostomy bags, children without shirts, children with mental issues who didn't want to be touched, people sensitive to radiation, and people who frankly don't want their junk touched. Where did you get the part that most Americans are thankful for you today? I'll have a shot of that drink, it sure sounds potent.

November 24, 2010 5:34 PM

Anonymous **Anonymous Said...**

Bob, how many strip-search machines were turned off or not in use? People can't opt out of something that's not being used.

November 24, 2010 5:37 PM

Anonymous **Anonymous Said...**

Well Bob, you're lying. There were three opt outs in one group during the time I was going through at one of the airports you identify as "no opt outs".

That aside, I don't think for a moment that there will be many (making the need to lie just silly, but that's another matter. After all, the gov't also told us Agent Orange was harmless: lying is in your DNA. But I digress.) There will be few because among other reasons FAR FAR more people who rarely fly are in the air this week. Those of us who do it all the time are just a bt less happy about your Kabuki theater.

November 24, 2010 6:05 PM

Anonymous **Anonymous Said...**

If opt-out is so terrible, why is it an option?

November 24, 2010 6:37 PM

Anonymous **Anonymous Said...**

Yes, it is well established that the average person will make the correct economic tradeoff that it is less costly to sacrifice civil rights than be a martyr. That doesn't legitimize your actions or even suggest people agree with them. However, I do think that when the passenger volumes are counted for this holiday season, you will see a material and visible negative effect.

November 24, 2010 6:39 PM

Anonymous **Anonymous Said...**

I think I commented last week that it is a typical bureaucratic response to protect one's job by putting every ounce of resources into making today go smoothly. Don't worry, John, you will still be fired. And you deserve it.

November 24, 2010 6:40 PM

Anonymous **Anonymous Said...**

TSA's primary mission isn't to keep passengers safe. It's to keep passengers scared of threats that aren't nearly as big as they would have us believe.

November 24, 2010 6:42 PM

[x] Anonymous **Anonymous Said...**

How does TSA respond to:
http://latimesblogs.latimes.com/money_co/2010/11/new-poll-says-61-oppose-new-airport-security-measures.html

61% of Americans oppose new security measures. Where's the link to this poll on the TSA homepage?

November 24, 2010 6:53 PM

[x] Anonymous **Anonymous Said...**

Gizmodo says that TSA turned off the machines at most airports, and wasn't doing the full body searches. They ask if "no opt-outs" means "no AIT machines".

No waits. No lines. That's great, but this should be ringing alarms: For the first time in the history of Thanksgiving travel, there are no lines at airport security.

I want to know how much over-time TSA blew on this PR stunt.

November 24, 2010 6:54 PM

[x] Blogger **Mike Said...**

Either the TSA has become the most efficient arm of the US Government, or the number of holiday travelers is likely far below normal.

My money's on the latter.

November 24, 2010 7:00 PM

[x] Anonymous **Anonymous Said...**

Great work today, Blogger Bob! We were thinking about your work at such a pivotal, possibly problematic time. Looks like you did a good job getting out the lack of delay and a positive story for TSA and USG!!

Doug at NASA

November 24, 2010 7:14 PM

[x] Anonymous **Anonymous Said...**

None of this post makes your procedures and less a violation of the 4th amendment. The majority of the people would let a police officer search their car if they were stopped for speeding but this does not give the cop a right to perform an unreasonable search.

Statement of Rep. Danny Davis (D-IL) on behalf of Ranking Member Sheila Jackson Lee (D-TX)

Subcommittee on Transportation Security
Committee on Homeland Security

Hearing "TSA Recent Scanner Trouble: Real Strategy or Wasteful Smokescreen"

November 15, 2012

This Subcommittee has closely followed Advanced Imaging Technology for several Congresses—under Democratic leadership and Republican leadership.

On this side of the aisle, my colleagues have questioned both the effectiveness of the technology and the cost of the machines.

However, few issues have caused us as much concern as whether these machines undermine the fundamental right of privacy.

My colleagues have regularly asked whether a passenger must surrender her basic right of bodily security to assure the nation's security.

It is gratifying to see that the Chairman shares both our concerns and our commitment to privacy.

On March 17, 2009, under the leadership of Congresswoman Jackson Lee, this Subcommittee held a hearing evaluating the detection and screening technologies being used by the Department of Homeland Security.

That hearing offered members a chance to understand the enhanced screening technologies, protocols and procedures.

In the aftermath of the Christmas Day bomber—also known as the Underwear bomber—we expressed our support for the deployment of these advanced imaging technologies and were assured that these new machines would effectively diminish the threats that continue to put aviation security at risk.

Since 2009, DHS and TSA have taken steps to implement A-I-T devices in most of the major airports in the United States.

However, we know that no technology is perfect.

Based on a conservative estimate, it appears that the Department has invested at least 80 million dollars on this technology so far.

Given the challenges that TSA has faced in assuring privacy protections in these machines, and the forward movement of technology, we must consider where we go from here.

Transportation Security Administration

Passenger Screening Using AIT

Initial Regulatory Impact Analysis

NPRM

RIN: 1652-AA67

INITIAL REGULATORY EVALUATION,

REGULATORY FLEXIBILITY DISCUSSION,

TRADE IMPACT ASSESSMENT, AND

UNFUNDED MANDATES ASSESSMENT

NOTICE OF PROPOSED RULEMAKING

(49 CFR Part 1540)

Regulatory and Economic Analysis

Office of Security Policy and Industry Engagement

Transportation Security Administration

Department of Homeland Security

Arlington, VA 20598

March 19, 2013

TABLE OF CONTENTS

LIST OF TABLES

LIST OF ABBREVIATIONS

AIT	Advanced Imaging Technology
APL	Applied Physics Laboratory
AQAP	Al Qaeda in the Arabian Peninsula
ATR	Automated Target Recognition
ATSA	Aviation and Transportation Security Act
BLS	Bureau of Labor Statistics
BTS	Bureau of Transportation Statistics
CAFR	City's Annual Financial Report
CBP	Customs and Border Protection
CDRH	Center for Devices and Radiological Health
CFR	Code of Federal Regulations
DHS	Department of Homeland Security
DLA	Defense Logistics Agency
DOT	Department of Transportation
EO	Executive Order
EPIC	Electronic Privacy Information Center
ETD	Explosives Trace Detection
FAA	Federal Aviation Administration
FAT	Factory Acceptance Test
FDA	Food and Drug Administration's
FTE	Full Time Equivalent
FOC	Full Operating Capacity
GDP	Gross Domestic Product

IED	Improvised Explosive Device
IO	Image Operator
IRFA	Initial Regulatory Flexibility Analysis
IRTPA	Intelligence Reform and Terrorism Prevention Act
MTSA	Maritime Transportation Security Act
NAICS	North American Industry Classification System
NIST	National Institute for Standards and Technology
NPRM	Notice of Proposed Rulemaking
OEM	Original Equipment Manufacturer
OMB	Office of Management and Budget
OT&E	Operational Test & Evaluation
PMIS	Performance Management Information System
PMO	Program Management Office
PSP	Passenger Screening Program
QT&E	Qualification Test & Evaluation
RFA	Regulatory Flexibility Act
RIA	Regulatory Impact Analysis
RMAT	Risk Management Analysis Tool
SAT	Site Acceptance Test
SBA	Small Business Administration
SAM	Screener Allocation Model
SME	Subject Matter Expert
SO	System Operator
SSI	Sensitive Security Information

TSA	Transportation Security Administration
TSIF	TSA Systems Integration Facility
TSL	Transportation Security Laboratory
TSO	Transportation Security Officer
UMRA	Unfunded Mandates Reform Act
VSL	Value of a Statistical Life
WTMD	Walk Through Metal Detector

EXECUTIVE SUMMARY

Changes to federal regulations must undergo several types of economic analyses. First, Executive Orders (EO) 13563 and 12866 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). EO 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. Under EO 12866, TSA must determine whether a regulatory action is significant and therefore subject to the requirements of the EO and review by the Office of Management and Budget (OMB). Section 3(f) of the EO defines a "significant regulatory action" as any regulatory action that is likely to result in a rule that: (1) has an annual effect on the economy of $100 million or more, or adversely affects in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local or tribal governments or communities (also referred to as economically significant); (2) creates serious inconsistency or otherwise interferes with an action taken or planned by another agency; (3) materially alters the budgetary impacts of entitlement grants, user fees, or loan programs or the rights and obligations of recipients thereof; or (4) raises novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in the EO.

This proposed rule is a "significant regulatory action" that is economically significant under section 3(f) (1) of EO 12866. Accordingly, OMB has reviewed this regulation. Second, the Regulatory Flexibility Act (RFA) of 1980 requires agencies to consider the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. § 2531-2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. In developing U.S. standards, this act requires agencies to consider international standards and, where appropriate, to use them as the basis for U.S. standards. Finally, the Unfunded Mandates Reform Act of 1995 (UMRA) (Public Law 104-4) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

In conducting these analyses on the Passenger Screening Using Advanced Imaging Technology (AIT) notice of proposed rulemaking (NPRM) (also referred to as the AIT NPRM), TSA provides the following conclusions and summary information:

(1) TSA has determined that this NPRM is a significant rulemaking within the definition of EO 12866, as estimated annual costs or benefits exceed $100 million in any year;
(2) TSA's Initial Regulatory Flexibility Analysis suggests that this rulemaking would not have a significant economic impact on a substantial number of small entities under section 605(b) of the RFA;
(3) TSA has determined that this NPRM imposes no significant barriers to international trade as defined by the Trade Agreement Act of 1979; and
(4) TSA has determined that this NPRM does not impose an unfunded mandate on State, local, or tribal governments as defined by the UMRA.

This executive summary highlights the costs of this NPRM, which proposes to codify the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. These costs are incurred by airport operators, the traveling public, Rapiscan, and TSA. Some airport operators incur utility costs for the additional electricity consumed by AIT machines. Although passenger processing with AIT may be slightly longer than a walk through metal detector (WTMD), overall passenger screening system times do not increase with AIT.[1] The small percentage of passengers who choose to opt out of AIT screening will incur opportunity costs due to the additional screening time needed to receive a pat-down. Rapiscan, a company that manufactures AIT machines, will incur a cost to remove

---

[1] AIT machines do not reduce total throughput per hour at the current screening environments as x-ray baggage screening operates at lower throughput rates. Passengers experience no additional wait time because passengers wait for their personal belongings after AIT or WTMD regardless of which screening technology is used. Chapter 1 details the assumptions and current state of the passenger screening environment.

backscatter AIT units in 2013 that have been deployed in previous years.[2] TSA incurs equipment costs associated with the life cycle of AIT machines (testing, acquisition, maintenance, etc.), personnel costs to hire Transportation Security Officers (TSOs) to operate the AIT machines, utility costs at reimbursed airports, and training costs to train other TSOs to operate AIT machines.

Need for Regulatory Action

In 2010, TSA was sued over its use of AIT by the Electronic Privacy Information Center (EPIC). In the decision rendered by the U.S. Court of Appeals for the District of Columbia Circuit in Electronic Privacy Information Center v. U.S. Department of Homeland Security,[3] the Court directed TSA to conduct notice and comment rulemaking on the use of AIT. However, the Court also allowed TSA to continue using AIT as part of its airport security operations. TSA developed this NPRM to comply with the Court's decision. This NPRM will provide public notice and an opportunity to comment on TSA's use of AIT.

TSA Response

Once TSA was given the responsibility to conduct security screening operations for commercial aviation, the agency deployed various technologies to screen persons and their baggage prior to boarding commercial aircraft. The primary passenger screening technology in place at screening checkpoints prior to the deployment of AIT was the walk-through metal detector (WTMD). WTMDs alarm if a passenger has metallic objects on his person, including such harmful objects as knives and guns. Passengers who alarm the WTMD receive additional screening to resolve an alarm. Current procedures for WTMD alarms allow a passenger to divest metallic objects from his person and pass through the WTMD until the alarm is resolved. If the alarm cannot be resolved with divesting metallic objects and repeating WTMD screening, a TSO performs

[2] On December 21, 2012, TSA terminated part of its contract with Rapiscan for the Convenience of the Government since it could not meet development related issues in regards to ATR by the Congressionally-mandated June 2013 deadline. As a result of the contract termination, Rapiscan will pay for the removal of all units still in the field.

[3] 653 F.3d 1 (D.C. Cir. 2011).

additional screening to resolve the alarm. If the passenger cannot undergo WTMD screening, the passenger receives a pat-down.

Cost and Baseline

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. As the AIT machine life cycle from deployment to disposal is eight years, the period of analysis for estimating the cost of AIT is eight years. However, as AIT deployment began in 2008, there are costs that have already been borne by TSA, the traveling public, and airport operators that were not due to this rule. Consequently, in the initial regulatory impact analysis for this proposed rule, TSA reports the AIT-related costs that have already occurred (years 2008 - 2011), while considering the additional cost of this rulemaking to be years 2012-2015.[4] By reporting the costs that have already happened and estimating future costs in this manner, TSA considers and discloses the full eight year life cycle of AIT machine deployment. The cost attributed to the NPRM compares the screening environment prior to the deployment and implementation of AIT screening (centered around WTMDs) to the screening environment with AIT technology. Consequently, costs and benefits estimated to result from the provisions of this NPRM are compared to the costs incurred by impacted entities if TSA continued to use WTMD-centered screening.

In this analysis, the number of AIT machines deployed from 2008 to 2011 is known and certain; the estimates for the number of machines deployed from 2012 to 2015 represent TSA's best estimate of AIT acquisition and deployment based on current and expected funding levels for the

---

[4] OMB's "Regulatory Impact Analysis: A Primer" states: "The benefits and costs of a regulatory action typically take place in the future." http://www.whitehouse.gov/sites/default/files/omb/inforeg/regpol/circular-a-4_regulatory-impact-analysis-a-primer.pdf . Circular A-4 describes costs and benefits in terms of future or expected costs and benefits (see "Developing Benefit and Cost Estimates," http://www.whitehouse.gov/omb/circulars_a004_a-4/). Circular A-94 instructs that "sunk costs and realized benefits should be ignored" and that "past experience is relevant only in helping to estimate what the value of future benefits and costs might be" (http://www.whitehouse.gov/omb/circulars_a094/).

program. Table 1 and Table 2 summarize the number of AIT screening machines TSA projects to deploy, by category of airport, over the eight-year analysis period.[5]

Table 1: AIT Newly Deployed by Year by Category of Airport

(AIT Units)

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	16	14	0	0	0	**30**
2009	0	2	0	0	0	**2**
2010	301	135	20	2	0	**458**
2011	1	42	16	10	0	**69**
2012	179	59	68	83	34	**423**
2013*	0	0	0	0	0	**0**
2014	14	9	1	5	15	**44**
2015	15	10	1	2	17	**45**

* TSA estimates the deployment figures for 2013 based on a weighted average assuming the first 5 months of the year with the Rapiscan units and the last 7 months of the year without the Rapiscan units. See Appendix B for the inputs and estimation for 2013.

[5] TSA categorizes federalized airports into groups as a measurement of passenger flow. Category X has the greatest number of passenger traffic while Category IVs have the least.

Table 2: AIT Units In-Service by Year by Category of Airport

	Category X	**Category I**	**Category II**	**Category III**	**Category IV**	**Total**
2008	16	14	0	0	0	**30**
2009	16	16	0	0	0	**32**
2010	317	151	20	2	0	**490**
2011	318	193	36	12	0	**559**
2012	497	252	104	95	34	**982**
2013*	366	212	99	93	34	**805**
2014	341	193	97	96	49	**776**
2015	356	203	98	98	66	**821**

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Table 3 shows the flow of AIT units throughout the duration of the analysis. Throughout 2013, Rapiscan AIT machine are removed from all TSA checkpoints. The term *newly deployed* refers to the number of additional AIT machines added to TSA checkpoints in the given year. The term *in-service* refers to the total number of current AIT machines actively being used at TSA checkpoints in the given year.

Table 3: Flow of AIT Units In and Out of the Airports

Year	**Rapiscans Deployed**	**Rapiscans Removed**	**In-Service Rapiscans**	**L3s Deployed**	**In-Service L3s**	**Total Deployed**	**Total In-Service**
	a	**b**	**$c_t = c_{t-1} + a - b$**	**d**	**$e_t = e_{t-1} + d$**	**f = a + d**	**g = c + e**
2008	0	0	0	30	30	**30**	**30**
2009	0	0	0	2	32	**2**	**32**
2010	250	0	250	208	240	**458**	**490**
2011	0	0	250	69	309	**69**	**559**
2012*	0	76	250	423	732	**423**	**982**
2013	0	174	0	0	732	**0**	**732**
2014	0	0	0	44	776	**44**	**776**
2015	0	0	0	45	821	**45**	**821**

* TSA assumes that the 76 Rapiscans were removed on the last day of 2012 and were in-service for the duration of 2012.

At the end of 2012, 76 Rapiscans AIT machines are removed while the remaining 174 are assumed to be removed on May 31, 2013. To account for Rapiscans removal in 2013, TSA uses a weighted average for its in-service number which is described in full in Appendix B.

TSA reports that the cost of AIT deployment from 2008-2011 has been approximately $841.2 million (undiscounted) and that TSA has borne over 98 percent of all costs related to AIT deployment. TSA projects that from 2012-2015 total AIT-related costs will be approximately $1.5 billion (undiscounted), $1.4 billion at a three percent discount rate, and $1.3 billion at a seven percent discount rate. During 2012-2015, TSA estimates it will also incur over 98 percent of AIT-related costs, with equipment and personnel costs being the largest categories of costs.

Table 4 below reports the costs that have already happened (2008-2011) by cost category, while Table 5 shows the additional costs TSA is attributing to this rulemaking (2012-2015).[6] Table 6 shows the total cost of AIT deployment from 2008 to 2015.

Table 4: Cost Summary (Net Cost[7] of AIT Deployment from 2008-2011) by Cost Component (Costs Already incurred in $ 1,000s – undiscounted)

Year	Passenger Opt-Outs	Industry Utilities	TSA Costs				Total
			Personnel	Training	Equipment	Utilities	
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$52,535.3
2009	$32.2	$5.7	$15,618.6	$88.0	$42,563.6	$20.4	$58,328.5
2010	$262.2	$158.2	$247,566.7	$5,332.8	$119,105.4	$241.4	$372,666.6
2011	$1,384.2	$186.7	$284,938.7	$15,354.4	$55,567.2	$269.1	$357,700.2
Total	**$1,685.6**	**$356.3**	**$562,813.0**	**$21,164.7**	**$254,661.3**	**$549.6**	**$841,230.6**

[6] Totals in tables throughout the regulatory evaluation may not sum due to rounding.

[7] TSA removed costs related to WTMD that would have occurred regardless of AIT deployment to obtain an estimated net cost for AIT. TSA shows these assumptions in the Baseline Cost section.

Table 5: Cost Summary (Net Cost of AIT Deployment 2012-2015) by Cost Component (AIT Costs in $ 1,000s)

Year	Passenger Opt-Outs	Industry Utilities	TSA Costs				Rapiscan	Total
			Personnel	Training	Equipment**	Utilities	Removal	
2012	$2,716.5	$325.7	$375,866.9	$12,043.0	$116,499.3	$473.0	$0.0	$507,924.4
2013*	$3,991.7	$329.3	$280,844.3	$4,277.5	$51,588.8	$324.4	$1,809.6	$343,165.7
2014	$4,238.7	$312.0	$263,677.6	$4,190.5	$51,397.8	$317.7	$0.0	$324,134.2
2015	$5,611.8	$300.3	$278,580.2	$4,144.2	$68,052.6	$365.7	$0.0	$357,054.9
Total	**$16,558.7**	**$1,267.3**	**$1,198,969.0**	**$24,655.2**	**$287,538.5**	**$1,480.9**	**$1,809.6**	**$1,532,279.2**
Discounted 3%	$15,265.0	$1,178.9	$1,118,459.3	$23,810.2	$269,233.7	$1,380.7	$1,705.7	$1,431,033.5
Discounted 7%	$13,766.6	$1,075.8	$1,024,344.7	$22,048.8	$247,810.4	$1,263.8	$1,580.6	$1,311,890.7

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

**Equipment costs for TSA include acquisition, operation, maintenance, Rapiscan unit removal in 2012 by TSA and reallocation of AIT units.

Table 6: Cost Summary (Net Cost of AIT Deployment 2008-2015) by Cost Component (AIT Costs in $ 1,000s -undiscounted)

Year	Passenger Opt-Outs	Industry Utilities	TSA Costs				Rapiscan	Total
			Personnel	Training	Equipment	Utilities	Removal	
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$0.0	$52,535.3
2009	$32.2	$5.7	$15,618.6	$88.0	$42,563.6	$20.4	$0.0	$58,328.5
2010	$262.2	$158.2	$247,566.7	$5,332.8	$119,105.4	$241.4	$0.0	$372,666.6
2011	$1,384.2	$186.7	$284,938.7	$15,354.4	$55,567.2	$269.1	$0.0	$357,700.2
2012	$2,716.5	$325.7	$375,866.9	$12,043.0	$116,499.3	$473.0	$0.0	$507,924.4
2013*	$3,991.7	$329.3	$280,844.3	$4,277.5	$51,588.8	$324.4	$1,809.6	$343,165.7
2014	$4,238.7	$312.0	$263,677.6	$4,190.5	$51,397.8	$317.7	$0.0	$324,134.2
2015	$5,611.8	$300.3	$278,580.2	$4,144.2	$68,052.6	$365.7	$0.0	$357,054.9
Total	**$18,244.4**	**$1,623.6**	**$1,761,782.0**	**$45,819.9**	**$542,199.9**	**$2,030.4**	**$1,809.6**	**$2,373,509.9**

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Security Benefits

The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT that is capable of detecting both metallic and non-metallic weapons and explosives. The nature of the threat to transportation security has evolved since September 11, 2001. Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. Below are examples of this threat:

- On December 22, 2001, on board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.

- In 2004, terrorists mounted a successful attack on two domestic Russian passenger aircraft using non-metallic explosives that were concealed on the torsos of female passengers.
- In 2006, terrorists in the United Kingdom plotted to bring liquid explosives on board aircraft that would be used to construct and detonate a bomb while in flight.
- A bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in the December 25, 2009 attempt by Umar Farouk Abdulmutallab to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In a recent terrorist plot thwarted in May 2012, AQAP had developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

As evidenced by the incidents described above, TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. The device used in the December 25, 2009, attempt is illustrative. It was cleverly constructed and intentionally hidden on a sensitive part of the body to avert detection. If detonated, the lives of the almost 300 passengers and crew and untold numbers of people on the ground would have been in jeopardy.

AIT is proven technology and provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security plan. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the walk-through metal detector.

In Tables 6 and 7 below, we present annualized cost estimates and qualitative benefits of AIT deployment. In Table 6, we show the annualized net cost of AIT deployment from 2012 to 2015. As previously explained (see footnote 3 above), costs incurred from 2008-2011 occurred in the past and are not considered costs attributable to this proposed rule. However, given the life cycle of the AIT technology considered in this analysis is eight years; we have also added Table 7 showing the annualized net cost of AIT deployment from 2008-2015 (full eight year life cycle including "sunk costs" from 2008 to 2011). While the total costs of AIT deployment for a full eight year life cycle (2008-2015) are higher than the total costs of AIT deployment during the four year period of 2012-2015, the annualized costs ($368,262.8 at 7 percent discount) of the full eight year cycle shown in Table 7 are actually lower than the annualized costs ($387,307.0 at 7 percent discount) of the 2012-2015 deployment shown in Table 6. As previously shown in Tables 3 and 4, AIT deployment costs in 2008 and 2009 are relatively low compared with the later year AIT expenditures, resulting in lower annualized costs for the eight year life cycle of 2008-2015. The costs are annualized and discounted at both three and seven percent and presented in 2011 dollars.

Table 7: OMB A-4 Accounting Statement ($ 1,000s for 2012-2015)

Category	***Primary Estimate***		***Minimum Estimate***	***Maximum Estimate***	***Source Citation (Initial RIA, preamble, etc.)***
BENEFITS					
Monetized benefits	Not estimated		Not estimated	Not estimated	Initial RIA
Annualized quantified, but unmonetized, benefits	0		0	0	Initial RIA
Unquantified benefits	The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT technology that is capable of detecting both metallic and non-metallic weapons and				Initial RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$387,307.0			Initial RIA
	(3%)	$384,986.7			
Annualized quantified, but unmonetized, costs	0		0	0	Initial RIA
Qualitative costs (unquantified)	Not estimated				Initial RIA
TRANSFERS					
Annualized monetized transfers: "on budget"	0		0	0	Initial RIA
From whom to whom?	N/A		N/A	N/A	None
Annualized monetized transfers: "off-budget"	0		0	0	Initial RIA
From whom to whom?	N/A		N/A	N/A	None
Miscellaneous Analyses/Category	***Effects***				***Source Citation (Initial RIA, preamble, etc.)***
Effects on state, local, and/or tribal	None				Initial RIA
Effects on small businesses	No significant economic impact anticipated. Prepared IRFA.				Initial Regulatory Flexibility Act
Effects on wages	None				None
Effects on growth	None				None

Table 8: OMB A-4 Accounting Statement ($ 1,000s for 2008-2015),

(Eight year lifecycle)

Category	***Primary Estimate***		***Minimum Estimate***	***Maximum Estimate***	***Source Citation (Initial RIA, preamble, etc.)***
BENEFITS					
Monetized benefits	Not estimated		Not estimated	Not estimated	Initial RIA
Annualized quantified, but unmonetized,	0		0	0	Initial RIA
Unquantified benefits	The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT technology that is capable of detecting both metallic and non-metallic weapons and explosives.				Initial RIA
COSTS					
Annualized monetized costs (discount rate in parentheses)	(7%)	$368,262.8			Initial RIA
	(3%)	$326,410.1			
Annualized quantified, but unmonetized, costs	0		0	0	Initial RIA
Qualitative costs (unquantified)	Not estimated				Initial RIA
TRANSFERS					
Annualized monetized transfers: "on budget"	0		0	0	Initial RIA
From whom to whom?	N/A		N/A	N/A	None
Annualized monetized transfers: "off-budget"	0		0	0	Initial RIA
From whom to whom?	N/A		N/A	N/A	None
Miscellaneous Analyses/Category	***Effects***				***Source Citation (Initial RIA, preamble, etc.)***
Effects on state, local, and/or tribal	None				Initial RIA
Effects on small businesses	No significant economic impact anticipated. Prepared IRFA.				IRFA
Effects on wages	None				None
Effects on growth	None				None

Alternatives

As alternatives to the preferred regulatory proposal presented in the NPRM, TSA examined three other options. The following table briefly describes these options, which include a continuation of the screening environment prior to 2008 (no action), increased use of physical pat-down searches that supplements primary screening with WTMDs, and increased use of explosive trace detection (ETD) screening that supplements primary screening with WTMDs. These alternatives, and the reasons why TSA rejected them in favor of the proposed rule, are discussed in detail in Chapter 3 of this regulatory evaluation.

Table 9: Comparison of Regulatory Alternatives

Regulatory Alternative	Name	Description
1	No Action	Under this alternative, the passenger screening environment remains the same as it was prior to 2008. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.
2	Pat-Down	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting a pat-down on a randomly selected portion of passengers after screening by a WTMD.
3	ETD Screening	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting Explosives Trace Detection (ETD) screening on a randomly selected portion of passengers after screening by a WTMD.
4	AIT (NPRM)	Under this alternative, the proposed alternative, TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down.

Initial Regulatory Flexibility Analysis

This NPRM proposes to codify the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. TSA identified 102 small entities that could have potentially incurred additional utility costs due to AIT; however, TSA reimburses the additional utility costs for five of these small entities. Consequently, this rule would cause 97 small entities to incur additional direct costs. Of the 97 small entities affected by this proposed rule, 96 are small governmental jurisdictions with populations less than 50,000. A privately-owned airport is considered small under SBA standards if revenue amounts to less than $30 million. TSA identified one small privately-owned airport.

The small entities incur an incremental cost for utilities as a result of increased power consumption from AIT operation. To estimate the costs of the deployment of AIT for small entities, TSA uses the average kilowatt hour (kWh) consumed per unit on an annual basis at federalized airports. Depending on the size of the airport, TSA estimates the average additional utility costs to range from $347 to $1,012 per year while the average annual revenue for these small entities ranges from $69.5 million to $133.1 million per year. Consequently, TSA estimates that the cost of this NPRM on small entities represents approximately 0.001 percent of their annual revenue. Therefore, TSA's Initial Regulatory Flexibility Analysis suggests that this rulemaking would not have a significant economic impact on a substantial number of small entities. Chapter 5 outlines the Initial Regulatory Flexibility Analysis assumptions and the analysis for these estimates.

CHAPTER 1: INTRODUCTION

TSA provides this regulatory evaluation to present an economic analysis of the AIT NPRM. This evaluation describes the previous screening environment—how the checkpoint operated prior to the implementation of AIT (i.e., baseline scenario), discusses required or expected changes to this environment resulting from the provisions of the proposed rule, and assesses the associated costs and burdens placed on impacted industries, governments, and the traveling public resulting from the provisions of the proposed rule.

Background

The nature of the threat to transportation security has evolved since September 11, 2001. Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. Below are examples of this threat:

- On December 22, 2001, onboard an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.
- In 2004, terrorists mounted a successful attack on two domestic Russian passenger aircraft using non-metallic explosives that were concealed on the torsos of female passengers.
- In 2006, terrorists in the United Kingdom plotted to bring liquid explosives on board aircraft that would be used to construct and detonate a bomb while in flight.
- A bombing plot by AQAP culminated in the December 25, 2009 attempt by Umar Farouk Abdulmutallab to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In a recent terrorist plot thwarted in May 2012, AQAP had developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

As evidenced by the incidents described above, TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. The device used in the December 25, 2009, attempt is illustrative. It was cleverly constructed and intentionally hidden on a sensitive part of the body to avert detection. If detonated, the lives of the almost 300 passengers and crew and untold numbers of people on the ground would have been in jeopardy.

Congressional Direction to Pursue AIT

In 2004, Congress authorized TSA to continue to explore the use of new technologies to improve its threat detection capabilities. 49 U.S.C. 44925. Specifically, the law provides:

> Deployment and use of detection equipment at airport screening checkpoints
>
> (a) Weapons and explosives.--The Secretary of Homeland Security shall 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 . . . the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.
>
> (b) [The TSA Administrator shall submit]. . . a strategic plan to promote the optimal utilization and deployment of explosive detection equipment at airports to screen individuals and their personal property. Such equipment includes walk-through explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners.

Additional references[8] in Congressional reports accompanying appropriations and authorizing legislation demonstrate Congress's continued direction to DHS and TSA to pursue enhanced screening technologies and imaging technology, specifically:[9]

> 1) Explanatory Statement, House Appropriations Committee Print for Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (FY09 DHS Appropriations) Pub.L. 110-329 at p. 640:
>
> > The bill provides $250,000,000 for Checkpoint Support to deploy a number of emerging technologies to screen airline passengers and carry-on baggage for explosives, weapons, and other threat objects by the most advanced equipment currently under development. TSA is directed to spend funds on multiple whole body imaging technologies including backscatter and millimeter wave as directed in the Senate report.

---

[8] See also, sec. 109 of the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71 (2001), as amended by sec. 1403(b) of the Homeland Security Act of 2002, Pub. L. 107-296, "(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation" and Title IV of the American Recovery and Reinvestment Act of 2009, Pub. L. 111-5 ". . .for procurement and installation of checked baggage explosives detection systems and checkpoint explosives detection equipment."

[9] Additionally, the following language appeared in S. Rep. No. 111-222, accompanying S. 3602, the Department of Homeland Security Appropriations Bill 2011 at 60-61: "As requested, $192,200,000 is provided to deploy an additional 503 AIT units bringing the total to 1,000. AIT units screen passengers for metallic and non-metallic threats—including weapons, explosives, and other objects concealed under layers of clothing. With this increase, there will be an AIT unit in most Category X, I, and II airports. The Committee is aware of efforts by TSA to deploy automated target recognition [ATR] capability with AIT units in fiscal years 2010 and 2011. ATR displays a passenger's image as a stick figure on a monitor attached to an AIT unit, improving privacy protections and eliminating the need for private rooms to view AIT images." Senate 3602 was not passed by Congress; rather, DHS's 2011 appropriations were provided through a series of continuing resolutions and Pub. L. 112-10, which appropriated funding at essentially the same level as in FY2010. Thus, while of limited legal effect, the statement does express the Senate Appropriation Committee's intent to fund AIT.

2) H. Rep. 110-862 at p. 64, FY09 DHS Appropriations:

> Over the past year, TSA has made some advances in testing, piloting, and deploying next-generation checkpoint technologies that will be used to screen airline passengers and carry-on baggage for explosives, weapons, and other threats. Even with this progress, however, additional funding is necessary to expedite pilot testing and deployment of advanced checkpoint explosive detection equipment and screening techniques to determine optimal deployment as well as preferred operational and equipment protocols for these new systems. Eligible systems may include, but are not limited to, advanced technology screening systems; whole body imagers; . . . The Committee expects TSA to give the highest priority to deploying next-generation technologies to designated Tier One threat airports.

3) S. Rep. 110-396 at p. 60, FY09 DHS Appropriations:

> WHOLE BODY IMAGERS. The Committee is fully supportive of emerging technologies at passenger screening checkpoints, including the whole body imaging program currently underway at Category X airports. These technologies provide an increased level of screening for passengers by detecting explosives and other non-metal objects that current checkpoint technologies are not capable of detecting. The Committee directs that funds for whole body imaging continue to be spent by TSA on multiple imaging technologies, including backscatter and millimeter wave.

4) H. Rep.110-259, at page 363, Conference Report to Implementing Recommendations of 9/11 Commission Act of 2007, Pub.L. 110-53, sec. 1601 - Airport checkpoint screening fund:

> The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) asserted that while more advanced screening technology is being developed, Congress should provide funding for, and TSA should move as expeditiously as possible to support, the installation of explosives detection trace portals or other applicable technologies at more of the nation's commercial airports. Advanced technologies, such as the use of non-intrusive imaging, have been evaluated by TSA over the last few years and have demonstrated that they can provide significant improvements in threat detection at airport passenger screening checkpoints for both carry-on baggage and the screening of passengers. The Conference urges TSA to deploy such technologies quickly and broadly to address security shortcomings at passenger screening checkpoints.

In addition, on January 7, 2010, the President issued a "Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack," which charged TSA with aggressively pursuing enhanced screening technology in order to prevent further such attempts.

As adversaries abandon traditional methods of attacking the aviation domain, their attempts grow more sophisticated and involve new means of disruption to aviation security. TSA recognizes the emerging threat of passenger-borne improvised explosive devices (IEDs) and the current trend of these devices transitioning from devices with metallic components to being composed completely of non-metallic components in order to subvert WTMDs. As the previously mentioned terrorist events demonstrate, the threat to aviation security is real and ever-evolving. Non-metallic weapons and explosives are now the foremost threat to commercial passenger aviation.

Section 44925 of the Intelligence Reform and Terrorism Prevention Act (IRTPA), Pub. L. 108-458, 118 Stat. 3638 (December 17, 2004) directs the Secretary of Homeland Security to give a high priority to developing and deploying at airport screening checkpoints equipment that detects non-metallic, chemical, biological, and radiological weapons and explosives that terrorists may try to smuggle on board an aircraft. This equipment addresses these new and evolving security threats to commercial aviation and the inability of WTMDs to detect non-metallic threats. To address the emerging threat of non-metallic weapons and explosives, TSA began an evaluation to determine the maturity and effectiveness of various technologies designed to detect non-metallic threats on passengers. After analyzing the latest intelligence and studying available technologies, TSA determined that the addition of AIT to its layered security approach provided the best opportunity to address the vulnerability of commercial aviation security to the evolving threat of non-metallic weapons and explosives.

In 2007, TSA initiated a pilot operation at several airports to test the detection capability of AIT on passengers who alarmed the WTMD. In 2008, TSA expanded its testing of AIT to additional airports, where AIT was used as the primary screening technology. The December 25, 2009 attempted bombing of Delta Flight 253, although ultimately unsuccessful, further highlighted the increasing need to deploy nationwide a technology or process capable of detecting non-metallic threats on the body. In addition, following that attempted attack, President Obama issued the "Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack," which charged TSA with aggressively pursuing enhanced screening technologies to prevent such attempts in the future, while at the same time protecting passenger privacy.[10] In the wake of the December 25, 2009 attempted aircraft bombing, TSA hastened to expand the deployment and use of AIT as the primary passenger screening technology.

[10] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack.

Market Failure

The threat of a terrorist attack against the aviation industry is real. Market failure, however, impedes the ability of private firms to provide the socially optimal level of security to prevent these attacks. Regulations are a tool used to correct market failure. In this case, due to the economics of externalities, the free market fails to provide adequate incentive for entities in the aviation industry to make socially optimal investments in security measures that reduce the probability of a successful terrorist attack.

Externalities are a cost or benefit from an economic transaction experienced by parties "external" to the transaction. In the case of commercial aviation, the consequences of an attack or other security incident may be significantly larger than what would be realized by an individual airport operator or commercial aircraft operator. Due to this fact, the private market does not provide the incentive for profit-maximizing firms to unilaterally spend the socially optimal amount of resources to prevent or mitigate a terrorist attack.

Because companies nevertheless likely suffer serious consequences in the case of a terrorist attack, many invest significant resources in implementing security measures. In a competitive marketplace, however, a firm has limited incentive to choose to make additional investments in security over their privately optimal amount. Making security investments above its privately optimal amount would increase a firm's cost of production and put the firm at a disadvantage against competitors who have not made similar investments.

Congress enacted the Aviation and Transportation Security Act (ATSA), Pub. L. 107-71, 115 Stat. 597 (November 19, 2001) to address the existing security measures, which proved to be inadequate to prevent the terrorist attack of September 11, 2001. This statute created TSA and gave TSA authority over security in all modes of transportation. ATSA also transferred responsibility for the screening of all passengers and property carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation from the private sector to the federal government and corrects the market failure that existed prior to the 9/11 terrorist attacks.

Need for Regulatory Action

In 2010, TSA was sued over its use of AIT by the Electronic Privacy Information Center (EPIC). In the decision rendered by the U.S. Court of Appeals for the District of Columbia Circuit in *Electronic Privacy Information Center v. U.S. Department of Homeland Security*,[11] the Court directed TSA to conduct notice and comment rulemaking on the use of AIT. However, in recognition of its efficacy in the detection of non-metallic threats, the Court also allowed TSA to continue using AIT as part of its airport security operations. TSA developed this NPRM to comply with the Court's decision. This NPRM will provide public notice and an opportunity to comment on TSA's use of AIT.

Equipment

AIT systems are screening devices with the capability to locate potential threats on a person, including those beneath clothing or otherwise obscured. The system displays an image of the passenger without obscuring items. TSA has introduced two different types of AIT to date. The first is the L3 Communications ProVision 100 AIT system (referred to throughout as the L3 units or machines). These systems bounce electromagnetic waves off the body; the reflection of these waves creates an image of the passenger that highlights anomalies. [12] The second system is the Rapiscan Secure 1000 Dual View AIT system (referred to throughout as the Rapiscan units, or machines). These systems scan passengers with low-energy x-ray beams at high speed. Rapiscan machines detect, digitalize, and display the reflection of the beam on a monitor for a TSO to examine for anomalies.

Initially, the images produced by the AIT were transmitted to an Image Operator (IO) stationed in a remote, windowless room unable to see the passenger being screened. The inability of both the AIT machines and the computers used by the IO to store the images provide an additional level of privacy protection. If the IO's interpretation of the image identifies a potential threat,

---

[11] 653 F.3d 1 (D.C. Cir. 2011).

[12]See "Safety of AIT" for a discussion of the safety of the millimeter wave equipment. The Food and Drug Administration has found that millimeter wave is safe and states on its website that "[m]illimeter wave security systems which comply with the limits set in the applicable national non-ionizing radiation safety standard . . . cause no known adverse health effects." http://www fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201 htm#2. For more information, visit http://www.tsa.gov/ait-how-it-works.

the IO verbally communicates the location of the anomaly via headset to the system operator (SO), who then conducts alarm resolution in accordance with standard operating procedures. TSA refers to these systems throughout as "AIT with IO."

Since then, software has been developed that both eliminates the need for the IO position and provides further privacy protection to passengers. This software, known as Automated Target Recognition (ATR), has the same capabilities as the AIT with IO; however, the AIT system with ATR (referred to throughout as "AIT with ATR") uses algorithms to analyze the same image analysis and determines the location of anomalies found during the scan of a passenger. A monitor attached to the AIT unit then displays a generic outline with highlights marking the location of any anomalies. This software allows the SO to examine the generic figure to locate any anomalies. There is no need for an IO when using AIT with ATR. If no anomalies are detected, the text "OK" appears on the monitor with no outline.

ATR software increases the passenger throughput rate of AIT while simultaneously decreasing the number of officers required to staff and operate the units. Moving forward, TSA plans to only purchase AIT systems that have ATR capability and remove those machines that do not have this capability. ATR development will also eliminate the need to construct remote viewing rooms used by the IO to view the images. ATR software was approved for use by TSA for the L3 units. In 2011, all L3 AIT machines were upgraded with the ATR software. All Rapiscan general-use backscatter units currently deployed at TSA checkpoints are being removed from operation by May 31, 2013.

Changes to the Screening Checkpoint

In order to deploy AIT, TSA made changes to checkpoint functions to include AIT. These changes modify checkpoint configurations and affect staffing levels as well as inform TSA how many AIT machines are necessary to reach full deployment. In addition, the information on checkpoint configurations illustrates how TSA continues to use WTMD alongside AIT.

Prior to AIT deployment, checkpoints consisted of lanes with WTMDs for passenger screening and x-ray machines to screen carry-on baggage. TSA initially deployed WTMDs in configurations, called modsets, of either a 1:1 or 2:2 configuration of x-ray machines to passenger screening technology. The difference between the two modsets implies that there will either be one x-ray and one WTMD or two x-rays and two WTMDs in a configuration. Before 2008, TSA began a checkpoint optimization program, in which TSA removed the second WTMD from 2:2 configurations in favor of a 2:1 configuration. The WTMD maintains a sufficient throughput to support two x-ray machines.

AIT with ATR provides sufficient throughput to handle that of one x-ray machine but not currently sufficient to handle that of two as discussed in the throughput discussion.[13] Therefore AIT has been deployed to date in modsets with two x-ray machines and a co-located WTMD, modsets with one x-ray machine and one co-located WTMD, and modsets with one x-ray machine and no co-located WTMD. Most AIT machines are co-located with a WTMD in a 2:2 configuration.

[13] For 1:1 modsets, TSA only locates an AIT with ATR in a modset with one x-ray machine and one AIT. TSA co-locates AIT with IO with WTMD and one x-ray machine to maintain current throughput levels.

CHAPTER 2: COST OF PROPOSED RULEMAKING

This section outlines TSA's estimates for the cost of AIT deployment. Cost elements include a utility cost to both airport operators and TSA, an opportunity cost for passengers opting out of AIT screening, a personnel cost, a training cost, and a life cycle cost of AIT.[14]

Methodology and Assumptions

The following sections outline the populations and other assumptions used in this analysis. This section presents estimates of the marginal cost of compliance to airport operators, the traveling public, and TSA for AIT screening. When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. As the AIT life cycle from deployment to disposal is eight years, the period of analysis for estimating the cost of AIT is eight years. However, as AIT deployment began in 2008, there are costs that have already been borne by TSA, the traveling public, and airport operators that were not due to this rule. Consequently, in the initial regulatory impact analysis for this proposed rule, TSA reports the AIT-related costs that have already occurred (years 2008-2011), while considering the additional cost of this rulemaking to be years 2012-2015. By reporting the costs that have already happened and estimating future costs in this manner, TSA considers the full eight year life cycle of AIT deployment.

TSA uses airport data to inform a number of its estimates, including data related to AIT deployment, checkpoint passenger throughput, and training for 2008 through 2011 of the analysis. TSA also relies on estimates from program office SMEs to project cost estimates incurred in the out years (2012 through 2015) of the analysis. TSA uses several assumptions related to industry size, growth, turnover, and labor costs throughout the regulatory evaluation. Lastly, TSA uses the Passenger Screening Program (PSP) costs to estimate the life cycle cost of AIT. TSA states all dollars in 2011 constant dollars. Using the Bureau of Economic Analysis

[14] TSA recognizes that some screening services are completed through TSA contracts. The contracted screening is identical to TSA-run screening and fully funded by TSA including staffing, equipment, training, and management at the airport. For the purposes of this evaluation, TSA does not differentiate between the contracted screening and TSA screening.

Gross Domestic Product (GDP) estimates, TSA inflates all historical figures to 2011 dollars, as shown in Table 10.[15]

Table 10: Inflation Index (Stated in 2011 Dollars)

Year	Inflation Index
2008	1.044
2009	1.035
2010	1.021
2011	1.000

Populations

TSA is responsible for screening checkpoints at 446 airports. These federalized airports are regulated under 49 CFR part 1542. TSA will use AITs for primary screening although WTMDs may be used for overflow, expedited screening, and certain other populations, such as crewmembers, passengers 12 years of age and under, and qualified individuals for TSA Pre✓™.[16] Table 11 shows the breakdown of part 1542-regulated airports into TSA's five categories.[17]

[15] In accordance with Circular A-4, TSA uses a GDP deflator to state all dollars in constant 2011 dollars. The GDP inputs are from the Bureau of Economic Analysis, Table 1.1.9 "Implicit Price Deflators for Gross Domestic Product" from the National Income and Product Accounts Table, found at http://www.bea.gov/iTable/iTable.cfm?ReqID=9&step=1

[16] TSA Pre✓™ allows select frequent flyers of participating airlines and members of U.S. Customs and Border Protection (CBP) Trusted Traveler programs who are flying on participating airlines, to receive expedited screening benefits during domestic travel. For more information on TSA Pre✓™, visit http://www.tsa.gov/tsa-pre%E2%9C%93%E2%84%A2.

[17] TSA categorizes federalized airports into groups as a measurement of passenger flow. Category X has the greatest number of passenger traffic and Category IV has the least.

Table 11: Number of Airports by Category

FAA Category	Number of Airports
X	28
I	57
II	79
III	127
IV	155
Total	**446**

Throughout the deployment of AIT, TSA has experienced changes in the acquisition of allowable technology type as well as the checkpoint strategy of how TSA plans to use AIT. The FAA Modernization and Reform Act of 2012 mandates that, beginning June 1, 2012, TSA "shall ensure that any advanced imaging technology used for the screening of passengers…is equipped with and employs [ATR]; and complies with such other requirements as the Assistant Secretary determines necessary to address privacy considerations" (sec. 828). The TSA Administrator issued an extension under subparagraph (A) of this act, whereby TSA has committed to meet this mandate by June 1, 2013.

All Rapiscan general-use backscatter units currently deployed at TSA checkpoints are being removed from operation by May 31, 2013. These units will not be disposed of but used in other government security functions. Due to security reasons, no Rapiscan machines will be made available to the public.

TSA determined that L3 units in some circumstances could be reallocated to replace the removed Rapiscan machines. The replacement of Rapiscan machines will be based on what equipment is needed to best address security at the airport using TSA's best estimate of the Pre ✓™ lanes expansion, checkpoint configuration and passenger volume at airports and at specific checkpoint lanes. If a Rapiscan unit was originally deployed in an underutilized or unnecessary placement in the airport, no L3 unit will replace the Rapiscan unit. L3 units in underutilized or unnecessary placements in an airport will be reallocated to replace a Rapiscan unit in a high need area. In order to backfill the removed Rapiscan units, TSA will need to reallocate 74 L3 units and reprioritize deployment of 60 already scheduled and purchased L3 machines in 2012 totaling 134 backfill L3 units. As a result, TSA projects the following changes:

- Removal of all 250 Rapiscan machines.
- Backfill of 134 Rapiscan machines with L3 units.

In addition to this policy change, the total deployment number could change as airports may expand or contract their operations or join or drop from the part 1542-regulated airports population due to changing economic conditions. Table 12 shows AIT deployment over the eight-year analysis period. The initial populations in 2008 through 2011 correspond to the numbers of AIT deployed from 2008 through 2011. Program office SMEs estimate the population of AIT deployment in 2012 through 2015. SMEs base these estimates on the current state of the acquisitions and procurement process along with the removal and backfill strategy outlined above.

Table 12: AIT Newly Deployed by Airport Category

(AIT Units)

Year	Category X	Category I	Category II	Category III	Category IV	Total
2008	16	14	0	0	0	**30**
2009	0	2	0	0	0	**2**
2010	301	135	20	2	0	**458**
2011	1	42	16	10	0	**69**
2012	179	59	68	83	34	**423**
2013*	0	0	0	0	0	**0**
2014	14	9	1	5	15	**44**
2015	15	10	1	2	17	**45**

*Estimates in 2013 reflect TSAs current deployment strategy based on the removal of Rapiscan units in 2013.

Because the decision to remove all Rapiscan machines from the airports affects the in-service units in 2013, TSA estimates a weighted average of in-service units and associated costs for year 2013. The weighted average assumes that from January 1st, 2013 to May 31st, 2013 all Rapiscan units are operational in the airports. From June 1st, 2013 to December 31st, 2013 TSA assumes that all Rapiscan machines are removed and all L3 units are reallocated to the new locations. Because TSA already removed 76 Rapiscan units in 2012, only the 174 units removed by Rapiscan will factor into the 2013 weighted average.[18] To estimate the weighted average, TSA estimates a cost of the Rapiscan units in the airport and a cost for after the removed Rapiscan machines. TSA weights the costs of the Rapiscan units by 5/12 to account for the five months

[18] All Rapiscan units will be removed from the Airports by May 31st, 2013 regardless of TSA removing the units or Rapiscan removing the units.

out of the year with Rapiscan units and weights the costs without the Rapiscan units by 7/12 to account for the remaining 7 months of the year. Appendix B outlines the assumptions and inputs necessary to estimate the weighted averages.

Throughput

TSA defines the passenger throughput rate as the number of passengers that a checkpoint configuration can process per hour. This time includes pat-downs and alarm resolutions of a given technology in the configuration. Current passenger throughput rates at TSA checkpoints average approximately 150 passengers per hour for modsets with one x-ray machine, and 300 passengers per hour in modsets with two x-ray machines. The WTMD can handle more passengers than AIT. However, the x-ray screening of carry-on baggage throughput constrains the overall screening process. AIT machines currently have a passenger throughput rate of approximately 115 per hour for AITs with IO, and 240 to 270 with AITs with ATR. Although a configuration with one AIT with IO and one x-ray machine would delay the passenger screening process, TSA never deploys that modset. A modset with one x-ray machine would either have one AIT with ATR or one AIT with IO and a WTMD. AIT with ATR maintains a higher throughput than the x-ray machine and therefore never constrains the screening environment.

Because both versions of AIT may not be able to handle throughput in a modset with two x-ray machines and one passenger screening mechanism by itself, TSA co-locates the AIT with a WTMD to maintain the current throughput rate of 300 passengers per hour. Therefore, the changes to the passenger screening process brought on by AIT do not affect the average time passengers move through a security check point.

An AIT with IO machine co-located with a WTMD and an AIT with ATR do not reduce total throughput per hour as x-ray baggage screening operates at lower throughput rates. Passengers experience no additional wait time because passengers wait for the x-ray screening of their personal belongings after they go through an AIT unit or a WTMD regardless of which screening technology is used.

Growth, Turnover, and Employment Costs

TSA uses historical data from its Performance Management Information System (PMIS) database to estimate the total passenger throughput at checkpoints for 2008 through 2011. To project this number for 2012 through 2015, TSA uses the FAA annual growth rate of 2.5 percent from the 2011 PMIS total as shown in Table 13.[19] To project training populations, TSA assumes a 9.0 percent attrition rate for TSOs.[20] TSA's Office of Human Capital estimates the separation rate from year 2011.

Table 13: Past and Estimated Passenger Throughput

Passenger Throughput	
2008	682,243,994
2009	626,962,827
2010	637,849,358
2011	638,274,548
2012	654,231,412
2013	670,587,197
2014	687,351,877
2015	704,535,674

The TSA Office of Finance and Administration estimates TSO personnel costs. TSA uses the historic fully-loaded FTE annual compensation rate for TSOs inflated to constant 2011 dollars. The annual compensation rate assumes the 2011 compensation rate for year 2012 to 2015. To

[19] FAA Aerospace Forecast FY 2012-2032. Page 68, Passenger Forecasts, http://www faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/2012%20FAA%20Aerospace%20Forecast.pdf

[20] The 9.0 percent attrition rate is based on the attrition rate in 2011 as estimated by TSA's Office of Human Capital.

arrive at a fully-loaded hourly compensation rate across the TSO population, TSA divides the annual FTE compensation by 2,080, the number of hours worked per year per employee. Table 14 shows the annual and hourly FTE assumptions used throughout the analysis.

Table 14: TSO FTE Annual and Hourly Compensation Rates[21]

Year	Historic FTE	Annual FTE in 2011$	Hourly FTE in 2011$
2008	$52,549.00	$54,861.16	$26.38
2009	$53,229.00	$55,092.02	$26.49
2010	$55,180.00	$56,338.78	$27.09
2011	$56,772.00	$56,772.00	$27.29
2012 – 2015	$56,772.00	$56,772.00	$27.29

Airport Utility Cost

Airport operators may incur costs for the additional utilities consumed by AIT machines. Likewise, TSA incurs incremental costs from certain airport operators who receive a utility cost reimbursement. Airport operator utility costs increase from the use of AIT, regardless of the modset. In cases where the AIT replaces WTMD, TSA subtracts the WTMD utility costs from the AIT utility costs. Table 15 breaks down the number of AIT units in-service by reimbursed airports and non-reimbursed airports.

[21] TSA rounds all FTE and wages rates to the nearest cent.

Table 15: AIT Units In-service by Reimbursed and Non-reimbursed Airports

Year	AIT Units In-service	AIT Units In-service at Reimbursed Airports	AIT Units In-service at Non-reimbursed Airports
2008	30	23	7
2009	32	25	7
2010	490	296	194
2011	559	330	229
2012	982	581	401
2013*	805	399	406
2014	776	391	385
2015	821	450	371

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

TSA estimates the incremental utility costs by multiplying the cost of kilowatt hours (kWh) consumed per unit by the number of units on an annual basis. TSA estimates an average cost per kWh at federalized airports at approximately $0.10 using data available from the U.S. Energy Information Administration.[22] Using this cost, TSA estimates a per-unit daily average cost of $2.23.[23] TSA estimates the utility costs by multiplying the number of units in operation by the

[22] TSA estimates this cost by taking the average of 2007-2011 retail electricity prices for the commercial sector as reported by the U.S. Energy Information Administration (http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_3).

[23] TSA calculates the per-unit utility cost per day as a weighted average of the power used to perform a scan and the power used while the system is idle. TSA assumes that the system will be operational for 16 hours (16 hours / 24 hours) of a day and idle for 8 hours (8 hours / 24 hours) of a day. TSA then estimates the weighted average of kW used per hour by taking the sum of the power consumption when the system is in operation (1.02) multiplied by the fraction of a day the system is in operation (16 hours / 24 hours) and the power consumption when the system is idle (0.70) multiplied by the percent of a day the system is idle (8 hours / 24 hours). This calculation results in an average kW used per hour of 0.9133 ((1.02 x (16/24)) + (0.70 x (8/24))). TSA then calculates the average kW used per day by multiplying the kW used per hour (0.9133) by 24 hours to obtain an average of

per-unit daily average and by the number of operating days. TSA estimates the airport utility costs from 2008-2011 as approximately $356,334 (undiscounted). From 2012-2015, TSA projects the airport utility costs to be approximately $1.3 million undiscounted, $1.2 million with three percent discounting, and $1.1 million with seven percent discounting. Table 16 reports prior year costs (2008-2011), while Table 16 shows the additional costs TSA attributes to this rulemaking (2012-2015).[24]

21.92 kWh per day (0.9133 x 24). TSA then multiplies this average number of kWh per day by the cost per kWh ($0.1019) to obtain a per-unit utility cost per day of $2.234 (21.92 x $0.1019). TSA uses $2.234 as the input for all per-unit unity cost for AIT. For WTMDs, TSA follows a similar formulation but assumes that the power consumption while operational and idle is 0.04 kW, with a per-day cost of $0.96 and a per unit cost of $0.098.

[24] For 2008, TSA estimates the annual utility cost to airports by multiplying the number of AITs deployed to non-reimbursed airports (7) by the per-unit daily average utility cost for AITs ($2.234) and by the number of days per year (365). This calculation results in a total utility cost to airports in 2008 for AIT deployment of $5,708 (7 x $2.234 x 365). TSA then estimates the utility cost savings to airports for WTMDs that would be removed in 2008 by multiplying the number of WTMDs removed (0) by the per-unit daily average utility cost for WTMDs ($0.10) and the number of days per year (365). This calculation results in a total utility cost savings to airports for WTMD removal of $0 (0 x $0.10 x 365) in 2008. TSA then calculates the total airport utility cost in 2008 of $5,708 by subtracting the utility cost savings from removal of WTMDs ($0) from the utility cost of AIT deployment ($5,708). TSA repeats this calculation for each year of the analysis period using the estimated numbers of AITs deployed and WTMDs removed for each year.

Table 16: Airport Utility Costs from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	**AITs at Non-reimbursed Airports**		**WTMDs at Non-reimbursed Airports**		
	AIT Units In-service a	**AIT Cost** b = a x $2.234 x 365	**Cumulative Removed (WTMD Units)** c	**WTMD Cost** d = c x $0.098 x 365	**Total Cost** e = b - d
2008	7	$5.7	0	$0.0	**$5.7**
2009	7	$5.7	0	$0.0	**$5.7**
2010	194	$158.2	0	$0.0	**$158.2**
2011	229	$186.7	0	$0.0	**$186.7**
Total	**437**	**$356.3**	**0**	**0**	**$356.3**

Table 17: Airport Utility Costs of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	AITs at Non-reimbursed Airports		WTMDs at Non-reimbursed Airports		Total Cost
	AIT Units In-service a	AIT Cost b = a x $2.234 x 365	Cumulative Removed (WTMD Units) c	WTMD Cost d = c x $0.098 x 365	Total Cost e = b - d
2012	401	$327.0	36	$1.3	**$325.7**
2013*	406	$331.1	49	$1.8	**$329.3**
2014	385	$313.9	55	$2.0	**$312.0**
2015	371	$302.5	62	$2.2	**$300.3**
Total	**1563**	**$1,274.5**	**202**	**$7.23**	**$1,267.3**
				3 % Discounting	$1,178.9
				7 % Discounting	$1,075.8

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Passenger Opportunity Cost

Passengers using AIT screening will not experience any increase in wait times as a result of this technology. Any passengers, however, may “opt out” of AIT screening and receive a pat-down by a TSO. These pat-downs can be conducted in the checkpoint area or in a private room. The small percentage of passengers opting out of AIT screening in favor of a pat-down experience increased wait times. TSA estimates the cost to these passengers by calculating the opportunity cost of a passenger’s time. Opportunity cost is a measure of the next best use of a resource, or, in this case, of a passenger’s time. The opportunity cost of a passenger’s time is a measure of the value of time that a passenger must forego from spending on other activities due to their increased time spent in a checkpoint area. Because a passenger's opportunity cost of time is valued based on what they must forego due to increased time in checkpoint areas, opportunity cost varies based on how the foregone time would have been spent (i.e., whether it is work or leisure time). The Department of Transportation's (DOT) Revised Departmental Guidance on Valuation of Travel Time in Economic Analysis estimated an average opportunity cost of a passenger's time of $43.57 per hour based on passenger incomes and purpose of travel (business or leisure).[25] TSA multiplies the opportunity cost of a passenger's time by the amount of time it takes for a pat-down to estimate the cost per passenger. TSA estimates that an additional pat-down costs $0.8726 for 80 seconds per passenger ($43.57 x 0.02 hours).[27]

TSA estimates the number of passengers receiving a pat-down from the historical number of individuals who opt out of AIT screening. From the PMIS, TSA estimates a 1.18 percent opt-out rate since 2009.[28] This percentage reflects the total number of passengers selected for AIT screening but who have opted out since 2009. TSA also uses PMIS data to obtain the total passenger throughput for 2008 through 2011. For years 2012 through 2015, TSA applies the FAA growth rate of 2.5 percent.[29] To estimate the passenger population that opts-out, TSA first estimates the AIT throughput of the total population and then multiplies that population by the 1.18 percent opt-out rate. TSA calculates the total opportunity cost of time by multiplying the total number of passengers assumed to opt out by the cost per pat-down (rounded to the nearest tenth decimal). TSA estimates the passenger opportunity cost from 2008-2011 as approximately $1.7 million (undiscounted). From 2012-2015, TSA projects the passenger opportunity cost to

---

[25] DOT estimates an hourly rate of $42.10 inflated to 2011 dollars to $43.57. http://ostpxweb.dot.gov/policy/reports/vot_guidance_092811c.pdf

[26] TSA uses $0.871 in the model for the input for passenger opportunity costs.

[27] TSA estimates 80 seconds for a pat-down based on field tests. The 80 second pat-down is equivalent to 0.0222 hours, TSA rounds this input to 0.02 hours.

[28] TSA observed a peak in opt-outs in 2009 (1.6 percent) but observed a steady decline with rates roughly 1 percent as of January 2013.

[29] FAA Aerospace Forecast FY 2012-2032. Page 68, Passenger Forecast, http://www faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/2012%20FAA%20Aerospace%20Forecast.pdf

be approximately $16.6 million undiscounted, $15.3 million with three percent discounting, and $13.8 million with seven percent discounting. Table 18 reports prior year costs (2008-2011), while Table 19 shows the additional costs TSA attributes to this rulemaking (2012-2015).[30]

Table 18: Passenger Opportunity Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	**Passengers** a	**AIT Throughput Percent of Total Passengers** B	**Number of Opt-Outs** c = a x b x 1.18%	**Total Cost for Opt-Outs** d = c x $0.871
2008	682,243,994	0.1%	8,050.5	$7.0
2009	626,962,827	0.5%	36,990.8	$32.2
2010	637,849,358	4.0%	301,064.9	$262.2
2011	638,274,548	21.1%	1,589,176.0	$1,384.2
Total	**2,585,330,727**		**1,935,282.2**	**$1,685.6**

[30] For 2008, TSA estimates the passenger opportunity cost by first multiplying the number of passengers (682,243,994) by the percent of AIT throughput for total passengers in 2008 (0.10%). This calculation results in a total AIT passenger throughput in 2008 of 682,244 (682,243,994 x 0.10%). TSA then multiplies the AIT passenger throughput in 2008 by the percent of passengers who opted out of AIT screening in 2008 (1.18%). This calculation results in a total number of opt-outs of 8,050.48 in 2008 (682,244 x 1.18%). To obtain the total passenger opportunity cost for opt-outs in 2008, TSA multiplies the number of opt-outs in 2008 (8,050.48) by the passenger opportunity cost per opt-out ($0.871) to obtain a total passenger opportunity cost of $7,012 (8,050.48 x $0.871) in 2008. TSA repeats this calculation for each year of the analysis period using the estimated numbers of passenger opt-outs for each year.

Table 19: Passenger Opportunity Cost of the Proposed Rule from 2012-2015

(Proposed AIT Costs in $ 1,000s)

Year	**Passengers** a[31]	**AIT Throughput Percent of Total Passengers[32]** b	**Number of Opt-Outs** c = a x b x 1.18%	**Total Cost for Opt-Outs** d = c x $0.871
2012	654,231,412	40.4%	3,118,852.0	$2,716.5
2013*	670,587,197	57.9%	4,582,904.7	$3,991.7
2014	687,351,877	60.0%	4,866,451.3	$4,238.7
2015	704,535,674	77.5%	6,442,978.7	$5,611.8
Total	**2,716,706,159**		**19,011,186.7**	**$16,558.7**
			3 % Discounting	$15,265.0
			7 % Discounting	$13,766.6

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

[31] TSA rounds the estimated passenger throughput to the third decimal point as inputs for the model.

[32] Although TSA removes Rapiscan AIT machines in 2013, the overall AIT passenger throughput is expected to continue to increase because of TSA's allocation strategy in 2013. This strategy involves relocating underutilized L3 AIT machines, which are capable of processing up to 240 - 270 passengers per hour as opposed to 115 passengers per hour with Rapiscan units, from lower volume airports to higher volume airports. Specific AIT throughput estimates are internal SSI data from TSA's Office of Security Capabilities.

Personnel Cost to TSA

TSA incurs a cost for additional personnel hired to operate AIT machines. TSA estimates this cost using assumptions from TSA's Screener Allocation Model (SAM) that dictates the allocation of personnel to each airport. The SAM estimates a personnel staffing level of 3.5 per lane for lanes with one WTMD. For lanes with a WTMD and an AIT with IO unit, the SAM estimates a 5.0 personnel staffing level. For lanes with a WTMD and an AIT with ATR unit, the SAM estimates a 4.5 personnel staffing level. Therefore, TSA estimates a personnel difference of 1.5 per lane for lanes with AIT with IO (5 – 3.5) and 1.0 per lane for those with AIT with ATR (4.5 – 3.5). The SAM also multiplies this difference by a factor of 3.5 to account for an estimated two shifts per lane per day, seven days of operation, the five day working schedule of a typical TSO, breaks, and any occurrences of sick or annual leave. To summarize, TSA estimates an additional 5.25 personnel (1.5 x 3.5) for each deployed AIT with IO unit and an additional 3.5 personnel (1.0 x 3.5) for each deployed AIT with ATR unit. TSA uses the fully loaded annual compensation rate for these employees estimated in Table 14. Table 20 demonstrates the relationship between AIT modsets and lanes (e.g., for every 1:1 modset is one lane and for every 2:1 modset is two lanes)

Table 20: AIT Modsets and Lanes

Year	AIT In-service Modsets		AIT Lanes In-service		AIT Lanes In-service[33] $e_t = e_{t-1} + c + d$
	1:1 a	2:1 b	1:1 c = a x 1	2:1 d = b x 2	
2008	9	21	9	42	51
2009	10	22	10	44	105
2010	143	347	143	694	942
2011	162	397	162	794	1,898
2012	286	696	286	1,392	3,576
2013*	213	570	213	1,141	4,930
2014	225	551	225	1,102	6,257
2015	240	581	240	1,162	7,659

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Table 21 and Table 22 present the cost incurred by TSA for the additional personnel necessary to operate and screen passengers with AIT machines. TSA estimates the number of personnel to maintain the AIT units in-service at full operating capacity, rounded to the nearest tenth decimal place. Because TSA estimates the total staffing level each year, the personnel populations account for any turnover in TSOs. TSA assumes that the TSO FTE includes training costs and therefore does not estimate the training cost for new hires separately in the section below. TSA estimates the cost of personnel from 2008-2011 as approximately $562.8 million (undiscounted).

---

[33] TSA estimates the lanes in-service by summing the current lane deployment and all prior year deployment.

From 2012-2015, TSA projects the cost of personnel to be approximately $1.2 billion undiscounted, $1.1 billion with three percent discounting, and $1.0 billion with seven percent discounting. Table 21 reports prior year costs (2008-2011), while Table 22 shows the additional costs TSA attributes to this rulemaking (2012-2015).

Table 21: Personnel Cost from 2008 – 2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	**Lanes In-service Covered by AIT**		**Personnel to Maintain Full Operating Capacity**		***Annual FTE***	**Total Cost**
	with IO *a*	***with ATR*** *b*	***AIT with IO*** *c = a x 5.25*	***AIT with ATR*** *d = b x 3.5*	*e*	***($1,000s)*** *f = (c + d) x e*
2008	51.0	0.0	267.8	0.0	$54,861	**$14,689.1**
2009	54.0	0.0	283.5	0.0	$55,092	**$15,618.6**
2010	837.0	0.0	4,394.3	0.0	$56,339	**$247,566.7**
2011	956.0	0.0	5,019.0	0.0	$56,772	**$284,938.7**
Total	**1,898.0**	**0.0**	**9,964.50**	**0.00**		**$562,813.0**

Table 22: Personnel Cost of the Proposed Rule from 2012 – 2015

(Proposed AIT Costs in $ 1,000s)

Year	Lanes In-service Covered by AIT[34]		Personnel to Maintain Full Operating Capacity		*Annual FTE*	Total Cost
	with IO *a*	*with ATR* *b*	*AIT with IO* *c = a x 5.25*	*AIT with ATR* *d = b x 3.5*	*e*	*($1,000s)* *f = (c + d) x e*
2012	427.2	1,250.8	2,242.80	4,377.84	$56,772	**$375,866.9**
2013*	119.8	1,233.7	628.91	4,317.98	$56,772	**$280,844.3**
2014	0.0	1,327.0	0.00	4,644.50	$56,772	**$263,677.6**
2015	0.0	1,402.0	0.00	4,907.00	$56,772	**$278,580.2**
Total	**547.0**	**5,213.5**	**2,871.7**	**18,247.31**		**$1,198,969.0**
					3 % Discounting	$1,118,459.3
					7 % Discounting	$1,024,344.7

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Training Cost to TSA

TSA incurs costs to train TSOs to operate and effectively screen passengers with AIT machines. TSOs take initial and recurring training on AIT operation and screening. Recurring training must be completed annually. Lastly, to account for TSA's shift from AIT with IO to AIT with

[34] TSA distributes the lanes between AIT with IO and AIT with ATR in 2012 based on the weighted average of the deployment of AIT type. Of the 982 AIT units deployed in 2012, 250 were AIT with IO and 732 were AIT with ATR. TSA estimates the lanes by technology type such that 25.46 percent (250/982) of the 1678 total lanes go to AIT with IO and 74.54 percent (732/982) of the 1678 lanes go to AIT with ATR. This results in 427.2 (25.46% x 1678) lanes with IO and 1250.8 (74.54% x 1678) lanes with ATR.

ATR, TSA estimates a transition training cost. The five components of training costs, along with their respective time requirements (shown in parentheses), are as follows:

- Initial AIT with IO training (20 hours)
- Recurring AIT with IO training (6 hours)
- Training to transfer from AIT with IO to AIT with ATR (at airports where AIT with IO was deployed prior to ATR development but later upgraded to ATR software) (14.23 hours[35])
- Initial AIT with ATR training (12 hours)
- Recurring AIT with ATR training (6 hours which includes recurring training for the SO position)

Detailed tables on the methodological procedures and calculations of personnel and the training populations are located in the Appendix. The tables below display the final training populations, for both initial and recurring, for both AIT technologies (L3 and Rapiscan).

[35] This estimate is based off the recorded training time of TSOs for two pilot programs conducting this type of training. 14 hours and 14 minutes was the average time spent by between the two programs (14.2333 hours). The AIT to L3 with ATR Differences Pilot courses were presented to a group of 51 participants from September 6th through September 7th, 2012 at both John F. Kennedy International Airport (JFK) and Los Angeles International Airport (LAX).

Table 23: L3 Training Population

	IO			ATR	
Year	Initial	Recurring[36]	IO to ATR	Initial	Recurring
2008	738.3	0.0	0.0	0.0	0.0
2009	166.2	0.0	0.0	0.0	0.0
2010	3,934.5	0.0	0.0	0.0	0.0
2011	5,650.3	0.0	9,142.0	14,837.3	0.0
2012	0.0	0.0	0.0	699.6	23,268.6
2013	0.0	0.0	0.0	2,156.4	21,811.1
2014	0.0	0.0	0.0	1,891.0	21,810.5
2015	0.0	0.0	0.0	1,870.6	21,568.4

[36] No historical recurring training for IO occurred in years 2008 to 2011.

Table 24: Rapiscan Training Population

	IO			ATR	
Year	Initial IO[37]	Recurring IO	IO to ATR	ATR Initial	Recurring with ATR
2008	0.0	0.0	0.0	0.0	0.0
2009	0.0	0.0	0.0	0.0	0.0
2010	5,908.2	0.0	0.0	0.0	0.0
2011	5,240.1	6,110.1	0.0	0.0	0.0
2012	1,021.5	10,328.7	14,816.4	0.0	0.0
2013	0.0	0.0	0.0	0.0	0.0
2014	0.0	0.0	0.0	0.0	0.0
2015	0.0	0.0	0.0	0.0	0.0

The following tables summarize the cost to training by the five components of training. To estimate the cost of training, TSA multiplies the assumed populations by the hourly wage rate and the corresponding hours of training. The following tables cover the five components of training. TSA uses the training populations in Tables 23 and 24 as inputs for the five training costs below.

---

[37] Although deployment for Rapiscan occurs only in 2010, the historic initial training for IO occurred over 2 calendar years. IO training in 2012 only includes initial training due to turnover.

Table 25: Initial AIT w/ IO Training Population and Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)[38]

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 20	d = a x c	e	f = e x 20	g = a x f	h = d + g
2008	$26.38	738.3	14,765.0	$389.5	0.0	0.0	$0.0	**$389.5**
2009	$26.49	166.2	3,323.1	$88.0	0	0.0	$0.0	**$88.0**
2010	$27.09	3,934.5	78,690.7	$2,131.7	5,908.20	118,164.0	$3,201.1	**$5,332.8**
2011	$27.29	5,650.3	113,006.0	$3,083.9	5,240.15	104,803.0	$2,860.1	**$5,944.0**
Total		**10,489.2**	**209,784.7**	**$5,693.2**	**11,148.3**	**222,967.0**	**$6,061.1**	**$11,754.3**

[38] For 2008, TSA estimates the initial training cost for AIT with IO by multiplying the estimated number of employees to be trained by the number of training hours per employee and average hourly compensation rate for a TSO. For the L3 technology in 2008, TSA multiplies the number of employees being trained (738.25) by the hours of training per employee (20) and by the average hourly compensation rate ($26.38) to obtain a total initial training cost of $389,501 (738.25 x 20 x $26.38). TSA repeats this calculation for Rapiscan technology to obtain a total initial training cost of $0 (0 x 20 x $26.38). TSA then sums these two costs to obtain a total training cost of $389,501 ($389,501+ $0) in 2008. TSA repeats this calculation for recurring costs for AIT with IO, and for both initial and recurring costs for AIT with ATR. TSA repeats these calculations for each year of analysis period, using the appropriate number of employees to be trained and annual compensation rates for each year.

Table 26: Initial AIT w/ IO Training Population and Cost of the Proposed Rule from 2012-2015

(Proposed AIT Costs in $ 1,000s)

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	Total
	a	b	c = b x 20	d = a x c	e	f = e x 20	g = a x f	h = d + g
2012	$27.29	0.0	0.0	$0.0	1,021.5	20,431.0	$557.6	**$557.6**
2013	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2014	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2015	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
Total		**0.0**	**0.0**	**$0.0**	**1,021.5**	**20,431.0**	**$557.6**	**$557.6**
							3 % Discounting	$541.3
							7 % Discounting	$521.1

Table 27: Recurring AIT w/ IO Training Population and Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	Hourly FTE	L3[39]			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	Total
	a	b	c = b x 6	d = a x c	e	f = e x 6	g = a x f	h = d + g
2008	$26.38	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2009	$26.49	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2010	$27.09	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2011	$27.29	0.0	0.0	$0.0	6,116.3	36,697.6	$1,001.5	**$1,001.5**
Total		**0.0**	**0.0**	**$0.0**	**6,116.3**	**36,697.6**	**$1,001.5**	**$1,001.5**

[39] TSA administered no historical L3 recurring training from 2008-2011.

Table 28: Recurring AIT w/ IO Training Population and Cost of the Proposed Rule from 2012-2015

(Proposed AIT Costs in $ 1,000s)

Year	Hourly FTE ($)	L3			Rapiscan			Total
		Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 6	d = a x c	e	f = e x 6	g = a x f	h = d + g
2012	$27.29	0.0	0.0	$0.0	10,328.7	61,971.9	$1,691.2	**$1,691.2**
2013	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2014	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2015	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
Total		**0.0**	**0.0**	**$0.0**	**10,328.7**	**61,971.9**	**$1,691.2**	**$1,691.2**
							3 % Discounting	$1,642.0
							7 % Discounting	$1,580.6

Table 29: IO Transition to ATR Training Population and Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 14.23[40]	d = a x c	e	f = e x 4	g = a x f	h = d + g
2008	$26.38	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2009	$26.49	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2010	$27.09	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2011	$27.29	9,142.0	130,121.1	$3,551.0	0.0	0.0	$0.0	**$3,551.0**
Total		**9,142.0**	**130,121.1**	**$3,551.0**	**0.0**	**0.0**	**$0.0**	**$3,551.0**

[40] TSA uses 14.2333 as the input for the estimation of IO transition to ATR training.

Table 30: IO Transition to ATR Training Population and Cost of the Proposed Rule from 2012-2015

(Proposed AIT Costs in $ 1,000s)

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 14.23[41]	d = a x c	e	f = e x 14	g = a x f	h = d + g
2012	$27.29	0.0	0.0	$0.0	14,816.4	210,886.8	$5,755.1	**$5,755.1**
2013	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2014	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2015	$27.29	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
Total		**0.0**	**0.0**	**$0.0**	**14,816.4**	**210,886.8**	**$5,755.1**	**$5,755.1**
							3 % Discounting	**$5,587.5**
							7 % Discounting	**$5,378.6**

[41] TSA uses 14.2333 as the input for the estimation of IO transition to ATR training.

Table 31: Initial AIT w/ ATR Training Population and Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 12	d = a x c	e	f = e x 12	g = a x f	h = d + g
2008	$26.38	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2009	$26.49	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2010	$27.09	0.0	0.0	$0.0	0.0	0.0	$0.0	**$0.0**
2011	$27.29	14,837.3	178,047.9	$4,858.9	0.0	0.0	$0.0	**$4,858.9**
Total		**14,837.3**	**178,047.9**	**$4,858.9**	**0.0**	**0.0**	**$0.0**	**$4,858.9**

Table 32: Initial AIT w/ ATR Training Population and Cost of the Proposed Rule from 2012-2015

(Proposed AIT Costs in $ 1,000s)

Year	Hourly FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Subtotal	
	a	b	c = b x 12	d = a x c	e	f = e x 12	g = a x f	h = d + g
2012	$27.29	699.6	8,395.2	$229.1	0.0	0.0	$0.0	**$229.1**
2013	$27.29	2,156.4	25,877.2	$706.2	0.0	0.0	$0.0	**$706.2**
2014	$27.29	1,891.0	22,692.4	$619.3	0.0	0.0	$0.0	**$619.3**
2015	$27.29	1,870.6	22,447.1	$612.6	0.0	0.0	$0.0	**$612.6**
Total		**6,617.7**	**79,412.0**	**$2,167.2**	**0.0**	**0.0**	**$0.0**	**$2,167.2**
							3 % Discounting	$1,999.1
							7 % Discounting	$1,803.8

Table 33: Recurring AIT w/ ATR Training Population and Cost from of the Proposed Rule 2012-2015

(AIT Costs in $ 1,000s)[42]

Year	FTE	L3			Rapiscan			Total
	($)	Employees	Hours	Subtotal	Employees	Hours	Sub-total	
	a	b	c = b x 6	d = a x c	e	f = e x 6	g = a x f	h = d + g
2012	$27.29	23,268.6	139,611.3	$3,810.0	0.0	0.0	$0.0	**$3,810.0**
2013	$27.29	21,811.1	130,866.4	$3,571.3	0.0	0.0	$0.0	**$3,571.3**
2014	$27.29	21,810.5	130,862.8	$3,571.2	0.0	0.0	$0.0	**$3,571.2**
2015	$27.29	21,568.4	129,410.4	$3,531.6	0.0	0.0	$0.0	**$3,531.6**
Total		**88,458.5**	**530,751.0**	**$14,484.2**	**0.0**	**0.0**	**$0.0**	**$14,484.2**
							3 % Discounting	$13,471.3
							7 % Discounting	$12,289.5

[42] Because ATR is introduced in 2011, TSA does not estimate any recurring training cost from 2008 to 2011.

TSA estimates the cost of training from 2008-2011 as approximately $21.2 million (undiscounted). From 2012-2015, TSA projects the cost of training to be approximately $24.7 million undiscounted, $23.2 million with three percent discounting, and $21.6 million with seven percent discounting. Table 34 reports prior year costs (2008-2011), while Table 35 shows the additional costs TSA attributes to this rulemaking (2012-2015).

Table 34: Training Cost from 2008-2011

(Costs already incurred in $ 1,000s - undiscounted)

Year	AIT with IO		IO to ATR	AIT with ATR		Total Cost
	Initial A	Recurring b	c	Initial d	Recurring e	f = a + b + c + d + e
2008	$389.5	$0.0	$0.0	$0.0	$0.0	**$389.5**
2009	$88.0	$0.0	$0.0	$0.0	$0.0	**$88.0**
2010	$5,332.8	$0.0	$0.0	$0.0	$0.0	**$5,332.8**
2011	$5,944.0	$1,000.5	$3,551.0	$4,858.9	$0.0	**$15,354.4**
Total	**$11,754.3**	**$1,000.5**	**$3,551.0**	**$4,858.9**	**$0.0**	**$21,164.7**

Table 35: Training Cost of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	AIT with IO		IO to ATR	AIT with ATR		Total Cost
	Initial a	Recurring b	c	Initial d	Recurring e	f = a + b + c + d + e
2012	$557.6	$1,691.2	$5,755.1	$229.1	$3,810.0	**$12,043.0**
2013	$0.0	$0.0	$0.0	$706.2	$3,571.3	**$4,277.5**
2014	$0.0	$0.0	$0.0	$619.3	$3,571.2	**$4,190.5**
2015	$0.0	$0.0	$0.0	$612.6	$3,531.6	**$4,144.2**
Total	**$557.6**	**$1,691.2**	**$5,755.1**	**$2,167.2**	**$14,484.2**	**$24,655.2**
Discounted 3%	$541.3	$1,642.0	$5,587.5	$1,999.1	$13,471.3	**$23,241.2**
Discounted 7%	$521.1	$1,580.6	$5,378.6	$1,803.8	$12,289.5	**$21,573.6**

AIT Life Cycle Cost to TSA

To estimate the life cycle cost of AIT, TSA divides the cost components into four high-level categories: acquisition, installation, and integration; maintenance; test and evaluation; and program management office (PMO) costs.

TSA's Office of Security Capabilities manages the PSP. The PSP includes several technologies, creating difficulties for estimating a life cycle cost of a single technology. Many of the costs to test, evaluate, maintain, and manage the technologies occur through private contracts covering the suite of technologies, which fosters economies of scale. Because these contracts cover several different technologies, the full contract cost cannot be easily allocated to one particular technology. TSA recognizes that new technologies would likely account for a larger than average share of the contract costs because newer technologies tend to have more complex and costly systems. In the following sections TSA allocates program-level life cycle costs to AIT.

TSA needs to make assumptions on the proportion of contract funds dedicated to AIT implementation. Under this methodology, TSA assumes that the acquisition cost of a technology directly correlates with other life cycle cost components. TSA derives AIT cost estimates from life cycle cost estimates as produced by TSA's Office of Security Capabilities.[43] TSA estimates that the acquisition cost of all AIT units relative to the acquisition costs of all units of the other technologies in TSA's PSP portfolio is approximately 40.5 percent.[44] Throughout this section, the 40.5 percent provides an approximate estimate of the AIT-specific costs when allocating the program level cost to AIT with no additional information.

TSA is removing all units that are not equipped with ATR from its checkpoints. TSA accounts for the removal of all 250 Rapiscan backscatter units by May 31, 2013. To ensure that these airports continue to screen passengers with AIT, TSA will reallocate 74 currently deployed units and reprioritize the deployment of 60 already scheduled L3 machines purchased in 2012.[45] These 134 L3 millimeter units will backfill the needs created by the removal of the Rapiscan machines. Throughout this section, the re-deployment of AIT and the removal of backscatter machines affect the cost elements based on the changes to deployment and the changes to the overall active units in the field.

---

[43] Internal document from TSA's Office of Security Capabilities (OSC), "Life Cycle Cost Estimate for Passenger Screening Program" As of June 22nd, 2012, Version 3.8. All estimates in the life cycle section reference this document unless otherwise noted.

[44] In the PSP program, TSA dedicates 40.5 percent of total acquisition costs to AIT in 2013 ($12,042,803 AIT acquisition cost / $29,745,848 total acquisition cost).

[45] TSA purchased these units but never deployed these units in 2012.

Reallocation

TSA accounts for the removal and reallocation of 74 previously deployed L3 AIT units with plans to reinstall them at other airports by May 31, 2013. Based on previous deployments, TSA estimates an average per-unit cost to reallocate an L3 AIT unit at $27,713, as shown in Table 36.[46] This cost includes:

- Systems integration;
- Removal, re-installment, shipping, rigging warehouse, other equipment relocation; and
- Ancillary equipment and infrastructure adjustments.

TSA multiplies the unit cost to allocate the units by the 74 units scheduled for reallocation. The reallocation costs TSA $2.1 million shown in Table 36 below. TSA does not include the costs to reprioritize the 60 L3 units acquired in 2012 in this estimate. In addition, the reallocation estimate does not include the cost to remove the 250 Rapiscan units. The Acquisition, Installation, Integration, Disposal, and Removal section includes these costs.

[46] TSA's Office of Security Capabilities provided the reallocation estimates based on an internal cost model for the reallocation plan.

Table 36: Reallocation Cost of L3 Units in 2013

(AIT Costs in $s)

Cost Category	Per-Unit Cost
Systems Integration Drawing Revisions	$2,500
Cost to Remove AIT	$8,000
Adjust WTMD and Install Security Glass	$1,050
Shipping	$2,200
Rigging Warehouse	$200
Cost to Reinstall	$7,500
Systems Integration Oversight	$3,300
Systems Integration Program Management	$1,520
Other Equipment Relocation at Install Airport	$763
Ancillary Equipment Adjustments	$500
Infrastructure Adjustments	$180
Per-unit Cost to Relocate and AIT	**$27,713**
Total Units Relocated	**74**
Total Cost for Reallocation	**$2,050,762**

Acquisition, Installation, Integration, Disposal, and Removal

TSA estimates acquisition, installation, integration, disposal, and removal costs using the newly deployed AIT technologies. To estimate the acquisition cost of new AIT units, TSA uses the current market prices for the L3 unit and the Rapiscan unit of $148,000 and $159,000, respectively. Based on current contract rates, TSA SMEs estimate the installation cost for the L3 and Rapiscan technology at $5,450 and $2,400, respectively. TSA SMEs estimates the integration cost at $30,000 per unit, regardless of the manufacturer.[47] The integration cost includes the cost of removing the existing technology from the airport but does not include the disposal cost. AIT deployment does not typically replace the current WTMD. Based on the eight-year life cycle of AIT, where the units newly deployed in 2008 will be replaced in 2015. TSA estimates a $550 per-unit disposal cost for the AIT units replaced in 2015.

Under unique circumstances, an AIT will completely replace the WTMD. An AIT will completely replace a WTMD when the surface area of the passenger lanes constrains the modset to one technology. TSA estimates that this configuration occurs in 2012 through 2015 with AIT replacing 56 WTMDs in 2012, 20 WTMDs in 2013, and 10 WTMDs in 2014 and 2015. TSA only includes the disposal cost of the WTMD when the deployment of AIT replaces the WTMD and thereby shortens the expected life cycle of the technology. TSA estimates the additional cost of a WTMD disposal at $550 per unit.[48] The PSP includes an annual Defense Logistics Agency (DLA) Disposition Service cost because this service directly coordinates disposal efforts and disposal is primarily only WTMDs, this cost is not included for AIT. The DLA Disposition Services existed before the onset of AIT and contributes to the optimization strategy of the WTMDs. Although AITs directly increase the number of WTMD disposal, the increased disposal does not affect the DLS Disposition Service functions. For additional clarity, Table 37 breaks down the specific disposal costs for each year, which are then shown as a cost component in Table 40.

[47] The cost of integration depends on the current configuration of the passenger screening environment; TSA uses the $30,000 estimate as a conservative cost estimate as most reconfigurations cost less than $30,000.

[48] TSA accounts for the removal of the WTMDs through the AIT integration cost; however the physical disposal is not captured in the integration cost.

Table 37: Disposal Cost of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)[49]

Year	**WTMD Replaced by AIT** **(WTMD Units)** a	**AIT End of Life Cycle** **(AIT Units)** b	**Total Replaced Units** c = a + b	**Total** d = c x $550
2012	56	0	56	$30.8
2013	20	0	20	$11.0
2014	10	0	10	$5.5
2015	10	30	40	$22.0
Total	**96**	**30**	**126**	**$69.3**
			3 % Discounting	$64.9
			7 % Discounting	$59.7

TSA plans to remove all 250 Rapiscan units by May 31, 2013. Both TSA and Rapiscan will pay for the removal costs. TSA removed 76 Rapiscan machines at the end of 2012 prior to the change in the policy to remove all Rapiscan units.[50] Rapiscan will pay for the removal for the remaining 174 units by May 31, 2013. TSA removed all 76 Rapiscan units from CAT X airports. [51]

[49] Disposal costs occur only in years 2012 through 2015.

[50] TSA originally followed a redeployment plan that moved L3 units with ATR and significantly higher throughput rate than Rapican units without ATR to airports with the highest volume of passenger traffic. The redeployment of Rapiscan units began when TSA anticipated that Rapiscan would deploy ATR units.

[51] The 76 units removed by TSA were in full active use for 2012 and were removed at the end of the year.

TSA assumes a per-unit cost of $10,400 to remove a Rapiscan machine.[52] TSA thus incurs a cost of $790,400 and Rapiscan incurs a cost of $1.8 million as shown in below.

Table 38: Onetime Rapiscan Removal Cost

(AIT costs in $1000s)

Year	Impacted Entity	Removed Rapiscan Units a	Cost per Rapiscan Unit b	Total Cost Removal Cost c = a x b
2012	TSA	76	$10.4	**$790.4**
2013	Rapiscan	174	$10.4	**$1,809.6**

TSA estimates the cost of acquisition, installation, integration, disposal and removal from 2008-2011 as approximately $104.5 million (undiscounted). From 2012-2015, TSA projects the cost of acquisition, installation, integration, disposal, and removal to be approximately $100.3 million undiscounted, $95.8 million with three percent discounting, and $90.3 million with seven percent discounting. Table 39 reports prior year costs (2008-2011), while Table 40 shows the additional costs TSA attributes to this rulemaking (2012-2015).[53] These tables do not include the cost to

[52] TSA bases the $10,400 removal cost on TSA's Office of Security Capabilities cost estimate assuming a $8,000 removal cost, a $2,200 shipping cost and a $200 warehouse rigging cost, as shown in Table 36 above.

[53] For 2008, TSA estimates the total acquisition, installation, integration, and disposal cost by calculating costs for each of these components and summing the results to obtain the total cost. TSA estimates the acquisition cost in 2008 by multiplying the number of units deployed by the per-unit cost for both the L3 and Rapiscan technologies. This calculation results in a total acquisition cost of $4,440,000 (30 x $148,000 (for L3 units)) + (0 x $159,000 (for Rapiscan units)) in 2008. TSA estimates the installation cost in 2008 with a similar calculation using the per-unit installation cost for each AIT unit. This calculation results in a total installation cost of $163,500 (30 x $5,450 (for L3 units))+ (0 x $2,400 (for Rapiscan units)) in 2008. TSA estimates the integration cost in 2008 with a similar calculation using the per-unit integration cost of $30,000 (identical for each AIT model). This calculation results in a total integration cost of $900,000 ((30 + 0) x $30,000) in 2008. TSA estimates the disposal cost in 2008 by multiplying the number of WTMDs to be disposed of in 2008 (0) by the per-unit disposal cost of $550. This calculation results in a total disposal cost for WTMDs of $0 (0 x $550) in 2008. TSA then sums these cost components for a total acquisition, installation, integration, and disposal cost of $5,503,500 ($4,440,000 + $163,500+ $900,000 + 0) in 2008. TSA repeats these calculations for each year of the analysis period using the appropriate number of deployment of AIT units and subsequent disposal of AIT and WTMD units.

Rapiscan to remove their AIT machines. TSA includes the total cost to Rapiscan in the final tables as a separate entity because TSA bears the remainder of the life cycle costs.

Table 39: TSA Acquisition, Installation, Integration, and Disposal Cost from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**L3 Deploy-Ment (AIT Units)** a	**Rapiscan Deploy-ment (AIT Units)** b	**L3 Delayed Deploy-ment (AIT Units)** c	**Acquisition Cost** d = a x $148,000 + b x $159,000	**Installation Cost** e = a x $5,450 + b x $2,400	**Integration Cost** f = (a + b) x $30,000	**Disposal Cost/ Removal** g = (disposed WTMD + AIT) x $550	**Total Cost** h = d + e + f + g
2008	30	0	0	$4,440.0	$163.5	$900.0	$0.0	$5,503.5
2009	2	0	0	$296.0	$10.9	$60.0	$0.0	$366.9
2010	208	250	0	$70,534.0	$1,733.6	$13,740.0	$0.0	$86,007.6
2011	69	0	0	$10,212.0	$376.1	$2,070.0	$0.0	$12,658.1
Total	**309**	**250**	**0**	**$85,482.0**	**$2,284.1**	**$16,770.0**	**$0.0**	**$104,536.1**

Table 40: TSA Acquisition, Installation, Integration, and Disposal Cost of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	**L3 Deploy-ment**[54] **(AIT Units)** a	**Rapiscan Deploy-ment (AIT Units)** b	**L3 Delayed Deploy-ment (AIT Units)** c	**Acquisition Cost** d = a x $148,000 + b x $159,000	**Installation Cost** e = a x $5,450 + b x $2,400	**Integration Cost** f = (a + b) x $30,000	**Disposal Cost/ Removal** [55] g = (disposed WTMD + AIT) x $550	**Total Cost** g = d + e + f + g
2012[56]	423	0	0	$62,604.0	$1,978.4	$10,890.0	$821.2	$76,293.6
2013[57]	0	0	60	$0.0	$327.0	$1,800.0	$11.0	$2,138.0
2014	44	0	0	$6,512.0	$239.8	$1,320.0	$5.5	$8,077.3
2015	75	0	0	$11,100.0	$408.8	$2,250.0	$22.0	$13,780.8
Total	**542**		**60**	**$80,216.0**	**$2,953.9**	**$16,260.0**	**$859.7**	**$100,289.6**
							3 % Discounting	$95,772.6
							7 % Discounting	$90,276.5

[54] The deployment in 2015 includes the 45 new AIT units and the 30 AIT units replacing the 2008 units.

[55] The disposal cost in 2015 includes 10 WTMDs plus the 30 AIT machines from 2008. TSA adds its one-time Rapiscan unit removal cost in 2012 of $790,400 to the disposal cost in 2012.

[56] The L3 units with delayed deployment were a part of the 423 L3 units in 2012. To allocate the life cycle cost, TSA assumes that the installation and integrations costs for the 60 units occur in 2013. In 2012, only 363 (423 – 60) units will be installed and integrated however, TSA acquired all 423 units in 2012.

[57] TSA assumes the L3 units with delayed deployment cost in 2013 only includes the installation and integration cost.

Maintenance

TSA estimates the maintenance cost of AIT services based on out-of-warranty maintenance, call center services, and general maintenance support services. The acquisition price of AIT includes a two-year warranty, thus maintenance costs occur between 2010 and 2015 for units acquired in 2008 through 2013. To estimate the maintenance costs based on contracts, TSA divides the maintenance contract total in 2013 by the number of units expected in the field.[58] This results in a per-unit cost of $15,642 per year. TSA multiplies the per-unit cost by the number of out-of-warranty AIT units in-service per year for each year of the analysis period.

Maintenance costs also include a ticketing call center and general maintenance support services.[59] The call center covers the maintenance requests, while the general maintenance support services manage all maintenance-related projects, including day-to-day logistics. TSA uses contractors to supply these services for the suite of PSP technologies. To allocate the cost to AIT, TSA scales the annual maintenance cost by the relative cost of maintenance for all other technologies, estimated at 19.3 percent in 2013.[60] TSA uses this percentage for all years of the analysis period. From this methodology, the call center costs $14,787,267 annually (19.3 percent x $76,617,964) while the general maintenance support services cost $5,762,579, annually (19.3 percent x $29,857,921).[61] TSA estimates the cost of maintenance, call centers, and support services from 2008-2011 as approximately $83.2 million (undiscounted). From 2012-2015, TSA projects the cost of maintenance, call centers, and support services to be approximately $117.6 million undiscounted, $109.0 million with three percent discounting, and $99.1 million with

---

[58] Siemens – HSTS04 – 09 – C – CT3173 contract supports the out-of-warranty maintenance with an estimated $15,642 per-unit cost.

[59] These services, as a part of the larger PSP, existed before and after the onset of AIT. TSA estimates a constant cost for these services each year since the contract remained unchanged by AIT and thus independent of the AIT units deployed.

[60] In the PSP program, TSA dedicates 19.3 percent of total maintenance costs to AIT in 2013 ($12,875,901 AIT maintenance cost / $66,638,785 total maintenance cost).

[61] Siemens – HSTS04 – 09 – C – CT3173 contract supports the call center; Logical Essence – HSTS04 – 09 – C – CT3101 and GST – Task Order 2 – HSTS04 – 10 – J – CT305 provide general support services.

seven percent discounting. Table 41 reports prior year costs (2008-2011), while Table 42 shows the additional costs TSA attributes to this rulemaking (2012-2015).[62]

Table 41: Maintenance Costs, Call Center, and Support Services from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**Units In-service** a	**Out-of-Warranty Maintenance** b = a x $15,642	**Call Center** c = $14,787,267	**Support Services** d = $5,762,579	**Total** e = b + c + d
2008	0	$0.0	$14,787.3	$5,762.6	$20,549.8
2009	0	$0.0	$14,787.3	$5,762.6	$20,549.8
2010	30	$469.3	$14,787.3	$5,762.6	$21,019.1
2011	32	$500.5	$14,787.3	$5,762.6	$21,050.4
Total	**62**	**$969.8**	**$59,149.1**	**$23,050.3**	**$83,169.2**

[62] For 2008, TSA estimates the total maintenance, call center, and support services costs by calculating the costs for each of these components and summing the results to obtain the total cost. TSA estimates the maintenance cost by multiplying the number of AIT units in-service by the per-unit maintenance cost of $15,642 to obtain a total maintenance cost of $0 (0 x $15,642) in 2008. TSA then adds to this maintenance cost the annual call center cost ($14,787,267) and annual support services cost ($5,762,579) to obtain a total maintenance, call center, and support services cost of $20,549,846 ($0 + $14,787,267 + $5,762,579) in 2008. TSA repeats these calculations for each year of the analysis period using the appropriate number of AIT units assumed to be out of warranty in each year.

Table 42: Maintenance Costs, Call Center, and Support Services of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	**Units In-service** a	**Out-of-Warranty Maintenance** b = a x $15,642	**Call Center** c = $14,787,267	**Support Services** d = $5,762,579	**Total** e = b + c + d
2012	490	$7,664.6	$14,787.3	$5,762.6	$28,214.4
2013	309	$4,833.4	$14,787.3	$5,762.6	$25,383.2
2014	732	$11,449.9	$14,787.3	$5,762.6	$31,999.8
2015	732	$11,449.9	$14,787.3	$5,762.6	$31,999.8
Total	**2,263**	**$35,397.8**	**$59,149.1**	**$23,050.3**	**$117,597.2**
				3 % Discounting	$109,034.5
				7 % Discounting	$99,073.2

Test and Evaluation

Before any new technology enters the field, TSA performs several stages of testing and evaluation. This section outlines these stages of testing and evaluation, from before procurement to final deployment.

In the initial stage, TSA performs qualification test and evaluation (QT&E). QT&E is a critical phase that evaluates a system's ability to meet the technical requirements specified by TSA and reflects the first test stage prior to procurement. QT&E occurs at two facilities, the Transportation Security Laboratory (TSL) and TSA Systems Integration Facility (TSIF). These two facilities perform testing independently on each technology. To estimate the cost for AIT testing, TSA scales the total cost of the facilities by the 40.5 percent acquisition price ratio developed earlier to estimate a cost of $5,896,778 for QT&E ($7,279,973 per facility x 2 facilities x 40.5 percent). QT&E occurs when TSA first considers a technology and in any subsequent upgrades of that technology, which TSA assumed to occur every two years.[63]

Next, TSA performs the operational test and evaluation (OT&E). This sequence of testing independently validates the extent to which candidate systems are operationally effective and suitable in the airport environment as well as safety testing for radiation emission. TSA estimates that, for each technology, 15 OT&Es will occur for a total cost of $613,905 ($40,927 per OT&E × 15 OT&Es per technology). Again, TSA assumes this cost occurs for each manufacturer initially and for subsequent upgrades every two years. In 2014, after the removal of the Rapiscan units, OT&E only occurs for the L3 technology.

The next two stages of testing consist of the factory acceptance test (FAT) and the site acceptance test (SAT). FATs are conducted at the Original Equipment Manufacturer (OEM) facility and SATs are conducted on-site at the airports. Both are conducted through TSA's Test & Evaluation Support Services contracts. A FAT and a SAT occur for each unit before initial deployment. Based on current TSA cost data, a FAT and a SAT cost $501and $864 per unit, respectively.[64] FATs and SATs occur for the 60 L3 units with delayed deployment, however the FAT occurs in 2012 and the SAT occurs in 2013. For the reallocated L3 units, TSA includes SAT costs in the reallocations costs under the Systems Integration costs in Table 36.[65]

TSA incurs program management costs (PMO) to run and facilitate the various stages of testing. Because TSA manages all technologies under this contract, TSA applies the 40.5 percent acquisition price ratio to the total cost of support services. PMO testing costs $1,383,095 annually (40.5 percent x $3,415,049). TSA estimates these costs separately from the general PSP PMO cost.

---

[63] To be conservative, TSA assumes the full QT&E cost for each upgrade. QT&E tends to be less extensive for subsequent upgrades compared to the full testing of the new technology.

[64] FAT and SAT costs are based on the Battelle HSTS04-05-D-DEP027 contract costs in 2009 inflated to 2011 dollars.

[65] FATs already occurred for these 60 AIT units when the units were originally deployed.

Finally, TSA uses a large contract that supports engineering services, changes, and initiatives. TSA accounts for the research and additional cost of upgrading the technology from AIT with IO to AIT with ATR and other subsequent research and development associated with the AIT platform. Again, this large contract covers the suite of technologies in the PSP. To allocate a portion of these costs to AIT, TSA scales the total cost by the 40.5 percent acquisition price ratio and estimates a cost of $18,802,859 million (40.5 percent x $46,426,811). This cost occurs in the years prior to testing.

TSA estimates the cost of testing and evaluation from 2008-2011 as approximately $55.4 million (undiscounted). From 2012-2015, TSA projects the cost of testing and evaluation to be approximately $54.7 million undiscounted, $50.6 million with three percent discounting, and $45.8 million with seven percent discounting. Table 43 reports prior year costs (2008-2011), while Table 44 shows the additional costs TSA attributes to this rulemaking (2012-2015).[66]

[66] For 2008, TSA estimates the testing and evaluation cost by calculating the costs for each of the components of testing and evaluation and summing the results to obtain the total cost. TSA estimates the QT&E cost at $5,896,778 in 2008. TSA estimates the OT&E cost by multiplying the OT&E cost for each technology ($613,905) by two to account for each technology, resulting in a total OT&E cost of $1,227,810 ($613,905 x 2) in 2008. TSA estimates the FAT/SAT cost by multiplying the number of AIT units deployed in 2008 (30) by the combined total FAT/SAT cost of $1,365 ($501 + $864), resulting in a total cost FAT/SAT cost of $40,950 (30 x $1,365) in 2008. TSA includes only engineering services ($18,802,859) in odd years, so engineering services cost is not incurred in 2008. TSA then sums the cost in 2008 for QT&E ($5,896,778), OT&E ($1,227,810), FAT/SAT ($40,950), and PMO ($1,383,095) to obtain a total cost for testing and evaluation of $8,548,633 in 2008. TSA repeats these calculations for each year of the analysis period using the appropriate number of AIT units and system upgrades in each year.

Table 43: Testing and Evaluation Cost from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**QT&E Cost** a = $5,896,778 (every 2 years)	**OT&E Cost** b = 2 x $613,905 (every 2 years)	**FAT/SAT Cost** c = AIT newly deployed x ($501+ $864)	**PMO Cost** d = $1,383,095 (every 2 years)	**Engineering Services Cost** e = $18,802,859 (every 2 years)	**Total Cost** f = a + b + c + d + e
2008	$5,896.8	$1,227.8	$41.0	$1,383.1	$0.0	$8,548.6
2009	$0.0	$0.0	$2.7	$0.0	$18,802.9	$18,805.6
2010	$5,896.8	$1,227.8	$625.2	$1,383.1	$0.0	$9,132.9
2011	$0.0	$0.0	$94.2	$0.0	$18,802.9	$18,897.0
Total	$11,793.6	$2,455.6	$763.0	$2,766.2	$37,605.7	$55,384.1

Table 44: Testing and Evaluation Cost of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	**QT&E Cost** a = $5,896,778 (every 2 years)	**OT&E Cost** b = 2 x $613,905 (every 2 years)	**FAT/SAT Cost** c = AIT newly deployed x ($501+ $864)[67]	**PMO Cost** d = $1,383,095 (every 2 years)	**Engineering Services Cost** e = $18,802,859 (every 2 years)	**Total Cost** f = a + b + c + d + e
2012	$5,896.8	$1,227.8	$525.6	$1,383.1	$0.0	$9,033.2
2013	$0.0	$0.0	$51.8	$0.0	$18,802.9	$18,854.7
2014	$5,896.8	$613.9	$60.1	$1,383.1	$0.0	$7,953.8
2015	$0.0	$0.0	$102.4	$0.0	$18,802.9	$18,905.2
Total	**$11,793.6**	**$1,841.7**	**$739.8**	**$2,766.2**	**$37,605.7**	**$54,747.0**
					3 % Discounting	$50,618.4
					7 % Discounting	$45,826.1

Program Management Office Cost

Several PMO costs occur to manage the PSP. PMO costs for the PSP include budget and financing, acquisition program documentation, deployment support, program support, testing and evaluation planning, communications support, executive support and other costs relating to managing the program. To run the PSP program, TSA provides internal PMO support and outside contractor support.[68] Because PMO support is less related to the cost of technologies and

[67] TSA assumes that the 2013 delayed deployment L3 units underwent FATs in 2012 and SATs in 2013. FATs occur before acquisition while SATs occur at deployment to the airport.

[68] Delloitte – HSTS04 – 08 – F – CT8600 contract supports the PSP program.

more related to the day-to-day support of the program, TSA is unable to directly allocate spending specifically to AIT. However, TSA estimates that 10 percent of the total PSP cost is dedicated to PMO. To indirectly account for these costs to AIT, TSA estimates a hypothetical PMO cost of 10 percent of the total cost of AIT. To estimate an annual PMO cost, TSA multiplies the total AIT cost by 10 percent and then divides the PMO cost evenly over the eight years ($515,723,196 x 10 percent / 8 years = $6,446,540).

TSA estimates the cost of PMO from 2008-2011 as approximately $25.8 million (undiscounted). From 2012-2015, TSA projects the cost of PMO to be approximately $25.8 million undiscounted, $24.0 million with three percent discounting, and $21.8 million with seven percent discounting. Table 45 reports prior year costs (2008-2011), while Table 46 shows the additional costs TSA attributes to this rulemaking (2012-2015).

Table 45: PMO Cost from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**AIT Cost** a_1	**PMO Cost** $b = \sum(a_{1+} a_2)$ x 10% / 8	**AIT Total Cost** c = a + b
2008	$34,602.0	$6,446.5	$41,048.5
2009	$39,722.3	$6,446.5	$46,168.9
2010	$116,159.6	$6,446.5	$122,606.1
2011	$52,605.5	$6,446.5	$59,052.0
Total	$243,089.4	$25,786.2	$268,875.5

Table 46: PMO Cost from of the Proposed Rule 2012-2015

(AIT Costs in $ 1,000s)

Year	**AIT Cost** a_2	**PMO Cost** $b = \sum(a_{1+} a_2) \times 10\% / 8$	**AIT Total Cost** $c = a + b$
2012	$113,541.2	$6,446.5	$119,987.8
2013	$46,375.9	$6,446.5	$52,822.5
2014	$48,030.9	$6,446.5	$54,477.5
2015	$64,685.8	$6,446.5	$71,132.3
Total	$272,633.8	$25,786.2	$298,420
	3 % Discounting	$23,962.4	$279,337.9
	7 % Discounting	$21,835.8	$257,011.6

Baseline Cost

To estimate the net cost of AIT, TSA accounts for the costs that would have occurred without the introduction of AIT. TSA estimates the total number of WTMDs that would be in operation independent of the deployment of AIT based on the screening environment prior to 2008 projected for 2008 through 2015. TSA subtracts these WTMD related costs from the total AIT costs, because these costs would have occurred even if AIT had not been deployed. For the baseline, TSA assumes that WTMD continues as the primary technology in the airport screening environment. To estimate the cost of using WTMD, TSA uses the cumulative total WTMD data for 2008 through 2011. Before AIT, TSA was undergoing an optimization plan for WTMD eliminating modsets using two WTMD and one personal item x-ray machine in favor of one WTMD and one personal item x-ray machine. For the baseline assumptions, TSA assumes this process would continue and optimization would be reached at 1,333 WTMD by 2014.[69] To project the number of WTMD in 2013, TSA assumes the midpoint of the known WTMD in 2012[70] and the optimization level of 1,333 in 2014. TSA assumes no acquisition, installation, or integration costs for the baseline because no new equipment would be purchased under the optimization strategy.[71] In addition, TSA assumes that no new testing and evaluation costs would be incurred under the baseline scenario. WTMD related costs subtracted from AIT costs include a maintenance cost and PMO cost. The process of estimating WTMD related costs parallels the methodology used for estimating the cost of AIT.

TSA assumes an annual maintenance cost of $721 per WTMD.[72] As with AIT, maintenance costs also include a ticketing call center and general maintenance support services. To allocate the cost to WTMDs, TSA scales the annual maintenance cost by the relative cost of maintenance to all other technologies. The WTMD maintenance cost comprises 1.7 percent of total maintenance costs in the PSP. Because WTMDs are the veteran technology, TSA assumes the cost to the call center and maintenance support services to be less than that of the new AIT. Multiplying the total contract cost by 1.7 percent, TSA estimates the cost of the call center to be $1,302,505 annually ($76,617,964 x 1.7 percent) and the general maintenance support services to be $507,585 annually ($29,857,921 x 1.7 percent).[73] TSA nets out these costs from the AIT total costs to only estimate the incremental cost of AIT over the baseline. For example, as discussed above, TSA assumes that 40.5 percent of these maintenance contracts are dedicated to AIT. However, without AIT, 1.7 percent of these contracts would cover the services for WTMD. By netting out these costs, TSA estimates the additional cost of AIT to the PSP.

[69] Although TSA estimates 821 total AIT units in the field in 2015, the reallocation strategy hinges on using WTMD for low utilization lanes, smaller airports and the Pre✓™ program included in the 1,333 estimate of WTMD.

[70] TSA uses known number of WTMDs in the field in 2012 up until May 2012.

[71] Based on the current fleet of WTMDs, TSA assumes the optimization strategy would target units nearing the end of their lifecycle and therefore does not consider an additional disposal cost for end of life cycle for WTMDs.

[72] Siemens – HSTS04 – 09 – C – CT3173 contract supports the out-of-warranty maintenance. Based on the contract TSA estimates the out-of-warranty maintenance cost at $721 per WTMD.

[73] Siemens – HSTS04 – 09 – C – CT3173 contract supports the call center; Logical Essence – HSTS04 – 09 – C – CT3101 and GST – Task Order 2 – HSTS04 – 10 – J – CT305 provide general support services.

As with AIT total costs, TSA assumes a level of PMO costs for WTMDs. As before, this cost reflects 10 percent of the total estimated costs distributed evenly over the eight-year analysis period, or $308,482 ($24,678,544 x 10 percent / 8 years). TSA estimates the baseline cost from 2008-2011 as approximately $14.2 million (undiscounted). From 2012-2015, TSA projects the baseline cost to be approximately $12.9 million undiscounted, $12.0 million with three percent discounting, and $11.0 million with seven percent discounting. Table 47 reports prior year costs (2008-2011), while Table 48 shows the additional costs TSA attributes to this rulemaking (2012-2015).[74] TSA subtracts this cost from the total AIT cost to obtain the estimated cost above the baseline.

[74] For 2008, TSA estimates the baseline cost by calculating the costs for maintenance, disposal, and PMO separately and then summing the results to obtain the total cost. TSA estimates the WTMD maintenance cost in 2008 by multiplying the cumulative number of WTMDs deployed (2,087) by the per-unit maintenance cost ($721) and adds to this cost the estimated call center cost ($1,302,505) and general maintenance cost ($507,585). This calculation results in a total maintenance cost of $3,314,817 ((2,087 x $721) + $1,302,505 + $507,585) in 2008. TSA estimates the PMO cost by multiplying the sum of maintenance costs by 10 percent, resulting in a total PMO cost of $308,482 ($24,678,544 x 10% / 8 years) in 2008. TSA then sums these cost components to obtain a total baseline cost of 3,623,299 ($3,314,817 + $308,482) in 2008. TSA repeats these calculations for each year of the analysis period using the appropriate number of WTMD units in each year.

Table 47: Cost of a WTMD Centered Screening Environment in the Absence of AIT from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**Baseline Cumulative WTMD** a	**Maintenance Cost** b = a x $721 + $1,302,505+ $507,585	**PMO Cost** c = ∑b x 10%/ 8 years	**Total Cost** d = b + c
2008	2,087	$3,314.8	$308.5	**$3,623.3**
2009	2,062	$3,296.8	$308.5	**$3,605.3**
2010	1,917	$3,192.2	$308.5	**$3,500.7**
2011	1,895	$3,176.4	$308.5	**$3,484.9**
Total	**1,895**	**$12,980.2**	**$1,233.9**	**$14,214.2**

Table 48: Cost of a WTMD Centered Screening Environment in the Absence of AIT for 2012-2015[75]

(WTMD Costs in $ 1,000s)

Year	**Baseline Cumulative WTMD** a	**Maintenance Cost** b = a x $721 + $1,302,505+ $507,585	**PMO Cost** c = ∑b x 10% / 8 years	**Total Cost** d = b + c
2012	1,900	$3,180.0	$308.5	**$3,488.5**
2013	1,617	$2,975.9	$308.5	**$3,284.4**
2014	1,333	$2,771.2	$308.5	**$3,079.7**
2015	1,333	$2,771.2	$308.5	**$3,079.7**
Total	**1,333**	**$11,698.3**	**$1,233.9**	**$12,932.2**
			3 % Discounting	$12,037.3
			7 % Discounting	$10,992.4

Total Life Cycle Costs

TSA estimates the life cycle costs of AIT accounting for the acquisition, installation, integration, maintenance, testing and evaluation, and PMO costs. To estimate the impact on society, TSA nets out the assumed baseline costs of WTMDs. TSA estimates the total life cycle cost from 2008-2011 as approximately $254.7 million (undiscounted). From 2012-2015, TSA projects the total life cycle cost to be approximately $287.6 million undiscounted, $267.4 million with three percent discounting, and $246.1 million with seven percent discounting. Table 49 reports prior

[75] This table reflects TSA's best estimate of the cost of the screening environment absent AIT from 2012 to 2015.

year costs (2008-2011), while Table 50 shows the additional costs TSA attributes to this rulemaking (2012-2015).[76]

Table 49: TSA Total Life Cycle Cost from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**Acquisition/ Installation/ Integration/ Disposal/ Removal Cost** a	**Maintenance Cost** b	**Testing and Evaluation Cost** c	**PMO Cost** d	**L3 Reallocation** e	**Baseline Cost** f	**Total Cost** f = a + b + c + d + e - f
2008	$5,503.5	$20,549.8	$8,548.6	$6,446.5	$0.0	$3,623.3	**$37,425.2**
2009	$366.9	$20,549.8	$18,805.6	$6,446.5	$0.0	$3,605.3	**$42,563.6**
2010	$86,007.6	$21,019.1	$9,132.9	$6,446.5	$0.0	$3,500.7	**$119,105.4**
2011	$12,658.1	$21,050.4	$18,897.0	$6,446.5	$0.0	$3,484.9	**$55,567.2**
Total	$104,536.1	$83,169.2	$55,384.1	$25,786.2	$0.0	$14,214.2	**$254,661.3**

[76] These totals do not reflect the cost to the Rapiscan Company to remove their technology, TSA includes these costs in the final summary tables.

Table 50: TSA Total Life Cycle Cost of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	**Acquisition/ Installation/ Integration/ Disposal/ Removal Cost**** a	**Maintenance Cost** b	**Testing and Evaluation Cost** c	**PMO Cost** d	**L3 Re-allocation** e	**Baseline Cost** f	**Total Cost** f = a + b + c + d + e - f
2012	$76,293.6	$28,214.4	$9,033.2	$6,446.5	$0.0	$3,488.5	**$116,499.3**
2013*	$2,138.0	$25,383.2	$18,854.7	$6,446.5	$2,050.8	$3,284.4	**$51,588.8**
2014	$8,077.3	$31,999.8	$7,953.8	$6,446.5	$0.0	$3,079.7	**$51,397.8**
2015	$13,780.8	$31,999.8	$18,905.2	$6,446.5	$0.0	$3,079.7	**$68,052.6**
Total	**$100,289.6**	**$117,597.2**	**$54,747.0**	**$25,786.2**	**$2,050.8**	**$12,932.2**	**$287,538.5**
3% Discounting	$95,722.6	$109,034.5	$50,618.4	$23,962.4	$1,933.0	$12,037.3	**$269,233.6**
7% Discounting	$90,276.5	$99,073.2	$45,826.1	$21,835.8	$1,791.2	$10,992.4	**$247,810.4**

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

** Removal cost for TSA includes 76 Rapiscan unit removals in 2012 by TSA.

TSA Utility Costs

As previously mentioned, TSA incurs an increase in the cost of utilities from the added power consumption of AIT machines at reimbursed airports. The methodology to estimate the increased utility costs parallels the methodology used for industry costs; the airport utilities section describes the derivation of the electricity cost. TSA estimates the TSA utility costs from 2008-2011 as approximately $549,600 (undiscounted). From 2012-2015, TSA projects the TSA utility costs to be approximately $1.5 million undiscounted, $1.4 million with three percent discounting, and $1.3 million with seven percent discounting. Table 51 reports prior year costs (2008-2011), while Table 52 shows the additional costs TSA attributes to this rulemaking (2012-2015).[77]

[77] TSA calculates the per-unit utility cost per day as a weighted average of the power used to perform a scan and the power used while the system is idle. TSA assumes that the system will be operational for 16 hours (16 hours / 24 hours) of a day and idle for 8 hours (8 hours / 24 hours) of a day. TSA then estimates the weighted average of kW used per hour by taking the sum of the power consumption when the system is in operation (1.02) multiplied by the fraction of a day the system is in operation (16 hours / 24 hours) and the power consumption when the system is idle (0.70) multiplied by the percent of a day the system is idle (8 hours / 24 hours). This calculation results in an average kW used per hour of 0.9133 ((1.02 x (16/24)) + (0.70 x (8/24))). TSA then calculates the average kW used per day by multiplying the kW used per hour (0.9133) by 24 hours to obtain an average of 21.92 kWh per day (0.9133 x 24). TSA then multiplies this average number of kWh per day by the cost per kWh ($0.1019) to obtain a per-unit utility cost per day of $2.234 (21.92 x $0.1019). TSA uses $2.234 as the input for all per-unit utility cost for AIT. For WTMDs, TSA follows a similar formulation but assumes that the power consumption while operational and idle is 0.04 kW, with a per-day cost of $0.96 and a per unit cost of $0.098.

Table 51: TSA Utility Costs from 2008-2011

(Costs already incurred in $ 1,000s – undiscounted)

Year	**AITs at Reimbursed Airports**		**WTMDs at Reimbursed Airports**		**Total Cost** e = b - d
	AIT Units In-service a	**AIT Cost** b = a x $2.234 x 365	**Removed WTMD Units (Cumulative)** c	**WTMD Cost** d = c x $0.098 x 365	
2008	23	$18.8	0	$0.0	**$18.8**
2009	25	$20.4	0	$0.0	**$20.4**
2010	296	$241.4	0	$0.0	**$241.4**
2011	330	$269.1	0	$0.0	**$269.1**
Total	**674**	**$549.6**	**0**	**$0.0**	**$549.6**

Table 52: TSA Utility Costs of the Proposed Rule from 2012-2015

(AIT Costs in $ 1,000s)

Year	AITs at Reimbursed Airports		WTMDs at Reimbursed Airports		Total Cost e = b - d
	AIT Units In-service a	AIT Cost b = a x $2.23 x 365	Removed WTMD Units (Cumulative) c	WTMD Cost d = c x $0.10 x 365	
2012	581	$473.8	20	$0.7	**$473.0**
2013*	399	$325.3	27	$1.0	**$324.4**
2014	391	$318.8	31	$1.1	**$317.7**
2015	450	$366.9	34	$1.2	**$365.7**
Total	**1821**	**$1,484.9**	**112**	**$4.0**	**$1,480.9**
				3% Discounting	$1,380.7
				7% Discounting	$1,263.8

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

Total Cost

TSA reports that the net cost of AIT deployment from 2008-2011 has been approximately $841.2 million (undiscounted) and that TSA has borne over 99 percent of installation and operational costs related to AIT deployment. TSA projects that from 2012-2015 total AIT-related costs will be approximately $1.5 billion (undiscounted), $1.4 billion at a three percent discount rate and $1.3 billion at a seven percent discount rate. During 2012-2015, TSA estimates it will also incur over 98 percent of AIT-related costs with equipment and personnel costs being the largest categories of costs. Table 53 below reports the costs that have already happened (2008-2011) by cost category, while Table 54 shows the additional costs TSA is attributing to this rulemaking (2012-2015).

Table 53: Net Cost Summary of AIT Deployment from 2008-2011 by Cost Component

(Costs already incurred in $ 1,000s - undiscounted)

Year	Passenger Opt-Outs	Industry Utilities	TSA Costs				Total
			Personnel	Training	Equipment	Utilities	
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$52,535.3
2009	$32.2	$5.7	$15,618.6	$88.0	$42,563.6	$20.4	$58,328.5
2010	$262.2	$158.2	$247,566.7	$5,332.8	$119,105.4	$241.4	$372,666.6
2011	$1,384.2	$186.7	$284,938.7	$15,354.4	$55,567.2	$269.1	$357,700.2
Total	**$1,685.6**	**$356.3**	**$562,813.0**	**$21,164.7**	**$254,661.3**	**$549.6**	**$841,230.6**

Table 54: Cost Summary of Proposed Rule (Net Cost of AIT Deployment 2012-2015) by Cost Component

(AIT Costs in $ 1,000s)

Year	Passenger Opt-Outs	Industry Utilities	TSA Costs				Rapiscan	Total
			Personnel	Training	Equipment **	Utilities	Removal	
2012	$2,716.5	$325.7	$375,866.9	$12,043.0	$116,499.3	$473.0	$0.0	$507,924.4
2013*	$3,991.7	$329.3	$280,844.3	$4,277.5	$51,588.8	$324.4	$1,809.6	$343,165.7
2014	$4,238.7	$312.0	$263,677.6	$4,190.5	$51,397.8	$317.7	$0.0	$324,134.2
2015	$5,611.8	$300.3	$278,580.2	$4,144.2	$68,052.6	$365.7	$0.0	$357,054.9
Total	**$16,558.7**	**$1,267.3**	**$1,198,969.0**	**$24,655.2**	**$287,538.5**	**$1,480.9**	**$1,809.6**	**$1,532,279.2**
Discounted 3%	$15,265.0	$1,178.9	$1,118,459.3	$23,810.2	$269,233.7	$1,380.7	$1,705.7	$1,431,033.5
Discounted 7%	$13,766.6	$1,075.8	$1,024,344.7	$22,048.8	$247,810.4	$1,263.8	$1,580.6	$1,311,890.7

*Estimates in 2013 reflect a weighted average based on the removal of Rapiscan units. See Appendix B.

**Equipment costs for TSA include acquisition, operation, maintenance, Rapiscan unit removal in 2012 by TSA and reallocation of AIT units.

Qualitative Impacts

This section describes qualitatively the potential impacts AIT has on privacy and health and the steps TSA has implemented to address any concerns passengers may have on both issues.

Privacy

TSA has addressed privacy concerns by removing all AIT machines without ATR from its checkpoints. As part of the Federal Aviation Administration Modernization and Reform Act of 2012, Congress mandated that all AIT units must be equipped with ATR by June 1, 2012.[78] As permitted by law, the deadline was extended to June 1, 2013. All of the millimeter wave units have been equipped with the ATR software. Rapiscan general-use backscatter units, without ATR, currently deployed at TSA checkpoints are being removed from operation by Rapiscan.[79] By June 1, 2013, only AIT equipped with ATR will be used at TSA checkpoints.

Machines equipped with ATR software create a generic outline that is displayed on a screen located on the AIT equipment and is viewable by the public. The software auto-detects anomalies concealed on the body that are then resolved through additional screening. The use of the ATR software enhances passenger privacy by eliminating the individual image as well as the need for a TSO to view the image for anomalies. ATR-enabled units deployed at airports are not capable of storing or printing the generic outline that will be visible to passengers (for additional discussion on AIT equipment and privacy safeguards see NPRM section III. *AIT Screening Protocols*). Examples of the generic outline that the ATR software produces are available on TSA's web site.[80] Even before the development of the ATR software, TSA instituted rigorous safeguards to protect the privacy of individuals who are screened using AIT. In addition, as noted by the Court in EPIC, the DHS Chief Privacy Officer has conducted several Privacy Impact Assessments (PIAs) on the use of AIT equipment to ensure that the public's privacy concerns related to AIT screening are adequately addressed. The PIA describes the strict measures TSA uses to protect privacy. The most recent update to the PIA is posted on the DHS website (http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf) is available in the docket for this rulemaking.

TSA's currently deployed AIT equipment do not produce photographs, nude or otherwise, nor do the units produce identifiable images of individuals that would enable personal

---

[78] P.L. 112-95

[79] http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract html.

[80] http://www.tsa.gov/ait-how-it-works

identification. To protect passenger privacy, for the backscatter AIT machines, TSA requirements dictate that a filter be applied that displays body contours and outlines, rather than a detailed image of a person's anatomy. Prior to the ATR upgrade on the millimeter wave AIT equipment, imaging software was required to blur the face on the resulting image. While more graphic images purportedly from the AIT machines have been circulated in the media, those images are not the type used by TSA's AIT equipment.

All images generated by an AIT unit without the ATR software are viewed by a trained TSO in a locked, remote location. The anonymity of the individual being screened is preserved, since the TSO assisting the individual at the AIT unit never views the image, and the TSO viewing the image never sees the individual being screened. No TSA personnel are permitted to view both the image and the individual. The two TSOs communicate using wireless headsets. If an anomaly is discovered on the image, TSA procedures require TSOs to use additional inspection methods to determine whether the anomaly is a threat. These methods may include visual inspection, and/or a pat-down to resolve the anomaly.

The AIT equipment that TSA deploys currently does not store, export, or print any images. Storage capability is disabled prior to deployment and TSA airport personnel are not able to activate the storage capability. In addition, the backscatter images are transmitted securely between the unit and the viewing room so they cannot be lost, modified, or disclosed. The images produced by the backscatter units are encrypted during transmission.[81] The images are deleted from the display in the viewing room when the individual is cleared. TSOs in the viewing room are prohibited from bringing electronic devices such as cameras, cell phones, or other recording devices into the room. Violations of these procedures subject the TSO to disciplinary action, which could include termination.

Finally, to give further effect to the Fair Information Practice Principles that are the foundation for privacy policy and implementation at DHS, individuals may opt-out of the AIT in favor of

---

[81] Prior to the ATR upgrade, images transmitted by the millimeter wave units were in a proprietary format that could only be viewed with proprietary equipment.

physical screening. TSA also provides notice of the use of AIT and the opt-out option at the checkpoint so that individuals may exercise an informed judgment on AIT.

TSA believes it has adequately addressed privacy concerns by removing all AIT machines without ATR from its checkpoint, adopting the use of ATR software in all its new machines and by providing an "opt-out" measure where the passenger can have a pat-down done by a TSO of the same gender. The additional time spent in the pat-down is captured in the Passenger Opportunity Cost Section of this Initial Regulatory Impact Analysis. TSA seeks comments on any aspect of privacy not addressed or any additional sources of information.

Health

AIT equipment has been subject to extensive testing that has confirmed that it is safe for individuals being screened, equipment operators, and bystanders. The exposure to ionizing x-ray beams emitted by the backscatter machines that are being removed pursuant to statue, as well as the non-ionizing electromagnetic waves from the millimeter wave machines is well within the limits allowed under relevant national health and safety standards. Prior to procuring and deploying both backscatter and millimeter wave AIT equipment, TSA tested the units to determine whether they would be safe for use in passenger screening. As explained below, TSA determined that the general-use backscatter and millimeter wave technologies were safe for use in screening the public because the x-ray and radio waves emissions were so low as to present a negligible risk to passengers, airline crew members, airport employees, and TSA employees (for discussion on AIT safety see NPRM section C *Safety of AIT*).

1. Millimeter Wave Units

The millimeter wave AIT systems that will be the only technology deployed at the checkpoint as of June 1, 2013 use nonionizing radio frequency energy in the millimeter wave spectrum to generate a three-dimensional image based on the energy reflected from the body. Millimeter wave imaging technology meets all known national and international health and safety standards. In fact, the energy emitted by millimeter wave technology is 1,000 times less than the international limits and guidelines. The millimeter wave AIT systems that TSA uses must comply with the 2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™-2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494-522, published April 1998. TSA's millimeter wave units are also consistent with Federal Communications Commission OET Bulletin 65, Health Canada Safety code 6, and RSS-102 Issue 3 for Canada. The FDA has also confirmed that millimeter wave security systems that comply with the IEEE Std. C95.1™-2005 cause no known adverse health effects.[82]

2. Backscatter Units

As required by statute, TSA will remove all currently deployed Rapiscan backscatter units by May 31, 2013. When in use, TSA addressed potential health concerns regarding the ionizing radiation emitted by general-use backscatter technology, TSA's procurement specifications required that the backscatter units must conform to American National Standards Institute/Health Physics Society (ANSI/HPS) N43.17, a consensus radiation safety standard approved by ANSI and HPS for the design and operation of security screening systems that use ionizing radiation .[83] The ANSI/HPS N43.17 standard was first published in 2002 and revised in 2009.[84] The annual dose limits in ANSI/HPS N43.17 are based on dose limit recommendations for the general public published by the National Council on Radiation Protection and Measurements in

---

[82] http://www fda.gov/Radiation-EmittingProducts/RadiationEmitting.ProductsandProcedures/SecuritySystems/ucm227201 htm.

[83] American National Standards Institute is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system. The Institute oversees the development and use of voluntary consensus standards by providing neutral, third-party accreditation of the procedures used by standards developing organizations, and approving their documents as American National Standards. Health Physics Society is a scientific organization of professionals who specialize in radiation safety. Its mission is to support its members and to promote excellence in the science and practice of radiation safety. As an independent nonprofit scientific organization, HPS is not affiliated with any government or industrial organization or private entity.

[84] American National Standard. "Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation," ANSI/HPS N43.17 (2009); Health Physics Society; McLean, VA. Copies can be ordered at: http://webstore.ansi.org/faq.aspx#resellers.

Report 116, "Limitations of Exposure to Ionizing Radiation."[85] The dose limits were set with consideration given to individuals, such as pregnant women, children and persons who receive radiation treatments, who may be more susceptible to radiation health effects. Further, the standard also takes into consideration the fact that individuals are continuously exposed to ionizing radiation from the environment. The ANSI/HPS N43.17 sets the maximum permissible dose of ionizing radiation from a general-use system per security screening at 0.25 microsieverts.[86] The standard also requires that individuals should not receive 250 microsieverts or more from a general-use x-ray security screening system in a year.

The radiation dose (effective dose) a passenger receives from a general-use backscatter AIT screening has been independently evaluated by the Food and Drug Administration's (FDA's) Center for Devices and Radiological Health, the National Institute for Standards and Technology, and the Johns Hopkins University Applied Physics Laboratory (JHU/APL). All results affirmed that the effective dose for individuals being screened, operators, and bystanders was well below the dose limits specified by ANSI.[87] These results were confirmed in a report issued by the DHS Office of Inspector General (OIG) in February 2012.[88] The OIG report found that the independent surveys show that backscatter radiation levels are below the established limits and that TSA complied with ANSI radiation safety requirements.

Typical doses from backscatter machines are no more than 0.05 microsieverts per screening, well below the ANSI/HPS N43.17 maximum dosage of 0.25 microsievert per screening. An

---

[85] The National Council on Radiation Protection and Measurements was founded in 1964 by Congress to cooperate with the International Commission on Radiological Protection, the Federal Radiation Council, the International Commission on Radiation Units and Measurements, and other national and international organizations, both governmental and private, concerned with radiation quantities, units, and measurements as well as radiation protection. The report is available at www ncrponline.org.

[86] The biological effect of radiation is measured in sieverts (Sv). One sievert equals 1,000 millisieverts and one millisievert equals 1,000 microsieverts.

[87] TSA's website at www.tsa.gov contains many articles and studies that discuss AIT safety, including a description of the built-in safety features of the Rapiscan Secure 1000, an Archives of Internal Medicine report on the risks of imaging technology, the FDA evaluation of backscatter technology, and other independent safety assessments of AIT.

[88] Department of Homeland Security, Office of Inspector General, "Transportation Security Administration's Use of Backscatter Units," OIG-12-38, February 2012.

individual would have to have been screened by the Rapiscan Secure 1000 more than 13 times daily for 365 consecutive days before exceeding the ANSI/HPS standard.

By comparison, a traveler would have to be screened 2,000 times to equal the dosage received in a single chest x-ray, which delivers 100 microsieverts of ionizing radiation. A typical bite-wing dental x-ray of 5 microsieverts would be equivalent to 100 screenings, and a two-view mammogram that delivers 360 microsieverts would be equivalent to 7,200 screenings.[89] A passenger on a one-way trip from New York to Los Angeles is exposed to approximately four microsieverts of ionizing radiation per hour of flight.[90]

ANSI/HPS also reflects the standard for a negligible individual dose of radiation established by the National Council on Radiation Protection and Measurements at 10 microsieverts per year. Efforts to reduce radiation exposure below the negligible individual dose are not warranted because the risks associated with that level of exposure are so small as to be indistinguishable from the risks attendant to environmental radiation that individuals are exposed to every day.[91] The level of radiation issued by the Rapiscan Secure 1000 is so low that most passengers would not have exceeded even the negligible individual dose. In fact, an individual would have to be screened more than 200 times a year by a Rapiscan Secure 1000 before they would exceed the negligible individual dose and, even then, would be below the ANSI/HPS N43.17 standard.

The European Commission released a report conducted by the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) on the risks related to the use of security scanners for passenger screening that use ionizing radiation such as the general-use backscatter AIT machines.[92] The committee found no short term health effects that can result from the doses of radiation delivered by security scanners. In the long term, it found that the

---

[89] HPS Fact Sheet: Radiation Exposure from Medical Exams and Procedures, January 2010, http://www hps.org/documents/Medical_Exposures_Fact_Sheet.pdf.

[90] http://www radiationanswers.org/radiation-sources-uses/natural-radiation.html.

[91] The World Health Organization estimates that each person is exposed, on average, to 2.4 millisieverts (i.e., 2400 microsieverts) of ionizing radiation each year from natural sources. www.who.int/ionizing_radiation/about/what_is_ir/en/index2 html.

[92] The SCENIHR is an independent committee that provides the European Commission with the scientific advice it needs when preparing policy and proposals relating to consumer safety, public health and the environment. The committee is made up of external experts. The report can be found at http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf

potential cancer risk cannot be estimated, but is likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources, and background risk due to other factors.

The ANSI/HPS N43.17 standard also requires that any general-use backscatter machine have safety interlocks to terminate emission of x-rays in the event of any system problem that could result in abnormal or unintended radiation emission. The Rapiscan Secure 1000 had three such features.[93] First, the unit was designed to cease x-ray emission once the programmed scan motion ends. That feature could not be adjusted. Second, the unit was programmed to terminate emission once the requisite number of lines of data necessary to create an image was received. Both of these automatic features reduced the possibility that emissions could continue if the unit malfunctions. Finally, the unit had an emergency stop button that would terminate x-ray emission.

Upon installation, a radiation emission survey was conducted on each Rapiscan Secure 1000 to ensure the unit operated properly. Preventive maintenance checks, including radiation safety surveys, were performed at least once every six months and after any maintenance that affected the radiation shielding, shutter mechanism, or x-ray production components, after any incident where damage was suspected, or after a unit was moved. The U.S. Army Public Health Command also conducted an independent radiation survey on deployed systems. The report confirmed that the general-use backscatter units tested were well within applicable national safety standards.[94]

The DHS Office of the Chief Procurement Officer is also requesting the National Academy of Sciences to convene a committee to review previous studies as well as current processes used by DHS and equipment manufacturers to estimate radiation exposure resulting from backscatter x-ray advanced imaging technology (AIT) systems used in screening air travelers and provide a report with findings and recommendations on: (1) whether exposures comply with applicable health and safety standards for public and occupational exposures to ionizing radiation, and (2)

---

[93] TSA's website contains a link to Rapiscan's safety features.

[94] The report is available on TSA's web site at http://www.tsa.gov/research/reading/xray_screening_technology_safety_reports.shtm.

whether system design (e.g., safety interlocks), operating procedures, and maintenance procedures are appropriate to prevent over exposures of travelers and operators to ionizing radiation. This study will not address legal, cultural, or privacy implications of this technology.

TSA does not include economic costs to the public associated with the use of the AIT machines because radiation exposure and doses received from ionizing and non-ionizing rays are negligible and do not attribute any significant risk as a result of their use in screening. In addition, while the radiation risk from X-ray screening is extremely low, passengers may choose to opt out of AIT screening and receive a pat down. TSA seeks comments on any aspect of health not addressed or any additional sources of information.

CHAPTER 3: ANALYSIS OF ALTERNATIVES

OMB Circular A-4 requires TSA to consider regulatory alternatives to the provisions of the NPRM. The subsequent sections qualitatively analyze the costs of each alternative, and it also discusses the rationale for rejecting alternatives in favor of the proposed provision.

Consideration of Regulatory Alternatives

In order to mitigate a vulnerability of existing aviation security, TSA sought to identify a means to detect non-metallic items concealed underneath the clothing of passengers traveling on commercial aircrafts. Through risk analysis, laboratory testing, and field testing, TSA identified several solutions capable of detecting non-metallic items. Although numerous technologies and processes were examined by TSA as potential solutions, only the top four alternatives are presented in this analysis. In Table 55, TSA presents the requirements of each alternative.

Table 55: Descriptive Summary of Regulatory Alternatives

Regulatory Alternative	Name	Description
1	No Action	Under this alternative, the passenger screening environment remains the same as it was prior to 2008. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.
2	Pat-Down	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting a pat-down on a randomly selected portion of passengers after screening by a WTMD.
3	ETD Screening	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.
4	AIT (NPRM)	Under this alternative, the proposed alternative, TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down.

Regulatory Alternative 1 – No Action

Under this alternative, TSA imposes no change to the passenger screening environment pre-2008. TSA continues to use WTMDs as the primary passenger screening technology and resolves alarms with a pat-down. WTMDs do not screen passengers specifically for non-metallic items under this alternative. While a pat-down may detect a non-metallic threat, this alternative uses a pat-down to resolve an alarm triggered by metallic objects.

Recent events highlight the need for a technology or process capable of detecting non-metallic threats concealed on passengers. In addition, this alternative fails to meet the instruction provided in the Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack, issued January 7, 2010.[95] While this alternative imposes no additional cost burden, it falls short in addressing or mitigating the threat to aviation security posed by non-metallic explosives and weapons. For this reason, TSA rejected this alternative in favor of deploying AIT to screening checkpoints.

Regulatory Alternative 2 – Pat-Down

Under this regulatory alternative, TSA continues to use the WTMD as the primary passenger screening technology and supplements WTMD screening with a pat-down. In this alternative, TSA would conduct a pat-down on a high volume of randomly selected passengers. This pat-down consists of a thorough physical inspection capable of detecting metallic and non-metallic items concealed under passengers' clothing undetected by the WTMD. Pat-downs have long been one of the many security measures TSA and other nations' transportation security agencies use to help detect hidden and dangerous items. Performing pat-downs on a high volume of randomly selected passengers address the threat of metallic and non-metallic weapons and explosives for a random sample of passengers; however, this strategy employs a substantial amount of resources with human capital and their respective ancillary costs to meet the security standard and throughput rate of AIT.

The main advantage of this alternative involves the use of currently deployed WTMD technology. This alternative imposes minimal technology acquisition costs to TSA. Although TSA still needs to replace WTMDs after their useful life, this alternative avoids the resource cost to test and evaluate a new technology, the upfront cost of acquiring a new technology, and the cost to deploy and integrate the new technology into checkpoints.

[95] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack

The main disadvantage of this alternative is that it does not screen passengers with the same level of security as an environment with AIT because not every passenger would receive a pat-down, thereby reducing the overall capability to detect non-metallic threats.

The second main disadvantage with this alternative is the length of time required to perform a pat-down. Based on field tests, the pat-down procedure takes, on average, 80 seconds to perform. Therefore, performing pat-downs on a significant number of passengers necessitates a substantial increase in staffing levels to maintain the current passenger throughput level (approximately 150 passengers per hour per lane). Without a staffing increase, passenger wait times and the associated opportunity cost increases. In addition increased queue times may create a risk to security as increased traffic throughput may be more difficult to control.

Additionally, as AIT represents a machine-based methodology, a screening environment centered on AIT provides a more consistent outcome over time. Further, TSA anticipates future advancements to AIT in detection capability, throughput, and privacy protection. Due to the reasons outlined above, TSA opted to reject implementing a random pat-down on a high volume of passengers to supplement WTMD screening for non-metallic explosives and weapons.

Regulatory Alternative 3 – Explosives Trace Detection Screening

Under this regulatory alternative, TSA continues to use the WTMD as the primary passenger screening technology and performs an ETD screening on a randomly selected population of passengers after WTMD screening. ETD screening involves swabbing a surface or individual and then testing the swab for traces of explosives. Additional ETD screening was found to somewhat address the threat of non-metallic explosives, but did not provide the same level of security as AIT due to the ETD being limited to explosives detection and not other non-metallic anomalies.

There are a number of disadvantages to this alternative. Although ETDs would help reduce the risk of non-metallic explosives being taken through the checkpoint, ETDs cannot detect other dangerous items such as weapons and IED components made of ceramics or plastics, whereas AIT is capable of detecting any anomaly concealed under clothing.

Second, incorporating ETD screening into the current checkpoint screening process can negatively impact the passenger's screening experience. Based on field tests, an ETD screening—from swab to test results—takes approximately 20-30 seconds. This would slow passenger throughput to levels below the current rate of 150 passengers per hour per lane, thereby increasing passenger wait times and the associated opportunity cost.

Third, while mechanical issues with ETDs are rare, throughput depends on the reliability and mechanical consistency of these machines. In the rare instance where an ETD may experience a mechanical issue, throughput may slow down for an extended period of time. Additionally, false alarms can and do occur from some innocuous products that may contain trace amounts of chemicals found in explosive materials, which may also impede throughput until the alarm is resolved.

Finally, this alternative requires an increase in ETD consumables, including swabs and gloves. This imposes a significant cost to keep sufficient amounts of these consumables in stock at all airports where TSA conducts screening.

The logistical concerns of implementing this alternative, in addition to the limited capability of ETD screening to detect other non-explosive threats, are the reasons TSA rejected this alternative in favor of deploying AIT to mitigate the threat to aviation security posed by both metallic and non-metallic weapons and explosives.

Regulatory Alternative 4 – Advanced Imaging Technology (NPRM)

The deployment and use of AIT as a means of screening passengers is the preferred alternative. TSA began deploying AIT machines to screening checkpoints in 2008. Currently, WTMDs and AIT machines are deployed as passenger screening technologies. Of these, only AIT is capable of detecting both metallic and non-metallic threats.

AIT safely screens passengers for metallic and non-metallic threats, including weapons, explosives, and other prohibited objects concealed under layers of clothing, without physical contact. AIT not only enhances security, it reduces the need for a pat-down among individuals with medical implants such as a pacemaker or a metal knee replacement. Based on field tests, a passenger can be screened by an AIT machine in 12 seconds, as opposed to the 80 seconds needed for a pat-down. AIT screening, however, is optional for all passengers. Passengers who opt out of AIT screening receive alternative screening, including a thorough pat-down to ensure an equivalent level of security.

AIT has a number of advantages over the other alternatives. AIT maintains a lower personnel cost and a higher passenger throughput rate than either the random pat-down of a high volume of passengers or ETD screening of people (Alternatives 2 and 3). ATR software development shifts anomaly detection from human image interpretation to an automated system. AIT systems with ATR alleviate passenger privacy concerns by eliminating observation of an individual's image. Further, the ATR software platform is upgradable, which leaves opportunity for future advancement towards faster processing times and enhanced aviation security.

The disadvantages of AIT include the cost and complexity of testing and evaluating a new technology, acquiring the technology, and integrating the technology into checkpoint configurations and standard operating procedures. In addition, AIT screening has resulted in an increase in staffing over baseline (Alternative 1) levels, and costs to train TSOs to operate AIT exceed what would have been imposed on TSA under some of the other alternatives considered.

Lastly, there exists potential for negative public perception of the health impacts from the use of backscatter AIT machines. Backscatter technology has been independently evaluated by the Food and Drug Administration's (FDA) Center for Devices and Radiological Health (CDRH), the National Institute for Standards and Technology (NIST), and the Johns Hopkins University Applied Physics Laboratory (APL), and all results confirm that the radiation doses for the individuals being screened, operators, and bystanders are well below the dose limits specified by the American National Standards Institute.[96] While TSA ensures the impact of backscatter and millimeter wave technologies are within industry standards, it may not be accepted by a portion of the flying public, increasing passenger opportunity costs as a result of opting out of the AIT

---

[96] ANSI/HPS N43.17 – 2002, American National Standard Radiation Safety for Personnel Screening Systems Using X-rays, ANSI/HPS N43.17 – 2009 Final for Publication, American National Standard Radiation Safety for Personnel Screening Systems Using X-ray or Gamma Radiation, 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])

screening in favor of a pat-down. TSA's Performance Management Information System (PMIS) reports that the opt-out rate peaked in December of 2010 at 1.6 percent but steadily declined to 0.9 percent as of January 2013.

After weighing the advantages and disadvantages of each alternative, TSA elected to deploy AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats. TSA requests public comment on all of the alternatives considered, as well as any additional alternatives that TSA does not include here but should consider in the future.

CHAPTER 4: BENEFITS OF PROPOSED RULEMAKING

The background section (Chapter 1) of this document and the NPRM preamble present a thorough discussion of the need for and the qualitative benefits of the AIT technology. The following section summarizes the benefits of the deployment of AIT as explained in the NPRM.

How This Regulation Increases Security

AIT is the most effective technology available to detect non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security.[97] Since TSA began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the walk-through metal detector. Specifically, since January, 2010, this technology has helped TSA officers detect hundreds of prohibited, dangerous, or illegal items concealed on passengers.[98] TSA's procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of anomalies concealed under an individual's clothing. While the detection requirements of AIT are classified, the procurement specifications require that any approved system be sensitive enough to detect small items.

Experience has confirmed that AIT will detect metallic and non-metallic items, including material that could be in various forms concealed under an individual's clothing. Instances of non-metallic items found using AIT have been discussed on TSA's blog.[99] A non-metallic martial arts weapon called a "Tactical Spike" was discovered in the sock of a passenger in Pensacola, Florida after being screened by AIT.[100] AIT has proven to be very effective at

---

[97] TSA bases this claim on comparative analysis conducted by TSA's Office of Security Capabilities in lab and field tests on AIT and alternative methods.

[98] Remarks of TSA Administrator John S. Pistole, Homeland Security Policy Institute, George Washington University, November 10, 2011.

[99] Http://blog.tsa.gov.

[100] "TSA Week In Review: Non Metallic Martial Arts Weapon Found with Body Scanner," http://blog.tsa.gov/2011/12/tsa-week-in-review-non-metallic-martial.html.

detecting objects intentionally hidden by passengers, which could pose a threat. Some of the items discovered concealed on passengers during AIT screening are small items, such as weapons made of composite, non-metallic materials, including a three inch pocket knife hidden on a passenger's back; little packets of powder, including a packet the size of a thumbprint; and a syringe full of liquid hidden in a passenger's underwear.[101] A plastic dagger hidden in the hemline of a passenger's shirt was detected using AIT[102] and a plastic dagger concealed inside a comb was detected in a passenger's pocket.[103] AIT's capability to identify these small items is important because in addition to weapons and explosive materials, TSA also searches for improvised explosive device components, such as timers, initiators, switches, and power sources. Such items may be very small. AIT enhances TSA's ability to find these small items and further assists TSA in detecting threats.

AIT is also effective in detecting metallic items. In December, 2011, a loaded .38 caliber firearm in an ankle holster was discovered during AIT screening of a passenger at Detroit Metropolitan Airport.[104] The versatility of AIT in detecting both metallic and nonmetallic concealed items makes it more effective and efficient than metal detectors as a tool to protect transportation security.

In addition, risk reduction analysis shows that the chance of a successful terrorist attack on aviation targets generally decreases as TSA deploys AIT. However, the results of TSA's risk-reduction analysis are classified. TSA estimates that from 2013 to 2015 total throughput of AIT increases from 57.9 percent to 77.5 percent resulting in more effective and efficient screening of passengers as illustrated in Table 18 and Table 19 in the passenger opportunity cost section.

---

[101] "Advanced Imaging Off To a Great Start," April 20, 2010, at http://blog.tsa.gov/2010/04/advanced-imaging-technology-off-to html and "Advanced Imaging Technology – Yes, It's Worth It," March 31, 2010, at http://blog.tsa.gov/2010/03/advanced-imaging-technology-yes-its html.

[102] "TSA Week in Review: Plastic Dagger Found With Body Scanner," May 4, 2012, at http://blog.tsa.gov/2012/05/tsa-week-in-review-plastic-dagger-found html.

[103] "TSA Week in Review: Comb Dagger Discovered With Body Scanner, 28 Loaded Guns, and More," August 17, 2012 at http://blog.tsa.gov/2012/08/tsa-week-in-review-comb-dagger html.

[104] http://blog.tsa.gov/2011/12/loaded-380-found-strapped-to-passengers.html.

TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. Devices have been, and will continue to be, constructed and intentionally hidden on parts of the body not detectable by current security protocols. Since 2001the use of non-metallic bombs highlight the adaptive and determined nature of terrorists. Terrorists adapt and evolve to attempt to evade detection , and as historical evidence shows, have developed weapons not detectable by WTMDs. AIT enhances the passenger screening environment twofold: AIT can detect non-metallic items as well as detect items concealed on sensitive parts of the body. AIT represents TSAs best available security measure against these emerging and changing threats.

To analyze the potential consequences of an attack that could be prevented by AIT technology, TSA evaluates the consequences associated with an IED attack where a passenger detonates the bomb while the aircraft is in flight. AIT prevents this type of scenario when AIT detects the necessary explosives before the terrorist reaches the aircraft.

When a terrorist detonates a bomb on a commercial aircraft, the bomb destroys the aircraft and kills all passengers and crew. Upwards of 300 people will be killed immediately onboard while, depending on where the aircraft falls, many more people will be killed by the falling debris. In addition to the lives lost, the bomb will cause considerable property damage. Damages include the high cost of the aircraft itself in addition to the property damage resulting from the falling debris. In a heavily populated area, the falling debris has potential to generate considerable damages to buildings, roadways and general infrastructure.

In addition to the direct impacts of a terrorist attack in terms of lost life and property, there are other more indirect impacts, particularly on aviation based terrorist attacks, that are difficult to measure. For example, one study estimates the 9/11 attacks as causing a .5 percentage decrease in GDP growth (or $60 billion dollars) and an upper bound estimate of twice that or $125 billion (in 2006 dollars).[105] Also, as noted by Cass Sunstein in the Laws of Fear, "…*fear is a real social*

[105] S. Brock Blomberg and Gregory D. Hess "*Estimating the Macroeconomic Consequence of 9/11*," Peace Economics, Peace Science and Public Policy, Volume 15 Issue 2 Article7, 2009. http://research.create.usc.edu/nonpublished_reports/166/

cost, and it is likely to lead to other social costs. If, for example, people are afraid to fly, the economy will suffer in multiple ways…"[106]

In addition, another study estimates at least 1,200 additional driving deaths were attributable to the effect of 9/11 as people substituted less-safe surface transportation for safer air transportation (as noted by these authors "*Our results show that the public response to terrorist threats can create unintended consequences that rival the attacks themselves in severity*." [107] In conclusion, as devastating as the direct impacts of a successful terrorist attack can be in terms of the immediate loss of life and property, avoiding the impacts of the more difficult to measure indirect effects are also substantial benefits of preventing a terrorist attack.

Advantages and Disadvantages of Regulatory Alternatives

TSA examined several different means to mitigate against the emerging non-metallic threats. TSA, as described in the alternative section, identified four alternatives to AIT screening:

- No action alternative
- Pat-Down
- ETD Screening
- AIT

Table 56 describes the four alternatives along with the advantages and disadvantages of each. Through risk analysis, laboratory testing, and field testing, TSA identified several solutions capable of detecting non-metallic items. After weighing the advantages and disadvantages of each alternative, TSA elected to deploy AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats. AIT reflects the best option to detect non-metallic weapons.

---

[106] Cass R. Sunstein, "Laws of Fear" p.127, 2005.

[107] Blalock et al, "*The Impact of 9/11 on Road Fatalities: The Other Lives Lost to Terrorism*" February 2, 2005. Abstract and page 1. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=677549

Table 56: Advantages and Disadvantages of Regulatory Alternatives

Regulatory Alternative	Name	Description	Advantages	Disadvantages
1	No Action	The passenger screening environment remains unchanged. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.	• No additional cost burden. • No additional perceived privacy concerns.	• Fails to meet the January 7, 2010 Presidential Memorandum[108] • Does not mitigate the non-metallic threat to aviation security
2	Pat-Down	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by with a pat-down on a randomly selected portion of passengers.	• Thorough physical inspection of metallic and non-metallic items. • Uses currently deployed WTMD technology. • Minimal technology acquisition costs	• Employs a substantial amount of human resources. • Increase in perceived privacy concerns. • Not every passenger is screened for non-metallic items. • Increased wait times

[108] http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack

Regulatory Alternative	Name	Description	Advantages	Disadvantages
3	ETD Screening	TSA continues to use WTMDs as the primary passenger screening technology. TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.	• Somewhat addresses the threat of non-metallic threats.	• Does not detect non-explosive non-metallic anomalies. • Increased wait times and associated passenger opportunity cost of time • Increase in ETD consumable
4	AIT (NPRM)	TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down.	• Safely screens passengers for metallic and non-metallic threats • Maintains lower personnel cost and higher throughput rates than the alternatives • ATR software alleviates passenger privacy concerns	• Incremental cost of acquisition to TSA • Incremental personnel cost to TSA • Incremental training cost to TSA • Potential for negative public perception on health and privacy concerns

CHAPTER 5: INITIAL REGULATORY FLEXIBILITY ANALYSIS

The Regulatory Flexibility Act (RFA) at 5 U.S.C. 603 requires agencies to consider the economic impact its rules will have on small entities. In accordance with the RFA, TSA has prepared an Initial Regulatory Flexibility Analysis (IRFA) that examines the impacts of the proposed rule on small entities (5 U.S.C 601 et seq.). A small entity may be:

- A small business, defined as any independently owned and operated business not dominant in its field that qualifies as a small business per the Small Business Act (15 U.S.C 632)
- A small not-for-profit organization
- A small governmental jurisdiction (locality with fewer than 50,000 people).

The definition of a small business varies from industry to industry, to properly reflect industry size differences. In this IRFA, TSA uses the SBA small business size standards for each relevant industry.

This IRFA addresses the following:

- A description of the reasons that action by the agency is being considered;
- A succinct statement of the objectives of, and legal basis for, the proposed rule
- A description – and, where feasible, an estimate of the number – of small entities to which the proposed rule will apply;
- A description of the projected reporting, recordkeeping, and other compliance requirements of the proposed rule, including an estimate of the classes of small entities that will be subject to the requirements and the types of professional skills necessary for preparation of the reports or records;
- An identification, to the extent practicable, of all relevant Federal rules that may duplicate, overlap, or conflict with the proposed rule; and

- A description of any significant alternatives to the proposed rule that accomplish the stated objectives of applicable statutes and may minimize any significant economic impact of the proposed rule on small entities, including alternatives considered.

Description of the Reasons that Action by the Agency is Being Considered

In the decision made by the U.S. Court of Appeals for the District of Columbia Circuit in *Electronic Privacy Information Center v. U.S. Department of Homeland Security*, the Court directed TSA to conduct notice and comment rulemaking on the use of AIT. This NPRM proposes to codify TSA's current use of AIT to conduct passenger screening.

Succinct Statement of the Objectives of, and Legal Basis for, the Proposed Rule

Pursuant to Congressional mandate, TSA is required to "provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft…"[109] The proposed rule adds a provision to 49 CFR part 1540 to clarify that this screening may include the use of AIT.

The main objective of the proposed rule is to codify the use of AIT as a means of screening passengers prior to entering the sterile area of an airport regulated under 49 CFR part 1540. This NPRM complies with the decision by U.S. Court of Appeals for the D.C. Circuit in *Electronic Privacy Information Center v. U.S. Department of Homeland Security*.

Description of and, Where Feasible, an Estimate of the Number of Small Entities to which the Proposed Rule will Apply

TSA's IRFA suggests that this rulemaking would not have a significant economic impact on a substantial number of small entities under section 605(b) of the RFA. An airport owned by a governmental entity is considered a small entity under the RFA if the owning government has a population of less than 50,000 people. Privately-owned airports are classified in NAICS code

---

[109] 49 U.S.C. 44901.

488119. A privately-owned airport is considered small under SBA standards if annual revenue amounts to less than $30 million.

In addition, this Initial Regulatory Impact Analysis includes costs to a business (costs incurred by Rapiscan). Costs incurred by Rapiscan are not direct costs due to requirements of this rule. Costs incurred by Rapiscan are due to the terms its contract with TSA. Nonetheless, TSA investigated if Rapiscan would be classified as a small business under the Regulatory Flexibility Act. TSA does not consider Rapiscan to be a small entity based on the employment size of their parent company, OSI Systems, Inc. OSI Systems is classified as NAICS code "Semiconductor and Related Devices Manufacturing" (334413). OSI Systems reports having 4,000 employees, which exceeds the 500 employee threshold to be considered small under SBA size standards for that industry.[110]

The owning entity of each airport was determined from FAA data, which lists the owners of all airports. The population served is based primarily on U.S. Census data (for counties and cities). Revenue data for counties and cities with populations above 25,000 are based on 2007 U.S. Census City and County Data book.[111] For those jurisdictions where revenue figures could not be found in the Census City and County data books, revenue data are taken from one of the following sources:

- The city's annual financial report (CAFR), when available online.
- www.city-data.com, a web site that compiles data from various government databases.
- The owner's annual financial report to the FAA.[112]

TSA scales all revenue data to 2011 dollars. To avoid double-counting the population, for airports that are owned by both a county and one or more cities within that county, the population is for the county only, while revenue is from both the county and the city.[113]

---

[110] http://files.shareholder.com/downloads/OSIS/2340310712x0x611139/7CC050BD-4B0D-4756-B76A-150EED5FBA20/OSI_Systems_Annual_Report_2012.pdf, Page 8 lists the approximate number of employees.

[111] The 2007 Census City and County Data book states revenue data in constant 2002 dollars. TSA uses a 2002 GDP factor of 1.230 to convert all revenue data to constant 2011 dollars. http://www.census.gov/statab/ccdb/cc07_tabB13.pdf.

[112] The FAA financial data cover only airport revenues and, therefore, understate the financial resources of the owning government.

Of the 446 federalized airports, TSA has identified a total of 102 small entities that may incur additional utility costs due to this rule. Small governmental jurisdictions make up 101 of the 102 small entities. TSA also identified one privately owned business; however TSA was unable to determine from publically available data if it is a small entity. To be conservative, TSA assumes the entity is a small business. Of the 101 small governmental jurisdictions, TSA reimburses the additional cost of utilities for 5 of them. Consequently, this rule causes 96 governmental jurisdictions to incur additional direct costs. Including the one small business, TSA estimates 97 small entities or 22 percent of all airports (97/446) will incur additional direct costs. Table 57 displays the number of airports and the number of small airports by category. The following section estimates the impact on these small entities by the relevant airport categories: Category II, III, and IV.

Table 57: Affected Small Entities

FAA Category	Number of Airports	Number of Small Entities	Number of Small Entities Reimbursed
X	28	0	0
I	57	0	0
II	79	6	1
III	127	16	1
IV	155	80	3
Total	**446**	**102**	**5**

Description of the Projected Reporting, Recordkeeping and Other Compliance Requirements of the Proposed Rule, Including an Estimate of the Classes of Small Entities that Will be Subject to the Requirement and the Type of Professional Skills Necessary for Preparation of the Report or Record

[113] TSA does not use county populations when cities and counties are geographically independent.

The proposed rule imposes no recordkeeping and reporting requirements.

Estimated Cost and Impact as a Percentage of Revenue

In this IRFA, TSA includes the additional utility costs incurred by airport operators but does not include the passenger opportunity cost incurred by individuals for opting out of AIT. As defined by the RFA, an individual is not considered to be a small entity. Additionally, the opting out delay has a minimal impact as it is estimated at 80 seconds and represents an opportunity cost of approximately one dollar per occurrence.

Small entities incur an incremental cost for utilities as a result of increased power consumption from AIT operation. To estimate the costs the deployment of AIT has on small entities TSA uses the average kilowatt hour (kWh) consumed per unit on an annual basis at federalized airports. TSA estimates an average cost per-kWh at these airports at $0.10 using data available from the U.S. Energy Information Administration.[114] Using this cost TSA estimates a per-unit daily average cost of $2.23.[115] TSA estimates the cost of utilities by multiplying the number of units in operation by the per-unit daily average and by the number of operating days. This cost varies by category of airport because FAA categorizes airports by size and TSA deploys more AIT units to larger airports. As shown in Table 58, TSA estimates that category II, III, and IV airports will

[114] TSA estimates this cost by taking the average of 2007-2011 retail electricity prices for the commercial sector as reported by the U.S. Energy Information Administration (http://www.eia.gov/electricity/monthly/epm_table_grapher.cfm?t=epmt_5_3).

[115] TSA calculates the per-unit utility cost per day as a weighted average of the power used to perform a scan and the power used while the system is idle. TSA assumes that the system will be operational for 16 hours (16 hours / 24 hours) of a day and idle for 8 hours (8 hours / 24 hours) of a day. TSA then estimates the weighted average of kW used per hour by taking the sum of the power consumption when the system is in operation (1.02) multiplied by the fraction of a day the system is in operation (16 hours / 24 hours) and the power consumption when the system is idle (0.70) multiplied by the percent of a day the system is idle (8 hours / 24 hours). This calculation results in an average kW used per hour of 0.9133 ((1.02 x (16/24)) + (0.70 x (8/24))). TSA then calculates the average kW used per day by multiplying the kW used per hour (0.9133) by 24 hours to obtain an average of 21.92 kWh per day (0.9133 x 24). TSA then multiplies this average number of kWh per day by the cost per kWh ($0.1019) to obtain a per-unit utility cost per day of $2.234 (21.92 x $0.1019). TSA uses $2.234 as the input for all per-unit unity cost for AIT.

incur an average annual increase in utility costs of $1,012, $629 and $347 on an annual basis, respectively.

Table 58: Average Utility Cost for Small Entities by Airport Category ($)

FAA Category	Number of AIT Units a	Cost per Unit per Day b	Total Cost per Year c = a x b x 365	Number of Airports d	Average Cost per Airport e = c / d
II	98	$2.23	$79,910	79	$1,012
III	98	$2.23	$79,910	127	$629
IV	66	$2.23	$53,817	155	$347

TSA estimates that of the 102 entities assumed to be small by SBA standards, 97 entities do not receive reimbursement from TSA. TSA estimates the average additional utility costs to range from $347 to $1,012 per year while the average annual revenue for these small entities ranges from $69.5 million to $133.1 million per year. Consequently, TSA estimates that the cost of this NPRM on small entities represents approximately 0.001 percent of their annual revenue. The remaining 5 entities receive reimbursement for their utilities and are therefore unaffected from an increase in utility costs as a result of AIT deployment. Table 59 summarizes the impacts of AIT deployment on small entities as a percentage of revenue.

Table 59: Ratio of Revenue to Compliance Costs for Small Governmental Jurisdictions Owning Part 1542 Airports ($)

FAA Category	Average Annual Revenue Per Small Entity[116] a	Average Annual Utility Costs b	Cost as a Percent of Revenue c = b / a
II	$133,082,989	$1,012	0.0008%
III	$95,391,288	$629	0.0007%
IV	$69,523,104	$347	0.0005%

Identification, to the Extent Practicable, of All Relevant Federal Rules that May Duplicate, Overlap, or Conflict with the Proposed Rule

The Agency is unaware of any Federal rules which may duplicate, overlap, or conflict with the proposed rule.

Description of any Significant Alternatives to the Proposed Rule that Accomplish the Stated Objectives of Applicable Statutes and that Minimizes any Significant Economic Impact of the Proposed Rule on Small Entities.

As alternatives to the preferred regulatory proposal are explained in the NPRM, TSA examined three additional options. Chapter 3 of this initial RIA explains these alternatives in more detail. The following table briefly describes these options, which include a continuation of the current screening environment (no action), increased use of physical pat-down searches that supplements primary screening with WTMDs, and increased use of ETD screening that supplements primary screening with WTMDs.

[116] As revenues for the one privately-owned airport are not publicly available, TSA does not include their revenue in the average revenue estimation.

Table 60: Comparison of Regulatory Alternatives

Regulatory Alternative	Name	Description
1	No Action	Under this alternative, the passenger screening environment remains the same as it was prior to 2008. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.
2	Pat-Down	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting a pat-down on a randomly selected portion of passengers after screening by a WTMD.
3	ETD Screening	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.
4	AIT (NPRM)	Under this alternative, the proposed alternative, TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down.

The no action alternative imposes no incremental burden on small entities; however this alternative fails to detect non-metallic objects. The pat-down alternative imposes a heavy burden on TSO staffing but no incremental burden on small entities. Although small entities would not be directly burdened under this alternative, performing pat-downs on a significant number of passengers necessitates a substantial increase in TSA staffing levels to maintain the current passenger throughput level. Without a staffing increase, passenger wait times and the associated opportunity cost increases. Finally, ETD would generate both a utility cost for small entities and a large amount of consumables for TSA and ETDs cannot detect dangerous items such as weapons and IED components made of ceramics or plastics whereas AIT is capable of detecting any anomaly concealed under clothing.

After weighing the advantages and disadvantages of each alternative, TSA elected to deploy AIT as a means of screening passengers to mitigate the vulnerability that exists with the inability of WTMDs to detect non-metallic threats. TSA requests public comment on all of the alternatives considered, as well as the impacts on small entities.

Preliminary Conclusion

Based on this preliminary analysis, TSA believes that deployment of AIT would not have a significant economic impact on a substantial number of small entities under section 605(b) of the RFA. TSA requests comment on all aspects of this analysis.

CHAPTER 6: INTERNATIONAL TRADE IMPACT ASSESSMENT

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. The Trade Agreement Act does not consider legitimate domestic objectives, such as safety, unnecessary obstacles. The statute also requires that international standards be considered and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this NPRM and has determined this proposed rule would not have an adverse impact on international trade.

CHAPTER 7: UNFUNDED MANDATES REFORM ACT ANALYSIS

Title II of the Unfunded Mandates Reform Act of 1995 (UMRA), Public Law 104–4, establishes requirements for Federal Agencies to assess the effects of their regulatory actions on State, local, and tribal governments and the private sector. Under section 202 of the UMRA, TSA generally must prepare a written statement, including a cost-benefit analysis, for proposed and final rules with ''Federal mandates'' that may result in expenditures by State, local, and tribal governments, in the aggregate, or by the private sector, of $100 million (adjusted for inflation) or more in any one year. Before TSA promulgates a rule for which a written statement is needed, section 205 of the UMRA generally requires TSA to identify and consider a reasonable number of regulatory alternatives and adopt the least costly, most cost effective, or least burdensome alternative that achieves the objectives of the rule. The provisions of section 205 do not apply when they are inconsistent with applicable law. Moreover, section 205 allows TSA to adopt an alternative other than the least costly, most cost-effective, or least burdensome alternative if the Administrator publishes with the final rule an explanation why that alternative was not adopted. Before TSA establishes any regulatory requirements that may significantly or uniquely affect small governments, including tribal governments, it must develop under section 203 of the UMRA a small government agency plan. The plan must provide for notifying potentially affected small governments, enabling officials of affected small governments to have meaningful and timely input in the development of TSA regulatory proposals with significant Federal intergovernmental mandates, and informing, educating, and advising small governments on compliance with the regulatory requirements.

TSA has determined that this rule does not contain a Federal mandate that may result in expenditures of $142 million or more in any one year (when adjusted for inflation) in 2011 dollars for either State, local, and tribal governments in the aggregate, or by the private sector. TSA will publish a final analysis, including its response to public comments, when it publishes a final rule.

APPENDIX A: TRAINING POPULATIONS FOR L3 and Rapiscan Units

TSA incurs costs to train TSOs to operate and effectively screen passengers using AIT machines. TSOs take initial and recurring training on AIT operation and screening. Recurring training must be completed annually. Additionally, to account for TSA's shift from AIT with IO to AIT with ATR, TSA estimates a transition training cost. The five components of training costs, along with their respective time requirements (shown in parentheses), are:

- Initial AIT with IO training (20 hours)
- Recurring AIT with IO training (6 hours)
- Training to transfer from AIT with IO to AIT with ATR (at airports where AIT with IO was deployed prior to ATR development but later upgraded to ATR software) (14.23 hours)
- Initial AIT with ATR training (12 hours)
- Recurring AIT with ATR training (6 hours)

Table A1 displays the number of additional units of AIT in the field based on technology, both for L3 and Rapiscan units. These data inform TSA on future training costs. This appendix will describe the L3 AIT actual and training population, then Rapiscan units estimated training population.

Table A1: Actual Number of Additional AIT Units in Field by Technology

Year	Rapiscan	L3	Total
2008	0	30	30
2009	0	2	2
2010	250	208	458
2011	0	69	69

Table A2: Estimated Number of Additional AIT Units in Field by Technology

Year	Rapiscan	L3	Total
2012	0	423	423
2013	0	0	0
2014	0	44	44
2015	0	45	45

For 2008-2011, TSA uses historical data on training populations to estimate training costs.[117] Historical data on training populations include counts for both initial training for new hires and initial training for employees entering the labor force due to turnover.

[117] Because TSA uses historical data, some of the estimates appear inflated based on prior assumptions on AIT staffing needs. In TSO training, TSA TSOs repeat courses and TSOs take courses outside of their necessary curriculum. However, TSA is unable to separate the mandatory training from the non-mandatory training.

Table A3: Unadjusted Historical Counts of the L3 Training Population[118]

Year	Employees in Initial Training (Historical) a	Cumulative Training Population b = ∑a	Recurring Training Population[119]
2008	1,006	1,006	0
2009	206	1,212	0
2010	5,828	7,040	0
2011	21,306	28,346	0

To project populations needing training in future years, TSA estimates the training populations in each year using the number of newly deployed AIT (Table A2, L3 Column) units multiplied by estimated need for TSOs to maintain full AIT coverage (0.0 TSOs per AIT).[120] TSA estimates the population in future years needing training based on the number of newly deployed AIT units and not on historical population data.

TSA also estimates the population of TSOs entering the labor force due to turnover. To estimate the turnover for the TSO population, TSA multiplies the prior year cumulative training population by the assumed 9.0 percent turnover rate from TSA's Office of Human Capital. For example, in 2012, TSA estimates the population of 2,551.1 L3 trained TSOs entering the labor

---

[118] Unadjusted training populations includes the population trained as new hires. Below, TSA nets out these populations to avoid double counting.

[119] TSA administered no historical L3 recurring training from 2008-2011.

[120] Originally, the training estimate for full capacity included an additional 250 Rapiscan units which would require 1,312.5 TSOs (250 x 5.25 TSOs per Rapiscan unit) and 265 L3 units which would require 927.5 additional TSOs (265 x 3.5 TSOs per L3 unit). We took out this level of personnel from the previous estimate and concluded that the number of TSA trained by the end of 2011 is such that no new TSOs (beyond turnover) need to be trained in 2012 - 2015.

force due to turnover (Table A4 Column B) by multiplying the 2011 cumulative population (28,346 from Table A3 Column B, 2011) by 9.0 percent. For each year, TSA then estimates the total population receiving initial training (Table A4 Column C) by summing the employees hired entering the labor force due to the additional deployment of AIT units (Table A4 Column A) and employees entering the labor force due to turnover (Table A4 Column B). Lastly, to estimate the population needing recurring training in each year (Table A4 Column E), TSA subtracts the initial training populations (Table A4, Column C) from the cumulative training population (Table A4, Column D). The cumulative training population is derived by adding the initial training population (Table A4 Column A) to the previous year's cumulative population. For example, in 2012 TSA adds the 0 additional employees receiving initial training to the cumulative population of 2011 (Table A3, Column B, 2011) to estimate the cumulative population training.

Table A4: Unadjusted Projection of the L3 Training Population

Year	Employees in Initial Training a = AIT newly deployed x 0.0*	Turnover $b = b^{**}_{-1}$ x 9.0%	Initial Training Population c = a + b	Cumulative Training Population $d = b_{-1} + \sum a$	Recurring Training Population e = d - c
2012	0	2,551.1	2,551.1	28,346.0	25,794.9
2013	0	2,551.1	2,551.1	28,346.0	25,794.9
2014	0	2,551.1	2,551.1	28,346.0	25,794.9
2015	0	2,551.1	2,551.1	28,346.0	25,794.9

* Based on the number of TSA trained by the end of 2011, the removal of the Rapiscan units and the reallocation of L3 units in the field lowered the staffing need such that no new TSOs (beyond turnover) need to be trained in 2012 - 2015.

**b_{-1} denotes the cumulative population from column B Table A2 in 2011

TSA estimates the population of TSOs entering the labor force due to the deployment of AIT. Table A5 displays the personnel to maintain full operating capacity previously calculated and displayed in the initial RIA (Tables 18 & 19). To separate the TSO population into the two companies, TSA estimates a constant TSO population hired on Rapiscan units (2,236.0) based on the number of lanes covered by Rapiscan deployment and the additional TSOs per lane. L3 personnel due to the AIT deployment (Table A5 Column D) is estimated by subtracting the Rapiscan population (Table A5 Column C) from the total population of AIT with IO (Table A5 Column A) and AIT with ATR (Table A5 Column B).

Table A5: Number of Personnel Hired Due to the AIT Deployment

Year	Personnel to Maintain Full Operating Capacity		*Rapiscan Cumulative Personnel due to the AIT Deployment*	*L3 Cumulative Personnel due to the AIT Deployment*
	AIT with IO *a*	*AIT with ATR* *b*	*c = c**	*d = a + b - c*
2008	267.8	0		267.8
2009	283.5	0		283.5
2010	4,394.3	0	2,242.8	2,151.5
2011	5,019.0	0	2,242.8	2,776.2
2012**	2,242.8	4,377.84	2,242.8	4,377.8
2013	0	4,378.50		4,378.5
2014	0	4,644.50		4,644.5
2015	0	4,907.00		4,907.0

c*- TSA estimates a constant TSO population trained on Rapiscan units (2,242.8) by assuming the 250 Rapiscan units deployed cover approximately 425.9 lanes and requiring an additional 5.25 TSOs per lane (427.2 lanes x 5.25 TSOs).

** In December 2012, 76 Rapiscan machines were removed, however, it is assumed the training requirements for these machines were met in 2012.

As in the cost section above, the personnel population that TSA calculates based on AIT deployment does not account for new personnel needs due to turnover. TSA estimates the personnel in each year that have been hired due to the newly deployed AIT units and entered the labor force due to turnover using the same 9.0 percent turnover rate for the cumulative personnel estimate for the prior year. For example, the 24.1 personnel hired in 2009 due to turnover (Table

A6 Column C, 2009) is 9.0 percent of the 267.8 cumulative personnel in 2008 (Table A5 Column D: Table A6 Column A). The population estimate for total initial training for personnel hired due to the newly deployed AIT units (Table A6 Column D) includes the initial training of new personnel (Table A6 Column B) and the initial training of personnel entering the labor force due to turnover (Table A6 Column C). TSA then estimates the population of personnel hired due to the AIT deployment that need recurring training (Table A6 Column E) by subtracting the initial training population (Table A6 Column D) from the cumulative personnel population in (Table A6 Column A) each year. Because TSA estimates the personnel costs in terms of FTE, the tables show the FTE equivalent of new hires rounded to the nearest tenth decimal.

Table A6: Personnel Included in the L3 Training Population

Year	Cumulative Personnel due to the AIT Deployment a	Initial Training from AIT Deployment for Personnel due to the AIT Deployment $b = a - a_{-1}$	Initial Training from Turnover for Personnel due to the AIT Deployment $c = a_{-1} \times 9.0\%$	Total Initial Training Population for Personnel due to the AIT Deployment $d = b + c$	Recurring Training Population for Personnel due to the AIT Deployment[121] $e = a - d$
2008	267.8	267.8		267.8	0.0
2009	283.5	15.8	24.1	39.8	0.0
2010	2,151.5	1,868.0	25.5	1893.5	0.0
2011	2,776.2	624.8	193.6	818.4	0.0
2012	4,377.8	1,601.6	249.9	1851.5	2,526.3
2013	4,378.5	0.7	394.0	394.7	3,983.8
2014	4,644.5	266.0	394.1	660.1	3,984.4
2015	4,907.0	262.5	418.0	680.5	4,226.5

[121] TSA administered no recurring training for L3 units from 2008 to 2011.

To estimate the training populations, TSA subtracts the personnel estimates above from the original training estimates. Table A7 combines the data from Tables A4 and A6 to calculate net initial and recurring training populations. In order to estimate net initial training population (Table A7 Column E), TSA subtracts the initial training from the AIT deployment (Table A6 Column D: Table A7 Column C) from the historical total initial training population (Table A3 Column A) and the forecasted initial training population (Table A4 Column C: Table A7 Column A). The same methodology is done to estimate net recurring training population. Net recurring population (Table A7 Column F) is the difference of recurring training population from the AIT deployment (Table A6 Column E: Table 7 Column D) from total recurring training population (Table A4 Column E: Table A7 Column B).

Table A7: Summary of L3 Training Populations

Year	Unadjusted Initial Training Population a	Unadjusted Recurring Training Population b	Total Initial Training Population for personnel hired due to the AIT Deployment c	Recurring Training Population for personnel hired due to the AIT Deployment d	Adjusted L3 Initial Training e = a - c	Adjusted L3 Recurring Training f = b - d
2008	1,006.0	0.0	267.8	0.0	738.3	0.0
2009	206.0	0.0	39.8	0.0	166.2	0.0
2010	5,828.0	0.0	1,893.5	0.0	3,934.5	0.0
2011	21,306.0	0.0	818.4	0.0	20,487.6	0.0
2012	2,551.1	25,794.9	1,851.5	2,526.3	699.6	23,268.6
2013	2,551.1	25,794.9	394.7	3,983.8	2,156.4	21,811.1
2014	2,551.1	25,794.9	660.1	3,984.4	1,891.0	21,810.5
2015	2,551.1	25,794.9	680.5	4,226.5	1,870.6	21,568.4

Next, TSA uses the estimated initial (Table A7 Column E) and recurring training populations (Table A7 Column F) in each year to allocate the training costs between the five different training categories: initial with IO, recurring with IO, transition from IO to ATR, initial ATR, and recurring ATR. TSA introduced the ATR technology in 2011, therefore all initial and recurring trainings from 2008 to 2010 is for initial IO training. In 2011 when ATR was introduced, TSA estimates the IO to ATR training population, which is outside the initial training population, based on TSA training records for 2011. TSA splits the initial population between IO and ATR based on historical training counts in 2011 with 72 percent of TSO trained on ATR.

Finally, TSA assumes all initial and recurring training from 2012 to 2015 involves ATR technology.

Table A8: L3 Training Population by Training Type

	IO			ATR	
Year	**Initial**	**Recurring**[122]	**IO to ATR**	**Initial**	**Recurring**
2008	738.3	0.0	0.0	0.0	0.0
2009	166.2	0.0	0.0	0.0	0.0
2010	3,934.5	0.0	0.0	0.0	0.0
2011	5,650.3	0.0	9,142.0	14,837.3	0.0
2012	0.0	0.0	0.0	699.6	23,268.6
2013	0.0	0.0	0.0	2,156.4	21,811.1
2014	0.0	0.0	0.0	1,891.0	21,810.5
2015	0.0	0.0	0.0	1,870.6	21,568.4

TSA uses the same methodology to calculation training populations for the Rapiscan technology with some minor modifications. The same tables that were presented for L3 technology are presented below with any slight modifications detailed in footnotes.

The rest of the tables show these same calculations for the Rapiscan technology.[123]

[122] No historical recurring training for L3 units occurred in years 2008 to 2011.

[123] Although the historical populations for the Rapiscan technology seem disproportionately high in comparison to their deployment numbers, TSA mainly deployed the Rapiscan units to large airport hubs, and thus observed a higher than average number of employees trained per Rapiscan unit.

Table A9: Unadjusted Historical Counts of the Rapiscan Training Population

Year	Employees in Initial Training (Historical) a	Cumulative Training Population $b = \sum a$	Recurring Training Population $c = b - a$
2008	0	0	0
2009	0	0	0
2010	8,151	8,151	0
2011	5,442	13,593	8,151

Table A10: Unadjusted Projection of the Rapiscan Training Population

Year	Employees in Initial Training a = AIT newly deployed x 0.0	Turnover $b = c_{-1} \times 9.0\%$	Initial Training Population $c = a + b$	Cumulative Training Population $d = c_{-}*_{1} + \sum a$	Recurring Training Population $e = d - c$
2012	0	1,223.4	1,223.4	13,593.0	12,369.6
2013	0	0.0	0.0	13,593.0	0.0
2014	0	0.0	0.0	0.0	0.0
2015	0	0.0	0.0	0.0	0.0

c_{-1} denotes the population from Column C Table A9 in 2011

TSA estimates separately the personnel hired due to the AIT rule by the L3 and Rapiscan technologies. For the Rapiscan technology, TSA estimates the total staffing needs in 2010 as 2,242.8 personnel, based on the 250 Rapiscan units deployed in 2010, and then repeats this calculation for future years.[124]

Table A11: Personnel Included in the Rapiscan Training Population

Year	Cumulative Personnel due to the AIT Deployment a	Initial Training from AIT Deployment for Personnel due to the AIT Deployment[125] $b = a - a_{-1}$	Initial Training from Turnover for Personnel due to the AIT Deployment c = a x 9.0%	Total Initial Training Population for personnel due to the AIT Deployment d = b + c	Recurring Training Population for personnel due to the AIT Deployment e = a - d
2008	0.0	0.0		0.0	0.0
2009	0.0	0.0	0.0	0.0	0.0
2010	2,242.8	2,242.8	0.0	2242.8	0.0
2011	2,242.8	0.0	201.9	201.9	2,040.9
2012	2,242.8	0.0	201.9	201.9	2,040.9
2013	0.0	0.0	201.9	201.9	0.0
2014	0.0	0.0	0.0	0.0	0.0
2015	0.0	0.0	0.0	0.0	0.0

[124] As discussed above, the deployment of AIT with IO in 2010 is equal to the one time deployment of the 250 Rapiscan units.

[125] TSA estimates the initial population trained on Rapiscan AITs assuming 250 Rapiscan AITs covering approximately 427 lanes requiring an additional 5.25 TSOs per lane (427.2 lanes x 5.25 TSOs).

Table A12: Summary of Adjusted Rapiscan Training Populations

Year	Unadjusted Initial Training Population a	Unadjusted Recurring Training Population b	Total Initial Training Population for personnel hired due to the AIT Deployment c	Recurring Training Population for personnel hired due to the AIT Deployment d	Adjusted Rapiscan Initial Training e = a - c	Adjusted Rapiscan Recurring Training f = b - d
2008	0.0	0.0	0.0	0.0	0.0	0.0
2009	0.0	0.0	0.0	0.0	0.0	0.0
2010	8,151.0	0.0	2,242.8	0.0	5,908.2	0.0
2011	5,442.0	8,151.0	201.9	2,040.9	5,240.1	6,110.1
2012	1,223.4	12,369.6	201.9	2,040.9	1,021.5	10,328.7
2013	0.0	0.0	0.0	0.0	0.0	0.0
2014	0.0	0.0	0.0	0.0	0.0	0.0
2015	0.0	0.0	0.0	0.0	0.0	0.0

Table A13: Rapiscan Training Population by Training Type

	IO			ATR	
Year	**Initial IO**[126]	**Recurring IO**	**IO to ATR**	**ATR Initial**	**Recurring with ATR**
2008	0.0	0.0	0.0	0.0	0.0
2009	0.0	0.0	0.0	0.0	0.0
2010	5,908.2	0.0	0.0	0.0	0.0
2011	5,240.1	6,110.1	0.0	0.0	0.0
2012	1,021.5	10,328.7	14,816.4	0.0	0.0
2013	0.0	0.0	0.0	0.0	0.0
2014	0.0	0.0	0.0	0.0	0.0
2015	0.0	0.0	0.0	0.0	0.0

[126] Although deployment for Rapiscan occurs only in 2010, the historic initial training for IO occurred over 2 calendar years. IO training in 2012 only includes initial training due to turnover.

APPENDIX B: COST ESTIMATE EXPLANATION OF 2013 RAPISCAN TECHNOLOGY REMOVAL

All Rapiscan general-use backscatter units currently deployed at TSA checkpoints are being removed from operation by May 31, 2013. TSA plans to remove all Rapiscan units from airports and complete the Rapiscan backfill by May 31st, 2013. To estimate the impact of the mid-year removal and replacement of the Rapiscan unit, TSA estimates a weighted average for 2013. TSA only applies the weighted average for cost elements that depend on the number of active units in the field because these costs will only occur during a portion of the year before the removal of Rapiscan units. These cost elements include the utility cost for industry and TSA, passenger opportunity cost, personnel cost, and maintenance cost. In contrast, TSA does not apply the weighted average to costs that depend on the deployment of AIT units, or to one-time costs like the removal of Rapiscan units.

Table B 1 shows the AIT units (both L3 and Rapsican units) in-service in the various airport categories in 2013. TSA assumes that 2013a reflects the active units at the start of 2013 while 2013b reflect only the L3 units originally deployed and utilized for backfill. The estimate of active units at the start of 2013 (2013a in Table B 1) include the Rapiscan units to be removed by the company. In 2012, before the TSA decision to remove the Rapiscan units from the airports, TSA removed 76 units. These 76 units are not included in the 2013a estimates. The difference between the 2013a and 2013b active AIT units is the 174 units that the Rapiscan removes. To estimate the cost of AIT in 2013, TSA weights the 2013a number of AIT units in each airport category by 5/12 (for the initial 5 months of the year where both Rapiscan and L3 units are in use) and the 2013b number by 7/12 (to account for the 7 months out of the year where only the L3 units are in use). The resulting weighted number of AIT units for each airport category is shown in Table B 1. This appendix outlines the inputs and assumptions made to estimate the weighted average 2013 figures.

Table B 1: AIT units In-service in the Field for 2013, Weighted and Unweighted Totals

	Cat X	Cat I	Cat II	Cat III	Cat IV	Total
2013a	421	252	104	95	34	**906**
2013b	327	184	96	91	34	**732**
Weighted Average	**366**	**212**	**99**	**93**	**34**	**805**

Airport Utility Cost

To estimate the airport utility cost for non-reimbursable AITs in 2013, TSA first estimates the number of AIT units in use at the start of 2013 (2013a). The active AIT units in 2013 includes the 341 L3 units already in the field and the Rapiscan units removed by Rapiscan in 2013 (155). This figure does not include the Rapiscan units removed by TSA, because the cost estimate for 2012 utilities includes these units. The total number of non-reimbursable AITs in 2013a is 496 (341 L3 units + 155 Rapiscan units removed by the company). Next, TSA combines the 496 units estimated for 2013a and the 2013b estimate of L3 units already in the field (341) as described above to obtain a weighted average of 406 units for 2013. TSA then calculates the airport utility costs for 2013 using the weighted average number of AIT units and the costs per kWh for AITs and WTMDs, as described in Tables 15 and 16 of the Regulatory Evaluation.

Table B 2: Airport Utility Costs in 2013

(AIT costs in 1000s)

Year	AITs		WTMDs		Total Cost
	Units In-service	***AIT Cost***	***Removed WTMDs***	***WTMD Cost***	
	a	b = (a x $2.23 x 365)	c	d = (c x $0.10 x 365)	***= b - d***
2013a	496	$404.4	49	$1.8	**$402.7**
2013b	341	$278.1	49	$1.8	**$276.3**
Weighted Total	**406**	**$331.0**	**49**	**$2.00**	**$329.0**

Passenger Opportunity Cost

To estimate the passenger opportunity cost for opting out of AIT in 2013, TSA only changes the assumption of the AIT throughput percent of total passengers. Based on the initial estimate of AIT throughput, TSA assumes that 55 percent of passengers go through AIT units at the start of 2013 (2013a). Once the reallocation of L3 units and removal of Rapiscan units occurs, TSA projects that the percent of AIT throughput will increase to 60 percent (2013b). TSA bases this increase in the percent of AIT passenger throughput on an optimization strategy involving strategically located L3 units at check points with high capacity. Similar to the weighted average calculations shown above, TSA calculates a weighted average percent AIT throughput by combining the 2013a and 2013b percentages of AIT passenger throughput, as shown in Table B 3. TSA then calculates passenger opportunity costs in 2013 using the weighted average AIT throughput percent, as described in the Regulatory Evaluation in Tables 17 and 18.

Table B 3: Passenger Opportunity Cost in 2013

(Proposed AIT Costs in $ 1,000s)

Year	Passengers a[127]	AIT Throughput Percent of Total Passengers b	Number of Opt-Outs c = a x b x 1.18%	Total Cost for Opt-Outs d = c x $0.871
2013a	670,587,197	55.0%	4,352,111	$3,790.7
2013b	670,587,197	60.0%	4,747,757	$4,135.3
Weighted Total	**670,587,197**	**58%**	**4,582,905**	**$3,991.7**

Personnel Cost

To estimate the personnel cost in 2013, TSA again calculates a weighted average based on the number of active units at the start of 2013 (2013a) and the number of L3 units originally deployed and utilized for backfill (2013b). Table B 4 presents the estimates for the number of

[127] TSA rounds the estimated passenger throughput to the third decimal point as inputs for the model.

AIT units and lanes covered by AIT for both 2013a and 2013b for each AIT technology (IO and ATR). TSA then calculates the personnel cost in 2013 using the weighted average number of AIT units and lanes covered by AIT, and the additional personnel needed to be hired, as described in the Regulatory Evaluation in Tables 20 and 21.

Table B 4: Personnel Cost in 2013

(AIT costs in 1000s)

Year	AIT Units In-service		Lanes In-Service Covered by AIT		Additional Personnel		Annual FTE	Total
	with IO	with ATR	with IO	with ATR	AIT with IO	AIT with ATR		h = (e + f) * g
	a	b	c	d	e = c * 5.25	f = d * 3.5	g	
2013a	174	732	287.5	1,209.5	1,509.38	4,233.24	$56.8	$326,019.7
2013b	0	732	0.0	1,251.0	0.00	4,378.50	$56.8	$248,576.2
Weighted Total	**73**	**732**	**119.8**	**1,233.7**	**628.91**	**4,317.98**		**$280,844.3**

Training Cost

TSA makes training and hiring decisions at the start of the year. Because TSA knows that the Rapiscan units will be removed and that several L3 units will be redistributed at the start of 2013, TSA does not include the cost to train new personnel on the Rapiscan units. Because of the removal Rapiscan units, TSA has a large enough currently trained population to operate the number of AITs planned throughout 2015. Only recurring training costs occur in 2013 and beyond.

AIT Lifecycle Cost

To estimate the AIT lifecycle cost in 2013, TSA first estimates the number of AIT units in-service at the start of 2013 (2013a). These AIT units represent those whose 2-year warranties are expiring. Therefore, the AIT units represented in this section represent deployment numbers from two years ago. As shown in Table B 6, the number of AIT units in-service in 2013 includes 309 L3 units and 250 Rapiscan units. The total number of AITs in-service in 2013a is thus 559 (309 L3 units + 250 Rapiscan units). Next, TSA combines the 559 units estimated for 2013a and 2013b estimate of number of L3 units in-service (309) as described above to obtain a weighted average number of AIT units in-service for 2013. TSA then calculates the AIT lifecycle cost for 2013 using the weighted average number of AIT units in-service and the various lifecycle costs, as described in Tables 35 and 49 of the Regulatory Evaluation.

Table B 5: Maintenance Costs, Call Center, and Support Services in 2013

(AIT costs in 1000s)

Year	**AIT Units In-service**	**Out-of-Warranty Maintenance**	**Call Center**	**Support Services**	**Total**
	a	**b = a x $15,642**	**c = $14,787,267**	**d = $5,762,579**	**e = b + c + d**
2013a	559	$8,743.9	$14,787.3	$5,762.6	$29,293.7
2013b	309	$4,833.4	$14,787.3	$5,762.6	$25,383.2
Total Weighted	**413**	**$6,463.0**	**$14,787.0**	**$5,763.0**	**$27,013.0**

TSA Utilities Cost

To estimate the utility cost to TSA in 2013, TSA first estimates the number of the AIT units in-service at reimbursed airports in 2013 (2013a). The AIT units in-service at reimbursed airports in 2013a includes 391 L3 units and the Rapiscan units removed by Rapiscan in 2013 (19). The number of AITs in-service in 2013a is thus 410 (391 L3 units and Rapiscans + 19 Rapiscan units removed by the company). Next, TSA combines the 419 units in-service estimated for 2013a and 2013b estimate of L3 units in-service in the field (391) as described above to obtain a weighted average of 399 units in-service for 2013. TSA then calculates its utility costs for 2013 using the weighted average number of AIT units in-service and the per kWh costs for AITs and WTMDs, as described in Tables 50 and 51 of the Regulatory Evaluation.

Table B 6: TSA Utility Costs in 2013

(AIT costs in 1000s)

Year	**AITs**		**WTMDs**		**Total Cost**
	AIT Units In-service	***AIT Cost***	***Removed WTMD***	***WTMD Cost***	
	a	b = (a x \$2.23 x 365)	c	d = (c x \$0.10 x 365)	**= *b - d***
2013a	410	\$334.3	27	\$1.0	**\$333.4**
2013b	391	\$318.8	27	\$1.0	**\$317.9**
Weighted Total	**399**	**\$325.0**	**27**	**\$1.00**	**\$324.0**

ORAL ARGUMENT NOT YET SCHEDULED

No. 16-1135, consolidated with No. 16-1139

**IN THE UNITED STATES COURT OF APPEALS
DISTRICT OF COLUMBIA CIRCUIT**

COMPETITIVE ENTERPRISE INSTITUTE, et al.,
Petitioners,

v.

UNITED STATES DEPARTMENT OF HOMELAND SECURITY, et al.,
Respondents.

ON PETITION FOR REVIEW OF FINAL RULE OF TRANSPORTATION SECURITY ADMINISTRATION

**JOINT APPENDIX
VOLUME II OF II (JA 416 – JA 773)**

BENJAMIN C. MIZNER
Principal Deputy Assistant Attoney General
CHANNING D. PHILLIPS
United States Attorney
MARK B. STERN
SHARON SWINGLE
(202) 353-2689
Attorneys, Appellate Staff
Civil Division, Room 7250
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

MARC ROTENBERG
Counsel of Record
ALAN BUTLER
JERAMIE SCOTT
Electronic Privacy Information Center
1718 Connecticut Ave. NW, Suite 200
Washington, DC 20009
(202) 483-1140
Counsel for Petitioner
Electronic Privacy Information Center

SAM KAZMAN
HANS BADER
COMPETITIVE ENTERPRISE INSTITUTE
1310 L Street NW, 7th Floor
Washington, DC 20005
(202) 331-2278
Counsel for Petitioner
Competitive Enterprise Institute

December 15, 2016

TABLE OF CONTENTS

VOLUME II

THIS PAGE INTENTIONALLY LEFT BLANK

Executive Order 13132

NHTSA does not believe that there would be sufficient federalism implications to warrant the preparation of a federalism assessment.

Paperwork Reduction Act

The proposed rule does not contain any information collection requirements under the Paperwork Reduction Act of 1995 (44 U.S.C. 3501–3520).

Unfunded Mandates Reform Act of 1995

NHTSA has determined that the requirements of Title II of the Unfunded Mandates Reform Act of 1995 do not apply to this rulemaking.

Privacy Act

Anyone is able to search the electronic form for all comments received into any of our dockets by the name of the individual submitting the comments (or signing the comment, if submitted on behalf of an association, business, labor union, etc.). For more information on DOT's implementation of the Privacy Act, please visit: *http://www.dot.gov/privacy.*

List of Subjects in 49 CFR Part 553

Rulemaking Procedures.

For the reasons set forth in the preamble, the National Highway Traffic Safety Administration proposes to amend 49 CFR part 553 of the Code of Federal Regulations as follows:

PART 553—RULEMAKING PROCEDURES

■ 1. The authority citation is revised to read 49 U.S.C. 322, 1657, 30103, 30122, 30124, 30125, 30127, 30146, 30162, 32303, 32502, 32504, 32505, 32705, 32901, 32902, 33102, 33103, and 33107; delegation of authority at 49 CFR 1.95.

■ 2. Add § 553.14 to Subpart B to read as follows:

§ 553.14 Direct final rulemaking.

If the Administrator, for good cause, finds that notice is unnecessary, and incorporates that finding and a brief statement of the reasons for it in the rule, a direct final rule may be issued according to the following procedures.

(a) Rules that the Administrator judges to be non-controversial and unlikely to result in adverse public comment may be published as direct final rules. These may include rules that:

(1) Are non-substantive amendments, such as clarifications or corrections, to an existing rule;

(2) Update existing forms or rules, such as incorporations by reference of the latest technical standards;

(3) Affect NHTSA's internal procedures, such as filing requirements and rules governing inspection and copying of documents;

(4) Are minor substantive rules or changes to existing rules on which the agency does not expect adverse comment.

(b) The **Federal Register** document will state that any adverse comment or notice of intent to submit adverse comment must be received in writing by NHTSA within the specified time after the date of publication of the direct final rule and that, if no written adverse comment or written notice of intent to submit adverse comment is received in that period, the rule will become effective a specified number of days after the date of publication of the direct final rule.

(c) If no written adverse comment or written notice of intent to submit adverse comment is received by NHTSA within the specified time after the date of publication in the **Federal Register**, NHTSA will publish a notice in the **Federal Register** indicating that no adverse comment was received and confirming that the rule will become effective on the date that was indicated in the direct final rule.

(d) If NHTSA receives any written adverse comment or written notice of intent to submit adverse comment within the specified time after publication of the direct final rule in the **Federal Register**, the agency will publish a notice withdrawing the direct final rule, in whole or in part, in the final rule section of the **Federal Register**. If NHTSA decides to proceed with a provision on which adverse comment was received, the agency will publish a notice of proposed rulemaking in the proposed rule section of the **Federal Register** to provide another opportunity to comment.

(e) An ''adverse'' comment, for the purpose of this subpart, means any comment that NHTSA determines is critical of any provision of the rule, suggests that the rule should not be adopted, or suggests a change that should be made in the rule. A comment suggesting that the policy or requirements of the rule should or should not also be extended to other Departmental programs outside the scope of the rule is not adverse.

■ 3. In § 553.15, revise paragraphs (a), (b)(1) and (b)(3) to read as follows:

§ 553.15 Contents of notices of proposed rulemaking and direct final rules.

(a) Each notice of proposed rulemaking, and each direct final rule, is published in the **Federal Register**, unless all persons subject to it are named and are personally served with a copy of it.

(b) * * *

(1) A statement of the time, place, and nature of the rulemaking proceeding;

* * * * *

(3) A description of the subjects and issues involved or the substance and terms of the rule;

* * * * *

■ 4. Revise § 553.23 to read as follows:

§ 553.23, Consideration of comments received.

All timely comments are considered before final action is taken on a rulemaking proposal or direct final rule. Late filed comments will be considered to the extent practicable.

Issued in Washington, DC on March 19, 2013, under authority delegated in 49 CFR part 1.95.

Christopher J. Bonanti,

Associate Administrator for Rulemaking.

[FR Doc. 2013–06724 Filed 3–25–13; 8:45 am]

BILLING CODE 4910–59–P

DEPARTMENT OF HOMELAND SECURITY

Transportation Security Administration

49 CFR Part 1540

[Docket No. TSA–2013–0004]

RIN 1652–AA67

Passenger Screening Using Advanced Imaging Technology

AGENCY: Transportation Security Administration, DHS.

ACTION: Notice of proposed rulemaking (NPRM).

SUMMARY: The Transportation Security Administration (TSA) is proposing to revise its civil aviation security regulations to clarify that TSA may use advanced imaging technology (AIT) to screen individuals at security screening checkpoints. This proposed rule is issued to comply with a decision of the U.S. Court of Appeals for the District of Columbia Circuit, which ordered TSA to engage in notice-and-comment rulemaking on the use of AIT for screening. The Court decided that TSA should provide notice and invite comments on the use of AIT technology for primary screening.

DATES: Submit comments by June 24, 2013.

ADDRESSES: You may submit comments, identified by the TSA docket number to this rulemaking, to the Federal Docket Management System (FDMS), a government-wide, electronic docket management system, using any one of the following methods:

Electronically: You may submit comments through the Federal eRulemaking portal at *http://www.regulations.gov.* Follow the online instructions for submitting comments.

Mail, In Person, or Fax: Address, hand-deliver, or fax your written comments to the Docket Management Facility, U.S. Department of Transportation, 1200 New Jersey Avenue SE., West Building Ground Floor, Room W12–140, Washington, DC 20590–0001; fax (202) 493–2251. The Department of Transportation (DOT), which maintains and processes TSA's official regulatory dockets, will scan the submission and post it to FDMS.

See **SUPPLEMENTARY INFORMATION** for format and other information about comment submissions.

FOR FURTHER INFORMATION CONTACT: Chawanna Carrington, Project Manager, Passenger Screening Program, Office of Security Capabilities, Transportation Security Administration, 701 South 12th Street, Arlington, VA 20598–6016; telephone: (571) 227–2958; facsimile: (571) 227–1931; email: *Chawanna.Carrington@tsa.dhs.gov.*

SUPPLEMENTARY INFORMATION:

Comments Invited

TSA invites interested persons to participate in this rulemaking by submitting written comments, data, or views. We also invite comments relating to the economic, environmental, energy, or federalism impacts that might result from this rulemaking action. See **ADDRESSES** above for information on where to submit comments.

With each comment, please identify the docket number at the beginning of your comments. TSA encourages commenters to provide their names and addresses. The most helpful comments reference a specific portion of the rulemaking, explain the reason for any recommended change, and include supporting data. You may submit comments and material electronically, in person, by mail, or fax as provided under **ADDRESSES**, but please submit your comments and material by only one means. If you submit comments by mail or delivery, submit them in an unbound format, no larger than 8.5 by 11 inches, suitable for copying and electronic filing.

If you would like TSA to acknowledge receipt of comments submitted by mail, include with your comments a self-addressed, stamped postcard on which the docket number appears. We will stamp the date on the postcard and mail it to you.

TSA will file all comments to our docket address, as well as items sent to the address or email under **FOR FURTHER INFORMATION CONTACT**, in the public docket, except for comments containing confidential information and sensitive security information (SSI).[1] Should you wish your personally identifiable information redacted prior to filing in the docket, please so state. TSA will consider all comments that are in the docket on or before the closing date for comments and will consider comments filed late to the extent practicable. The docket is available for public inspection before and after the comment closing date.

Handling of Confidential or Proprietary Information and Sensitive Security Information (SSI) Submitted in Public Comments

Do not submit comments that include trade secrets, confidential commercial or financial information, or SSI to the public regulatory docket. Please submit such comments separately from other comments on the rulemaking. Comments containing this type of information should be appropriately marked as containing such information and submitted by mail to the address listed in **FOR FURTHER INFORMATION CONTACT** section.

TSA will not place comments containing SSI in the public docket and will handle them in accordance with applicable safeguards and restrictions on access. TSA will hold documents containing SSI, confidential business information, or trade secrets in a separate file to which the public does not have access, and place a note in the public docket explaining that commenters have submitted such documents. TSA may include a redacted version of the comment in the public docket. If an individual requests to examine or copy information that is not in the public docket, TSA will treat it as any other request under the Freedom of Information Act (FOIA) (5 U.S.C. 552) and the FOIA regulations of the Department of Homeland Security (DHS) found in 6 CFR part 5.

Reviewing Comments in the Docket

Please be aware that anyone is able to search the electronic form of all comments in any of our dockets by the name of the individual who submitted the comment (or signed the comment, if an association, business, labor union, etc., submitted the comment). You may review the applicable Privacy Act System of Records Notice published in the **Federal Register** on April 11, 2000 (65 FR 19477) and modified on January 17, 2008 (73 FR 3316).

You may review TSA's electronic public docket on the Internet at *http://www.regulations.gov.* In addition, DOT's Docket Management Facility provides a physical facility, staff, equipment, and assistance to the public. To obtain assistance or to review comments in TSA's public docket, you may visit this facility between 9:00 a.m. to 5:00 p.m., Monday through Friday, excluding legal holidays, or call (202) 366–9826. This docket operations facility is located in the West Building Ground Floor, Room W12–140 at 1200 New Jersey Avenue SE., Washington, DC 20590.

Availability of Rulemaking Document

You can get an electronic copy using the Internet by—

(1) Searching the electronic FDMS Web page at *http://www.regulations.gov;*

(2) Accessing the Government Printing Office's Web page at *http://www.gpoaccess.gov/fr/index.html;* or

(3) Visiting TSA's Web site at *http://www.tsa.gov* and accessing the link for ''Stakeholders'' at the top of the Web page, selecting the link for ''Research Center'' in the left column, and then the link for ''Security Regulations'' in the left column.

In addition, copies are available by writing or calling the individual in the **FOR FURTHER INFORMATION CONTACT** section. Make sure to identify the docket number of this rulemaking.

Table of Contents

[1] ''Sensitive Security Information'' or ''SSI'' is information obtained or developed in the conduct of security activities, the disclosure of which would constitute an unwarranted invasion of privacy, reveal trade secrets or privileged or confidential information, or be detrimental to the security of transportation. The protection of SSI is governed by 49 CFR part 1520.

I. Executive Summary

A. Purpose of the Regulation

TSA is proposing to amend its regulations to specify that screening and inspection of an individual conducted to control access to the sterile area of an airport or to an aircraft may include the use of advanced imaging technology (AIT), also referred to as whole body imaging, as a screening method. Terrorists have repeatedly attempted to cause harm with the aid of weapons and devices smuggled aboard aircraft. It is the primary mission of DHS to prevent terrorist attacks within the United States and to reduce the vulnerability of the United States to terrorism.[2] The use of AIT is an important tool in accomplishing that mission.

This NPRM is being issued to comply with the decision rendered by the U.S. Court of Appeals for the District of Columbia Circuit in *Electronic Privacy Information Center* v. *U.S. Department of Homeland Security*.[3] In that case, the U.S. Court of Appeals directed TSA to conduct notice-and-comment rulemaking on the use of AIT as a screening method for passengers. The Court did not require TSA to stop using AIT to screen passengers, explaining that ''vacating the present rule would severely disrupt an essential security operation,'' and that the rule is ''otherwise lawful.''[4]

B. Summary of Major Provisions

The proposed rule codifies the use of AIT to screen individuals at aviation security screening checkpoints. This NPRM discusses the following points regarding the use of AIT:

- The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons.
- AIT currently provides the best available opportunity to detect non-metallic anomalies[5] concealed under clothing without touching the passenger and is an essential component of TSA's security layers.
- Congress has authorized TSA to procure and deploy AIT for use at security checkpoints.
- TSA implemented stringent safeguards to protect the privacy of passengers undergoing AIT screening when AIT units were initially deployed and enhanced privacy even further by upgrading its millimeter wave AIT units with automatic target recognition (ATR) software. An AIT unit equipped with ATR creates a generic outline, not an image of a specific individual, and eliminates the need for operator interpretation of an image. TSA is removing all units that are not equipped with ATR from its checkpoints by May 31, 2013.[6]
- The safety of the two types of AIT equipment initially deployed was tested by TSA and independent entities and all results confirmed that both the backscatter and millimeter wave technologies are safe because the x-ray or radio waves emissions are well below applicable safety and health standards, and are so low as to present a negligible risk to passengers, airline crew members, airport employees, and TSA employees.[7]
- TSA has provided a detailed explanation of AIT procedures on its webWeb site at *www.tsa.gov/ait-how-it-works* (which allows opt out procedures for passengers) and posted signs at airport checkpoints to notify passengers about AIT and alternative screening procedures. The level of acceptance by passengers has been high; the vast majority of passengers do not object to AIT screening.
- TSA's experience in using AIT confirms that it is effective in detecting small, non-metallic items hidden underneath passenger clothing that could otherwise escape detection. When an item is detected, additional screening must be performed to determine whether the item is prohibited.

C. Costs and Benefits

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. As the AIT machine life cycle from deployment to disposal is eight years, the period of analysis for estimating the cost of AIT is eight years. However, as AIT deployment began in 2008, there are costs that have already been borne by TSA, the traveling public, and airport operators that were not due to this rule. Consequently, in the Initial Regulatory Impact Analysis for this rule, TSA is reporting the AIT-related costs that have already occurred (years 2008–2011), while considering the additional cost of this rulemaking to be years 2012–2015. By reporting the costs that have already happened and estimating future costs in this manner, TSA considers and discloses the full eight-year life cycle of AIT deployment.

TSA reports that the net cost of AIT deployment from 2008–2011 has been $841.2 million (undiscounted) and that TSA has borne over 99 percent of all costs related to AIT deployment. TSA projects that from 2012–2015 net AIT-related costs will be approximately $1.5 billion (undiscounted), $1.4 billion at a three percent discount rate, and $1.3 billion at a seven percent discount rate. During 2012–2015, TSA estimates it will also incur over 98 percent of AIT-related costs with equipment and personnel costs being the largest categories of expenditures. Table 1 below reports the costs that have already occurred (2008–2011) by cost category, while Table 2 shows the additional costs TSA is attributing to this rulemaking (2012–2015). Table 3 shows the total cost of AIT deployment from 2008 to 2015.

TABLE 1—NET COST[8] SUMMARY OF AIT DEPLOYMENT FROM 2008–2011 BY COST COMPONENT

[Costs already incurred in $ thousands—undiscounted]

Year	Passenger opt outs	Industry utilities	TSA costs				Total
			Personnel	Training	Equipment	Utilities	
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$52,535.3
2009	32.2	5.7	15,618.6	88.0	42,563.6	20.4	58328.5
2010	262.2	158.2	247,566.7	5,332.8	119,105.4	241.4	372,666.6

[2] 49 U.S.C. 114.

[3] 653 F.3d 1 (DC Cir. 2011).

[4] *Id.* at 8.

[5] An anomaly is any object that would not ordinarily be found on someone's person.

[6] The manufacturer of these units will bear the costs of removal and storage. TSA is following the Federal Management Regulation process to transfer and donate this equipment to other DHS components and then to other Federal, State, and local government agencies, if necessary. TSA will not hold any public auction or sale and will not donate or abandon any of the equipment to the public in the interests of security.

[7] See, *http://www.tsa.gov/ait-safety.*

TABLE 1—NET COST [8] SUMMARY OF AIT DEPLOYMENT FROM 2008–2011 BY COST COMPONENT—Continued

[Costs already incurred in $ thousands—undiscounted]

Year	Passenger opt outs	Industry utilities	TSA costs				Total
			Personnel	Training	Equipment	Utilities	
2011	1,384.2	186.7	284,938.7	15,354.4	55,567.2	269.1	357,700.2
Total	1,685.6	356.3	562,813.0	21,164.7	254,661.3	549.6	841,230.6

[8] TSA removed costs related to Walk Through Metal Detectors (WTMDs) that would have occurred regardless of AIT deployment to obtain an estimated net cost for AIT.

TABLE 2—COST SUMMARY (NET COST OF AIT DEPLOYMENT 2012–2015) BY COST COMPONENT

[AIT Costs in $ thousands]

Year	Passenger Opt Outs	Industry Utilities	TSA Costs				Rapiscan Removal	Total
			Personnel	Training	Equipment	Utilities		
2012	$2,716.5	$325.7	$375,886.9	$12,043.0	$116,499.3	$473	$0.0	$507,924.4
2013	3,991.7	329.3	280,844.3	4,277.5	51,588.8	324.4	1,809.6	343,165.7
2014	4,238.7	312.0	263,677.6	4,190.5	51,397.8	317.7	0.0	324,134.2
2015	5,611.8	300.3	278,580.2	4,144.2	68,052.6	365.7	0.0	357,054.9
Total	16,558.7	1,267.3	1,198,969.0	24,655.2	287,538.5	1,480.9	1,809.6	1,532,279.2
Discounted 3%	15,265.0	1,178.9	1,118,459.3	23,810.2	269,233.7	1,380.7	1,705.7	1,431,033.5
Discounted 7%	13,766.6	1,075.8	1,024,344.7	22,048.8	247,810.4	1,263.8	1,580.6	1,311,890.7

TABLE 3—COST SUMMARY (NET COST OF AIT DEPLOYMENT 2008–2015) BY COST COMPONENT

[AIT Costs in $ thousands—undiscounted]

Year	Passenger opt outs	Industry utilities	TSA costs				Rapiscan removal	Total
			Personnel	Training	Equipment	Utilities		
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$0.0	$52,535.3
2009	32.2	5.7	15,618.6	88.0	42,563.6	20.4	0.0	58,328.5
2010	262.2	158.2	247,566.7	5,332.8	119,105.4	241.4	0.0	372,666.6
2011	1,384.2	186.7	284,938.7	15,354.4	55,567.2	269.1	0.0	357,700.2
2012	2,716.5	325.7	375,866.9	12,043.0	116,499.3	473.0	0.0	507,924.4
2013	3,991.7	329.3	280,844.3	4,277.5	51,588.8	324.4	1,809.6	343,165.7
2014	4,238.7	312.0	263,677.6	4,190.5	51,397.8	317.7	0.0	324,134.2
2015	5,611.8	300.3	278,580.2	4,144.2	68,052.6	365.7	0.0	357,054.9
Total	18,944.4	1,623.6	1,761,782.0	45,819.9	542,199.9	2,030.4	1,809.6	2,373,509.9

The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT that is capable of detecting both metallic and non-metallic weapons and explosives.[9] Terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives. AIT is a proven technology based on laboratory testing and field experience and is an essential component of TSA's security screening because it provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without the need to touch the passenger. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using the WTMD.

II. Background

A. The Evolving Threat to Aviation Security

The need for security screening at airports dates back to the 1960s when the most significant threat to aviation security was hijacking. To combat this threat, metal detectors were installed at airports and used by air carriers to detect firearms and other metallic weapons. In 1974, Congress passed the Air Transportation Security Act,[10] which directed the Federal Aviation Administration (FAA) to require all passengers to be screened by weapon-detecting devices, and conduct research to develop and evaluate systems, procedures, facilities, and devices to protect persons and property aboard aircraft. Since that time, technological and procedural improvements have been implemented to keep pace with evolving threats.

Following the events of September 11, 2001, it was clear that the security screening at airports was insufficient to protect the traveling public against the threat posed by Al Qaeda and other terrorists who sought to harm the United States by targeting civil aviation. In response to those events, TSA was created to ensure freedom of movement

[9] Metal detectors and AITs are both designed to detect metallic threats on passengers, but go about it in different ways. Metal detectors rely on the inductance that is generated by the metal, while AIT relies on the metal's reflectivity properties to indicate an anomaly. AIT capabilities exceed metal detectors because AIT can detect metallic/non-metallic weapons, non-metallic bulk explosives, and non-metallic liquid explosives.

[10] Public Law 93–366.

for people and commerce by preventing terrorist attacks, reducing the vulnerability of the United States to terrorism, and effectively securing all modes of transportation, including aviation.

Pursuant to law, TSA is required to ''provide for the screening of all passengers and property, including United States mail, cargo, carry-on and checked baggage, and other articles, that will be carried aboard a passenger aircraft * * *.'' [11] Regulations restricting the carriage of weapons, explosives, and incendiaries on an individual's person or accessible property and requiring individuals to submit to the screening and inspection of their person and accessible property prior to entering a sterile area or boarding an aircraft were transferred from FAA to TSA in February 2002.[12] TSA took over operation of the screening checkpoints from the air carriers and began instituting additional protocols and new equipment to detect individuals and items that could pose a threat to aviation security.

The FAA had begun exploring AIT in the mid-1990s and started testing and evaluating AIT in 2000. Once TSA was established, the evaluation of AIT and other technology that could detect metallic and non-metallic threats continued. TSA began testing early AIT equipment and protocols to evaluate the size of the units, image quality, detection capabilities, safety, and other operational issues.

Since September 11, 2001, the nature of the threat to transportation security has evolved as terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. As the recent instances described below demonstrate, non-metallic explosives have become one of the greatest threats to aviation security. TSA has responded to the developing threats by deploying new screening protocols and increasing its use of technology to improve its ability to detect weapons, explosives, and incendiaries.

On December 22, 2001, on board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe. Following this terrorist attempt, screening procedures were revised by enhancing the screening of footwear.

In 2004, terrorists mounted a successful attack on two domestic Russian passenger aircraft using explosives that were concealed on the torsos of female passengers. TSA responded to this demonstrated security vulnerability by implementing a variety of enhancements to its standard operating procedures. Revised pat-down protocols that increased the thoroughness of pat-downs on the female torso were among the enhancements implemented to improve the ability to detect explosives concealed on the body.

In 2006, terrorists in the United Kingdom plotted to bring on board aircraft liquid explosives that would be used to construct and detonate a bomb while in flight. Following this threat, TSA again adjusted its security procedures by limiting the amount of liquids that could be brought on board aircraft and enhancing the screening of liquids, aerosols, and gels. TSA also deployed technology to improve detection of liquid explosives.

On December 25, 2009, a bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in Umar Farouk Abdulmutallab's attempt to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear. TSA's pat-down procedures then in effect may not have detected the device. TSA modified its screening procedures to improve its ability to detect explosives hidden in an area of the body that previously was not thoroughly searched and hastened to expand deployment of AIT to improve its ability to detect non-metallic explosives concealed on the body through the use of technology, rather than the pat-down.[13]

In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges. TSA immediately instituted new screening requirements for cargo bound for the United States.

In May 2012, AQAP developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft. Fortunately, this device was obtained by an undercover operative and was not given to a potential suicide bomber. The device was provided to the Federal Bureau of Investigation for technical and forensic analysis and the results indicate that terrorists have modified certain characteristics of the bomb in comparison with the December 25, 2009 bomb in an attempt to avoid the 2009 bombing attempt's design failure.

As evidenced by the incidents described above, TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. The device used in the December 25, 2009 attempt is illustrative. It was cleverly constructed and intentionally hidden on a sensitive part of the body to avert detection. If this attack were successful as planned, the lives of the almost 300 passengers and crew and potentially people on the ground would have been in jeopardy.

As these examples of the real and ever-evolving threats to aviation security demonstrate, non-metallic explosives are now one of the foremost known threats to passenger aircraft. The best defense against these and other terrorist threats remains a risk-based, layered security approach that uses a range of screening measures, both seen and unseen. This includes the use of AIT, which is proven technology for identifying non-metallic explosives during passenger screening, such as the device Umar Farouk Abdulmutallab attempted to detonate on Christmas Day 2009. TSA requests comment on the threat to aviation security described above and the risk-based, layered security approach it has adopted.

B. Layers of Security

TSA deploys approximately 50,000 Transportation Security Officers (TSOs) at more than 446 domestic airports with over 700 security checkpoints to screen nearly 2 million passengers each day using various screening methods and technologies. Although the airport checkpoints are the most visible layer of security used by TSA, TSA also relies extensively on intelligence regarding potential and actual terrorist threats to inform and identify what security measures are necessary to meet the nature of those threats. Other security layers include checking passenger manifests against records from the Government known or suspected terrorist watch lists through TSA's Secure Flight program, examining identity and travel documents, using explosives detection systems, and conducting random security operations at the checkpoint and throughout the airport.

Because even the best intelligence does not identify in advance every individual who would seek to do harm to passengers, aviation security, and the United States, TSA must rely on the security expertise of its frontline personnel—TSOs, Federal Air Marshals, Transportation Security Specialists-Explosives, Behavior Detection Officers,

[11] 49 U.S.C. 44901.

[12] *See* 49 CFR 1540.107 and 1540.111.

[13] On January 7, 2010, the President issued a ''Presidential Memorandum Regarding 12/25/2009 Attempted Terrorist Attack,'' which charged TSA with aggressively pursuing enhanced screening technology in order to prevent further such attempts, while at the same time protecting passenger privacy. A copy of that memorandum is available in the docket for this rulemaking and can be found at *http://www.whitehouse.gov/the-press-office/presidential-memorandum-regarding-12252009-attempted-terrorist-attack.*

and explosives detection canine teams, among others—to help prevent acts of terrorism.

Effective technology is an essential component of TSA's arsenal of tools to detect and deter threats against our nation's transportation systems. Since its creation, TSA has deployed an increasingly sophisticated range of next generation detection equipment—including bottled liquid scanners, advanced technology x-ray systems, explosives trace detection (ETD) units, and AIT—as the threats to aviation security change and become more sophisticated. As recent history illustrates, TSA changes its screening equipment and procedures as needed to respond to evolving threats based on experience and the latest intelligence. TSA's layered approach and its ability to deploy new security methods to respond to the latest threats are necessary to provide adequate security for the traveling public. Advanced Imaging Technology currently provides the best opportunity to detect metallic and non-metallic threats concealed on the body under clothing without physical contact.[14]

C. Congressional Direction To Pursue AIT

In 2004, Congress directed TSA to continue to explore the use of new technologies to improve its threat detection capabilities.[15] Specifically, the law provides:

Deployment and use of detection equipment at airport screening checkpoints

- Weapons and explosives.—The Secretary of Homeland Security shall 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 * * * the types of weapons and explosives that terrorists would likely try to smuggle aboard an air carrier aircraft.
- [The TSA Administrator shall submit] * * * a strategic plan to promote the optimal utilization and deployment of explosive detection equipment at airports to screen individuals and their personal property. Such equipment includes walk-through explosive detection portals, document scanners, shoe scanners, and backscatter x-ray scanners.

Additional references in congressional reports accompanying appropriations and authorizing legislation demonstrate Congress' continued direction to DHS and TSA to pursue enhanced screening technologies and imaging technology, including:

(1) Explanatory Statement, House Appropriations Committee Print for Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009 (FY09 DHS Appropriations) Pub. L. 110–329 at p. 640:

The bill provides $250,000,000 for Checkpoint Support to deploy a number of emerging technologies to screen airline passengers and carry-on baggage for explosives, weapons, and other threat objects by the most advanced equipment currently under development. TSA is directed to spend funds on multiple whole body imaging technologies including backscatter and millimeter wave as directed in the Senate report.

(2) H. Rep. 110–862 at p. 64, FY09 DHS Appropriations:

Over the past year, TSA has made some advances in testing, piloting, and deploying next-generation checkpoint technologies that will be used to screen airline passengers and carry-on baggage for explosives, weapons, and other threats. Even with this progress, however, additional funding is necessary to expedite pilot testing and deployment of advanced checkpoint explosive detection equipment and screening techniques to determine optimal deployment as well as preferred operational and equipment protocols for these new systems. Eligible systems may include, but are not limited to, advanced technology screening systems; whole body imagers; * * * The Committee expects TSA to give the highest priority to deploying next-generation technologies to designated Tier One threat airports.

(3) S. Rep. 110–396 at p. 60, FY09 DHS Appropriations:

WHOLE BODY IMAGERS. The Committee is fully supportive of emerging technologies at passenger screening checkpoints, including the whole body imaging program currently underway at Category X airports. These technologies provide an increased level of screening for passengers by detecting explosives and other non-metal objects that current checkpoint technologies are not capable of detecting. The Committee directs that funds for whole body imaging continue to be spent by TSA on multiple imaging technologies, including backscatter and millimeter wave.

(4) H. Rep.110–259, at Web page 363, Conference Report to Implementing Recommendations of 9/11 Commission Act of 2007, Pub. L. 110–53, sec. 1601—Airport checkpoint screening fund:

The National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission) asserted that while more advanced screening technology is being developed, Congress should provide funding for, and TSA should move as expeditiously as possible to support, the installation of explosives detection trace portals or other applicable technologies at more of the nation's commercial airports. Advanced technologies, such as the use of non-intrusive imaging, have been evaluated by TSA over the last few years and have demonstrated that they can provide significant improvements in threat detection at airport passenger screening checkpoints for both carry-on baggage and the screening of passengers. The Conference urges TSA to deploy such technologies quickly and broadly to address security shortcomings at passenger screening checkpoints.[16]

D. U.S. Court of Appeals Decision in EPIC v. DHS

In July 2010, the EPIC petitioned the U.S. Court of Appeals for the District of Columbia Circuit for review of TSA's use of AIT as a primary screening device to screen airline passengers. EPIC argued that the use of AIT violated various federal statutes and the Fourth Amendment to the Constitution and should have been the subject of notice-and-comment rulemaking.

The Court of Appeals issued a decision on July 15, 2011, which rejected nearly all of EPIC's claims.[17] In ruling on EPIC's Fourth Amendment claim, the Court held that screening passengers at an airport is an administrative search that does not rely on individualized suspicion. ''Instead, whether an administrative search is 'unreasonable' within the condemnation of the Fourth Amendment 'is determined by assessing, on the one hand, the degree to which it intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests'.'' [18]

The Court found that the ''balance clearly favors the Government here.'' [19] The Court recognized the clear need for AIT screening, and the advantages the AIT provides over the WTMD. The Court stated that ''[t]he need to search

[14] In September 2012, TSA initiated a limited procurement for next generation AIT units for the purpose of testing such units in a laboratory environment. The outcome of the testing will determine if the units will proceed to testing in an airport environment. TSA anticipates that next generation AIT units will have enhanced detection capabilities, faster passenger throughput, and a smaller footprint.

[15] 49 U.S.C. 44925.

[16] *See also,* sec. 109 of the Aviation and Transportation Security Act (ATSA), Public Law 107–71 (2001), as amended by sec. 1403(b) of the Homeland Security Act of 2002, Public Law 107–296, ''(7) Provide for the use of voice stress analysis, biometric, or other technologies to prevent a person who might pose a danger to air safety or security from boarding the aircraft of an air carrier or foreign air carrier in air transportation or intrastate air transportation'' and Title IV of the American Recovery and Reinvestment Act of 2009, Public Law 111–5 ''* * * for procurement and installation of checked baggage explosives detection systems and checkpoint explosives detection equipment.''

[17] *Electronic Privacy Information Center* v. *U.S. Department of Homeland Security,* 653 F.3d 1 (D.C. Cir. 2011).

[18] *Id.* at 10 (quoting *United States* v. *Knights,* 534 U.S. 112, 118–119 (2001)).

[19] *Id.*

airline passengers 'to ensure public safety can be particularly acute' and, crucially, an AIT scanner, unlike a magnetometer, is capable of detecting, and therefore of deterring, attempts to carry aboard airplanes explosives in liquid or powder form.'' [20]

As explained in the decision, the AIT scanners then in use produce a ''crude image of an unclothed person * * *.''[21] In rejecting EPIC's privacy argument, the Court recognized that TSA has taken steps:

[T]o mitigate the effect a scan using AIT might have upon passenger privacy: Each image produced by a scanner passes through a filter to obscure facial features and is viewable on a computer screen only by an officer sitting in a remote and secure room. As soon as the passenger has been cleared, moreover, the image is deleted; the officer cannot retain the image on his computer, nor is he permitted to bring a cell phone or camera into the secure room.[22]

The Court also noted that three Privacy Impact Assessments (PIAs) of the AIT program had been completed and were sufficient. ''[T]he petitioners make no more specific objection that would enable us to disturb the [Chief Privacy Officer's] conclusion that the privacy protections built into the AIT program are sufficiently 'strong'.'' [23]

In its decision, the Court acknowledged that Congress authorized TSA to prescribe the details of the screening process. The Court noted that ''Congress did * * * in 2004, direct the TSA to 'give a high priority to developing, testing, improving, and deploying' at airport screening checkpoints a new technology 'that detects nonmetallic, chemical, biological, and radiological weapons, and explosives, in all forms'.'' [24] The Court observed that TSA responded to this directive through the development and procurement of AIT scanners, which enable the operator of the machine to detect non-metallic objects, such as a liquid or powder, which a metal detector cannot detect, without touching the passengers coming through the checkpoint.[25]

TSA tested the use of AIT machines in 2009 for primary screening at a limited number of airports. The Court acknowledged that ''based on the apparent success of the test, the TSA decided early in 2010 to use the scanners everywhere for primary screening.'' [26] The Court also pointed out that passengers are not required to go through the AIT screening process. The Court stated ''no passenger is ever required to submit to an AIT scan * * * [and] signs at the security checkpoint notify passengers they may opt instead for a patdown.'' [27] The Court also rejected EPIC's claims that the AIT is unlawful under the Video Voyeurism Prevention Act and the Religious Freedom Restoration Act.

In ruling on EPIC's Administrative Procedure Act claim, the Court determined that TSA did not justify ''its failure to initiate notice-and-comment rulemaking before announcing it would use AIT scanners for primary screening.'' [28] Even though privacy precautions had been implemented, the Court stated ''it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon * * * personal privacy in a way a magnetometer does not.'' [29] Thus, the Court found the use of the AIT in primary screening ''substantively affects the public to a degree sufficient to implicate the policy interests animating notice-and-comment rulemaking.'' [30] The Court did not require TSA to stop using AIT. ''[D]ue to the obvious need for the TSA to continue its airport security operations without interruption, we remand the rule to the TSA but do not vacate it * * *.'' [31]

III. AIT Screening Protocols

A. Types of AIT Equipment

TSA engaged in extensive laboratory and operational testing before approving the two types of AIT equipment initially deployed. In February 2007, TSA initiated a pilot operation at an airport to test AIT detection capability in the secondary screening position for aviation passengers who set off the alarm of the WTMD. In January 2008, TSA published a PIA to cover AIT screening of all passengers at the security screening checkpoint. Throughout 2007 and 2008, additional AIT units were tested in the secondary screening position and TSA continued to evaluate different types of AIT equipment, including both general-use x-ray backscatter and millimeter wave. In 2009, TSA began to evaluate using AIT in the primary screening position as an alternative to WTMD.[32] Deploying AIT in the primary position to screen all passengers for both metallic and non-metallic threats allows TSA to use the technology to its full capability. In February 2010, TSA submitted a report to Congress on privacy protections and deployment of AIT.[33]

TSA has compared AIT to other transportation security equipment and manual processes, including ETD, WTMD, and pat-downs. Based on the testing results, TSA determined that AIT currently offers the best opportunity to detect both metallic and non-metallic threat items concealed underneath clothing, such as the explosives carried by Mr. Abdulmutallab, without physical contact.

One type of AIT equipment initially deployed by TSA, the Rapiscan Secure 1000, uses backscatter technology. Unlike a traditional x-ray machine, which relies on the transmission of x-rays through an object, general-use backscatter technology projects low level x-ray beams over the body surface at high speed. The reflection or ''backscatter'' of the beam is detected and digitized to create an image.[34]

The L–3 ProVision, another type of AIT equipment currently deployed by TSA, uses millimeter-length radio waves. Millimeter wave technology bounces electromagnetic waves off of the human body to detectors in the machine, which a computer then interprets in order to create a black and white image.[35]

Working with the DHS Science & Technology Directorate and private industry, TSA began testing ATR software in 2010. Automatic Target Recognition software generates a generic outline and not an individual image.[36]

[20] *Id.* (quoting *City of Indianapolis* v. *Edmond,* 531 U.S. 32, 47–48) (internal citation omitted).

[21] *Id.* at 3.

[22] *Id.* at 4.

[23] *Id.* at 9.

[24] *Id.* at 3 (quoting sec. 4013 of the Intelligence Reform and Terrorism Prevention Act of 2004, Pub. L. 108–458, 118 Stat. 3719).

[25] *Id.*

[26] *Id.*

[27] *Id.*

[28] *Id.*

[29] *Id.* at 6.

[30] *Id.*

[31] *Id.* at 8.

[32] In addition to the AIT equipment described below, TSA evaluated infrared (IR) technology, which scans for temperature differences on the body's surface or for temperature imbalances between the body, clothes, and any hidden objects.

[33] ''Advanced Imaging Technologies: Passenger Privacy Protections,'' Fiscal Year 2010 Report to Congress, February 25, 2010.

[34] An example of the image produced by the backscatter technology is posted on TSA's Web site at *http://www.tsa.gov/travelers-guide/ait-how-it-works.*

[35] See ''Safety of AIT'' for a discussion of the safety of the millimeter wave equipment. The Food and Drug Administration has found that millimeter wave is safe and states on its Web site that ''[m]illimeter wave security systems which comply with the limits set in the applicable national non-ionizing radiation safety standard * * * cause no known adverse health effects.'' *http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm#2.*

[36] Examples of the generic outline that the ATR software produces are available on TSA's Web site at *http://www.tsa.gov/travelers-guide/ait-how-it-works.*

In July 2011, TSA began installing ATR software on millimeter wave AIT units and completed installation on all millimeter wave units currently in use. This advancement significantly enhances privacy by eliminating the passenger-specific images referred to in the *EPIC* v. *DHS* decision.

As part of the Federal Aviation Administration Modernization and Reform Act of 2012, Congress mandated that all AIT units must be equipped with ATR by June 1, 2012.[37] As permitted by law, the deadline was extended to June 1, 2013. While all of the millimeter wave units have been equipped with the ATR software, Rapiscan was unable to develop ATR software that would work on the general-use backscatter units. As a result, TSA terminated its Rapiscan ATR delivery order and all Rapiscan general-use backscatter AIT units currently deployed at TSA checkpoints are being removed from operation by Rapiscan.[38] By June 1, 2013, only AIT equipped with ATR will be used at TSA checkpoints.

TSA will continue to evaluate current AIT systems and associated screening procedures, as well as any new technologies and procedures that may be considered for deployment, to ensure that they are safe and meet all relevant government and consensus industry standards, are effective against established and anticipated threats, and require the least disruption and intrusion on passenger privacy possible.

B. Privacy Safeguards for AIT

The use of ATR software enhances passenger privacy by eliminating images of individual passengers, as well as the need for a TSO to view the individual images to identify anomalies.[39] Automatic Target Recognition software auto-detects anomalies concealed on the body and displays these on a generic outline, which is viewable on a screen located on the AIT equipment. These anomalies are then resolved through additional screening. Automatic Target Recognition-enabled units deployed at airports are not capable of storing or printing the generic outline that will be visible to passengers. TSA has installed the software on all currently-deployed millimeter wave units. As noted above, AIT units without ATR software are being removed from operation and only ATR-equipped AIT units will be used at the checkpoint as of June 1, 2013.

Section 222 of the Homeland Security Act requires that the Privacy Office assure that the use of technologies sustain and do not erode privacy protections relating to the use, collection, and disclosure of personal information, and to conduct a privacy impact assessment (PIA) for proposed rules impacting the privacy of personal information (6 U.S.C. 142). Even before the development of the ATR software, TSA instituted rigorous safeguards to protect the privacy of individuals who are screened using AIT. In addition, as noted by the Court in *EPIC* v. *DHS,* the DHS Chief Privacy Officer has conducted several PIAs on the use of AIT equipment to ensure that the public's privacy concerns related to AIT screening are adequately addressed. These PIAs meet the requirements of section 222 for this NPRM and describe the strict measures TSA uses to protect privacy.[40] To the extent that TSA receives substantive comments on privacy issues related to the use of AIT, they will be addressed in the final rule and any resulting changes will be addressed appropriately in a revised PIA.

While graphic images purportedly from TSA's AIT machines have been circulated in the media, those images were not the type produced by TSA's AIT equipment. Neither of the AIT technologies that have been used by TSA produced photographs or images that would enable personal identification. As deployed by TSA, neither technology is able to store, print, or export any image.

When using the backscatter technology, TSA requirements dictated that a filter be applied to prevent a detailed image of an individual. In addition, the images were viewed by a trained TSO in a locked, remote location. The anonymity of the individual being screened was preserved, since the TSO assisting the individual at the AIT unit never saw the image, and the TSO viewing the image never saw the individual being screened. No TSA personnel were permitted to view both the image and the individual. The backscatter units did not store, print, or export any images. Storage capability was disabled prior to deployment, and TSA airport personnel were not able to activate the storage capability. In addition, the backscatter images were transmitted securely between the unit and the viewing room so they could not be lost, modified, or disclosed. The images produced by the backscatter units were encrypted during transmission. The images were deleted from the screen in the viewing room when the individual was cleared. TSOs in the viewing room were prohibited from bringing electronic devices such as cameras, cell phones, or other recording devices into the room. Violations of these procedures subjected the TSO to disciplinary action, which included termination.

To give further effect to the Fair Information Practice Principles that are the foundation for privacy policy and implementation at DHS, individuals may opt-out of the AIT in favor of physical screening. TSA provides notice of the use of AIT and the opt-out option at the checkpoint so that individuals may exercise an informed judgment on AIT. Signs are posted that explain the technology and state ''use of this technology is optional. If you choose not to be screened by this technology you will receive a thorough pat down.''[41] TSA requests comment on the privacy safeguards discussed above and on the ability of passengers to opt-out of AIT screening.

C. Safety of AIT

AIT equipment has been subject to extensive testing that has confirmed that it is safe for individuals being screened, equipment operators, and bystanders.[42] The exposure to ionizing x-ray beams emitted by the backscatter machines that are being removed pursuant to statute, as well as the non-ionizing electromagnetic waves from the millimeter wave machines is well within the limits allowed under relevant national health and safety standards. Prior to procuring and deploying both backscatter and millimeter wave AIT equipment, TSA tested the units to determine whether they would be safe for use in passenger screening. As explained further below, TSA determined that the general-use backscatter and millimeter wave technologies were safe for use in screening the public because the x-ray and radio waves emissions were so low as to present a negligible risk to passengers, airline crew members, airport employees, and TSA employees.

1. Millimeter Wave Units

The millimeter wave AIT systems that will be the only technology deployed at

[37] Public Law 112–95.

[38] *http://blog.tsa.gov/2013/01/rapiscan-backscatter-contract.html.*

[39] Before the installation of ATR software, TSA required that all millimeter wave machines blur the face of the passenger.

[40] The most recent update to the PIA is posted on the DHS Web site at *http://www.dhs.gov/xlibrary/assets/privacy/privacy-pia-tsa-ait.pdf* and is available in the docket for this rulemaking.

[41] See AIT Signs at *http://www.tsa.gov/ait-how-it-works.*

[42] See AIT: Safety at *http://www.tsa.gov/ait-safety.*

the checkpoint as of June 1, 2013 use non-ionizing radio frequency energy in the millimeter wave spectrum to generate a three-dimensional image based on the energy reflected from the body. Millimeter wave imaging technology meets all known national and international health and safety standards. In fact, the energy emitted by millimeter wave technology is 1,000 times less than the international limits and guidelines. The millimeter wave AIT systems that TSA uses must comply with the 2005 Institute of Electrical and Electronics Engineers, Inc. Standard for Safety Levels with Respect to Human Exposure to Radio Frequency Electromagnetic Fields (IEEE Std. C95.1™–2005) as well as the International Commission on Non-Ionizing Radiation Protection Guidelines for Limiting Exposure to Time-Varying Electric, Magnetic, and Electromagnetic Fields, Health Physics 74(4); 494–522, published April 1998. TSA's millimeter wave units are also consistent with Federal Communications Commission OET Bulletin 65, Health Canada Safety Code 6, and RSS–102 Issue 3 for Canada. The FDA has also confirmed that millimeter wave security systems that comply with the IEEE Std. C95.1™–2005 cause no known adverse health effects.[43]

2. Backscatter Units

As required by statute, TSA will remove all currently deployed Rapiscan backscatter units by May 31, 2013. When in use, TSA addressed potential health concerns regarding the ionizing radiation emitted by general-use backscatter technology. TSA's procurement specifications required that the backscatter units must conform to the consensus radiation safety standard of the American National Standards Institute (ANSI)[44] and Health Physics Society (HPS)[45] for the design and operation of security screening systems that use ionizing radiation. That standard is ANSI/HPS N43.17, which was first published in 2002 and revised in 2009.[46]

The annual dose limits in ANSI/HPS N43.17 are based on dose limit recommendations for the general public published by the National Council on Radiation Protection and Measurements[47] in Report 116, ''Limitations of Exposure to Ionizing Radiation.''[48] The dose limits were set with consideration given to individuals, such as pregnant women, children, and persons who receive radiation treatments, who may be more susceptible to radiation health effects. Further, the standard also takes into consideration the fact that individuals are continuously exposed to ionizing radiation from the environment. ANSI/HPS N43.17 sets the maximum permissible dose of ionizing radiation from a general-use system per security screening at 0.25 microsieverts.[49] The standard also requires that individuals should not receive 250 microsieverts or more from a general-use x-ray security screening system in a year.

The radiation dose (effective dose) a passenger receives from a general-use backscatter AIT screening has been independently evaluated by the Food and Drug Administration's (FDA's) Center for Devices and Radiological Health, the National Institute for Standards and Technology, and the Johns Hopkins University Applied Physics Laboratory. All results affirmed that the effective dose for individuals being screened, operators, and bystanders was well below the dose limits specified by ANSI/HPS N43.17.[50] These results were confirmed in a report issued by the DHS Office of Inspector General (OIG) in February 2012.[51] The OIG report found that the independent surveys show that backscatter radiation levels are below the established limits and that TSA complied with ANSI/HPS N43.17.

Typical doses from backscatter machines are no more than 0.05 microsieverts per screening, well below the ANSI/HPS N43.17 maximum dosage of 0.25 microsievert per screening. An individual would have to have been screened by the Rapiscan Secure 1000 more than 13 times daily for 365 consecutive days before exceeding the ANSI/HPS standard.

By comparison, a traveler would have to be screened via Rapiscan/backscatter AIT 2,000 times to equal the dosage received in a single chest x-ray, which delivers 100 microsieverts of ionizing radiation. A typical bite-wing dental x-ray of 5 microsieverts would be equivalent to 100 backscatter screenings, and a two-view mammogram that delivers 360 microsieverts would be equivalent to 7,200 backscatter screenings.[52] A passenger flying one-way from Washington, DC to Los Angeles is exposed to approximately 19.1 microsieverts of ionizing radiation over the course of the 4.7 hour flight.[53]

ANSI/HPS also reflects the standard for a negligible individual dose of radiation established by the National Council on Radiation Protection and Measurements at 10 microsieverts per year. Efforts to reduce radiation exposure below the negligible individual dose are not warranted because the risks associated with that level of exposure are so small as to be indistinguishable from the risks attendant to environmental radiation that individuals are exposed to every day.[54] The level of radiation issued by the Rapiscan Secure 1000 is so low that most passengers would not have exceeded even the negligible individual

[43] *http://www.fda.gov/Radiation-EmittingProducts/RadiationEmittingProductsandProcedures/SecuritySystems/ucm227201.htm.*

[44] ANSI is a private, non-profit organization that administers and coordinates the U.S. voluntary standards and conformity assessment system. The Institute oversees the development and use of voluntary consensus standards by providing neutral, third-party accreditation of the procedures used by standards developing organizations, and approving their documents as American National Standards.

[45] HPS is a scientific organization of professionals who specialize in radiation safety. Its mission is to support its members and to promote excellence in the science and practice of radiation safety. As an independent nonprofit scientific organization, HPS is not affiliated with any government or industrial organization or private entity.

[46] American National Standard, ''Radiation Safety for Personnel Security Screening Systems Using X-Ray or Gamma Radiation,'' ANSI/HPS N43.17 (2009); Health Physics Society, McLean, VA. Copies can be ordered at: *http://webstore.ansi.org/faq.aspx#resellers.*

[47] The National Council on Radiation Protection and Measurements was founded in 1964 by Congress to cooperate with the International Commission on Radiological Protection, the Federal Radiation Council, the International Commission on Radiation Units and Measurements, and other national and international organizations, both governmental and private, concerned with radiation quantities, units, and measurements as well as radiation protection.

[48] Copies of the report can be ordered at: *http://www.ncrppublications.org/Reports/116.*

[49] The biological effect of radiation is measured in sieverts. One sievert equals 1,000 millisieverts and one millisievert equals 1,000 microsieverts.

[50] TSA's Web site at *http://www.tsa.gov/travelers-guide/ait-safety* contains many articles and studies that discuss AIT safety, including a description of the built-in safety features of the Rapiscan Secure 1000, an Archives of Internal Medicine report on the risks of imaging technology, the FDA evaluation of backscatter technology, and other independent safety assessments of AIT.

[51] Department of Homeland Security, Office of Inspector General, ''Transportation Security Administration's Use of Backscatter Units,'' OIG–12–38, February 2012.

[52] HPS Fact Sheet: Radiation Exposure from Medical Exams and Procedures, January 2010, *http://hps.org/documents/Medical_Exposures_Fact_Sheet.pdf.*

[53] Federal Aviation Administration, ''What Aircrews Should Know About Their Occupational Exposure to Ionizing Radiation,'' DOT–FAA–AM–03–1 (October 2003) at p. 9. Available at: *http://www.faa.gov/data_research/research/med_humanfacs/oamtechreports/2000s/media/0316.pdf.*

[54] The World Health Organization estimates that each person is exposed, on average, to 2.4 millisieverts (*i.e.,* 2400 microsieverts) of ionizing radiation each year from natural sources. *www.who.int/ionizing_radiation/about/what_is_ir/en/index2.html.*

dose. In fact, an individual would have to be screened more than 200 times a year by a Rapiscan Secure 1000 before he or she would exceed the negligible individual dose and, even then, the exposure would be below the ANSI/HPS N43.17 standard.

The European Commission released a report conducted by the Scientific Committee on Emerging and Newly Identified Health Risks (SCENIHR) on the risks related to the use of security scanners for passenger screening that use ionizing radiation such as the general-use backscatter AIT machines.[55] The committee found no short term health effects that can result from the doses of radiation delivered by security scanners. In the long term, it found that the potential cancer risk cannot be estimated, but is likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources, and background risk due to other factors.

The ANSI/HPS N43.17 standard also requires that any general-use backscatter machine have safety interlocks to terminate emission of x-rays in the event of any system problem that could result in abnormal or unintended radiation emission. The Rapiscan Secure 1000 had three such features. First, the unit was designed to cease x-ray emission once the programmed scan motion ends. That feature could not be adjusted. Second, the unit was programmed to terminate emission once the requiWeb site number of lines of data necessary to create an image was received. Both of these automatic features reduced the possibility that emissions could continue if the unit malfunctions. Finally, the unit had an emergency stop button that would terminate x-ray emission.

Upon installation, a radiation emission survey was conducted on each Rapiscan Secure 1000 to ensure the unit operated properly. Preventive maintenance checks, including radiation safety surveys, were performed at least once every six months; after any maintenance that affected the radiation shielding, shutter mechanism, or x-ray production components; after any incident where damage was suspected; or after a unit was moved. The U.S. Army Public Health Command also conducted an independent radiation survey on deployed systems. The report confirmed that the general-use backscatter units tested were well within applicable national safety standards.[56]

The DHS Office of the Chief Procurement Officer is also requesting the National Academy of Sciences to review previous studies as well as the current processes used by DHS and equipment manufacturers to estimate radiation exposure resulting from general-use backscatter equipment and to provide a report on whether radiation exposures comply with applicable health and safety standards and whether system design operating procedures and maintenance procedures are appropriate.

D. AIT Procedures at the Checkpoint

TSA's regulations require that ''[i]ndividuals may not enter or be present within a secured area, air operations area, security identification display area, or sterile area without complying with the systems, measures, or procedures used to control access to such areas.'' [57] In addition, ''[i]ndividuals may not enter a sterile area or board an aircraft without submitting to the screening and inspection of their person and accessible property in accordance with the procedures being applied to control access to that area or the aircraft.'' [58] Federal law also requires that air carriers refuse to transport a passenger who does not consent to a search of his person or baggage,[59] and authorizes air carriers to refuse to transport a passenger or property the carrier decides is, or might be, inimical to safety.[60]

The specific security procedures, systems, or measures that TSA deploys are included in its Standard Operating Procedures (SOPs). The SOPs instruct the TSOs how to conduct the screening measures currently in use. Terrorists continue to seek ways to thwart aviation security measures and could use information on TSA procedures, such as the instructions on how to operate AIT equipment and the AIT equipment specifications, to plan and execute attacks. Therefore, the SOPs are SSI and are not made public as such disclosure would prove detrimental to transportation security.[61]

In response to the decision in *EPIC* v. *DHS,* TSA is proposing to add the following language to its current regulations at 49 CFR 1540.107, quoted above, to specifically address AIT screening:

(d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.

In addition, TSA has posted information on its Web site on what individuals can expect when submitting to AIT screening. AIT screening is currently optional, but when opting out of AIT screening, a passenger will receive a pat-down. When TSA deploys AIT equipment at a screening lane, a sign is posted to inform the public that AIT may be used as part of the screening process prior to passengers entering the machine so that each passenger may exercise an informed decision on the use of AIT. The sign also indicates that a passenger who chooses not to be screened by AIT will receive a pat-down. However, TSA has found that since 2009, fewer than two percent of passengers opt for a pat-down in lieu of AIT screening.[62]

TSA's Web site [63] explains that AIT looks for any items, both metallic and non-metallic, that might be anywhere on the body. It recommends that individuals remove all items from pockets and their person and place them in carry-on baggage prior to entering the checkpoint. It notes that removal will lessen the chance that additional screening will be required. The Web site also explains that for AIT units not equipped with ATR, the TSO who views the image cannot see the individual; while for AIT equipped with ATR software, the screen with the generic outline is located on the scanner and is visible to the passenger and the TSO. The Web site states that AIT is optional.

After any items are removed, individuals are directed to enter the

[55] The SCENIHR is an independent committee that provides the European Commission with the scientific advice it needs when preparing policy and proposals relating to consumer safety, public health and the environment. The committee is made up of external experts. The report can be found at *http://ec.europa.eu/health/scientific_committees/emerging/docs/scenihr_o_036.pdf.*

[56] The report is available on TSA's Web site at *http://www.tsa.gov/travelers-guide/ait-safety.*

[57] 49 CFR 1540.105(a)(2).

[58] 49 CFR 1540.107(a).

[59] 49 U.S.C. 44902(a), 49 CFR 1544.201(c).

[60] 49 U.S.C. 44902(b).

[61] SSI is defined in footnote 1.

[62] TSA's Web site describes the results of independent polling on AIT acceptance showing strong public support for and understanding of the need for AIT. See *http://www.tsa.gov/ait-more-information.* In addition, passengers with joint replacements or other medical devices that would regularly set off the alarm on a metal detector often prefer AIT because it is quicker and less invasive than a pat-down. See *http://www.tsa.gov/traveler-information/advanced-imaging-technology-ait.* An internet campaign in 2010 failed in an attempt to disrupt checkpoint operations by urging passengers to request a pat-down in lieu of AIT screening during the Thanksgiving holiday travel period. See ''Opt Out Turns Into Opt In,'' The TSA Blog, November 24, 2010, *http://blog.tsa.gov/2010_11_24_archive.html.*

[63] *http://www.tsa.gov/travelers-guide/ait-how-it-works.*

AIT. Once inside, individuals are directed to stand with arms raised, and to remain still for several seconds while the image is created. When using AIT with ATR, the image is not an image of the individual passenger, rather a generic outline that indicates where the anomaly is detected. Individuals are directed to exit the opposite side of the portal. Once the image is reviewed and any anomalies are resolved, the image is deleted. This process usually takes less than a minute.

TSA has also refined its procedures to make sure that the screening process addresses the needs of families. TSA never separates a child from an accompanying adult and makes sure that the accompanying adult observes the entire screening process. Advanced Imaging Technology is safe for children, and children may undergo screening using AIT as long as they are able to stand with their hands above their head for the five to seven seconds needed to conduct the scan. However, TSA no longer requires children who are 12 years old or younger to be screened by AIT and will direct those passengers to the WTMD unless instructed otherwise by an accompanying adult.[64] TSA has also implemented procedures to accommodate those passengers with disabilities and medical conditions that make them ineligible for AIT screening because they cannot stand in the necessary pose.

IV. Deployment of AIT

As of February 22, 2013, TSA has deployed over 800 AIT machines at approximately 200 airports in the United States.[65] TSA is removing the 174 Rapiscan general-use backscatter units from its checkpoints and by June 1, 2013, only units equipped with ATR software will be used to conduct screening.

Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using metal detectors. Once an anomaly is detected, additional screening is required to determine if the item is prohibited.

Since January 2010, this technology has helped TSA officers detect hundreds of prohibited, dangerous, or illegal items concealed on passengers.[66] TSA's procurement specifications require that any AIT system must meet certain thresholds with respect to the detection of anomalies concealed under an individual's clothing. While the detection requirements of AIT are classified, the procurement specifications require that any approved system be sensitive enough to detect smaller items, such as a Web pager, wallet, or small bottle of contact lens solution.

Experience has confirmed that AIT will detect metallic and non-metallic items, including material that could be in various forms concealed under an individual's clothing. For example, a non-metallic martial arts weapon called a ''Tactical Spike'' was discovered in the sock of a passenger in Pensacola, Florida after being screened by AIT.[67] Advanced Imaging Technology is also effective in detecting metallic items. In December, 2011, a loaded .38 caliber firearm in an ankle holster was discovered during AIT screening of a passenger at Detroit Metropolitan Airport.[68] The versatility of AIT in detecting both metallic and non-metallic concealed items without physical contact makes it more effective than metal detectors as a tool to protect transportation security.

Some of the items discovered concealed on passengers during AIT screening are small items, such as weapons made of composite, non-metallic materials, including a three inch pocket knife hidden on a passenger's back; little packets of powder, including a packet the size of a thumbprint; and a syringe full of liquid hidden in a passenger's underwear.[69] A plastic dagger hidden in the hemline of a passenger's shirt was detected using AIT[70] and a plastic dagger concealed inside a comb was detected in a passenger's pocket.[71] Advanced Imaging Technology's capability to identify these small items is important because in addition to weapons and explosive materials, TSA also searches for improvised explosive device components, such as timers, initiators, switches, and power sources. Such items may be very small. Advanced Imaging Technology enhances TSA's ability to find these small items and further assists TSA in detecting threats.

V. Rulemaking Analyses and Notices

A. Regulatory Evaluation Summary and Economic Impact Analyses

Changes to Federal regulations must undergo several economic analyses. First, Executive Order (E.O.) 12866, Regulatory Planning and Review (58 FR 51735, October 4, 1993), as supplemented by E.O. 13563, Improving Regulation and Regulatory Review (76 FR 3821, January 21, 2011), directs each Federal agency to propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs. Second, the Regulatory Flexibility Act of 1980 (5 U.S.C. 601 *et seq.,* as amended by the Small Business Regulatory Enforcement Fairness Act (SBREFA) of 1996) requires agencies to consider the economic impact of regulatory changes on small entities. Third, the Trade Agreements Act (19 U.S.C. 2531–2533) prohibits agencies from setting standards that create unnecessary obstacles to the foreign commerce of the United States. Fourth, the Unfunded Mandates Reform Act of 1995 (UMRA) (2 U.S.C. 1531–1538) requires agencies to prepare a written assessment of the costs, benefits, and other effects of proposed or final rules that include a Federal mandate likely to result in the expenditure by State, local, or tribal governments, in the aggregate, or by the private sector, of $100 million or more annually (adjusted for inflation).

B. Executive Orders 12866 and 13563 Assessment

Executive Orders 12866 and 13563 direct agencies to assess the costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). Executive Order 13563 emphasizes the importance of quantifying both costs and benefits, reducing costs, harmonizing rules, and promoting flexibility. This rule is a

[64] See Advanced Imaging Technology (AIT) at *http://www.tsa.gov/traveler-information/traveling-children.*

[65] TSA maintains a list of airports that have AIT machines on its Web site at *http://www.tsa.gov/travelers-guide/ait-frequently-asked-questions.*

[66] Remarks of TSA Administrator John S. Pistole, Homeland Security Policy Institute, George Washington University, November 10, 2011.

[67] ''TSA Week In Review: Non Metallic Martial Arts Weapon Found with Body Scanner,'' *http://blog.tsa.gov/2011/12/tsa-week-in-review-non-metallic-martial.html.*

[68] *http://blog.tsa.gov/2011/12/loaded-380-found-strapped-to-passengers.html.*

[69] ''Advanced Imaging Off To a Great Start,'' April 20, 2010, at *http://blog.tsa.gov/2010/04/advanced-imaging-technology-off-to.html* and ''Advanced Imaging Technology—Yes, It's Worth It,'' March 31, 2010, at *http://blog.tsa.gov/2010/03/advanced-imaging-technology-yes-its.html.*

[70] ''TSA Week in Review: Plastic Dagger Found With Body Scanner,'' May 4, 2012, at *http://blog.tsa.gov/2012/05/tsa-week-in-review-plastic-dagger-found.html.*

[71] ''TSA Week in Review: Comb Dagger Discovered With Body Scanner, 28 Loaded Guns, and More,'' August 17, 2012 at *http://blog.tsa.gov/2012/08/tsa-week-in-review-comb-dagger.html.*

''significant regulatory action'' that is economically significant under sec. 3(f)(1) of E.O. 12866. Accordingly, the Office of Management and Budget (OMB) has reviewed this regulation.

In conducting these analyses, TSA has determined:

(1) This rulemaking is a ''significant regulatory action'' as defined in the E.O.

(2) An Initial Regulatory Flexibility Analysis suggests this rulemaking would not have a significant economic impact on a substantial number of small entities.

(3) This rulemaking would not constitute a barrier to international trade.

(4) This rulemaking does not impose an unfunded mandate on State, local, or tribal governments, or on the private sector under UMRA.

These analyses, available in the docket, are summarized below. This NPRM proposes to codify the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. These costs are incurred by airport operators, the traveling public, Rapiscan, and TSA. Some airport operators incur utility costs for the additional electricity consumed by AIT machines. The small percentage of passengers (approximately one percent) who choose to opt out of AIT screening will incur opportunity costs due to the additional screening time needed to receive a pat-down. Rapiscan, a company that manufactures AIT machines, will incur a cost to remove backscatter AIT units in 2013 that have been deployed in previous years.[72] TSA incurs equipment costs associated with the life cycle of AIT machines (testing, acquisition, maintenance, *etc.*); personnel costs to hire TSOs to operate the AIT machines; utility costs at reimbursed airports; and training costs to train TSOs to operate AIT, and to detect and resolve any anomalies that may be discovered during AIT screening.

When estimating the cost of a rulemaking, agencies typically estimate future expected costs imposed by a regulation over a period of analysis. Because the AIT machine life cycle from deployment to disposal is eight years, the period of analysis for estimating the cost of AIT is also eight years. However, as AIT deployment began in 2008, there are costs that have already been borne by airport operators, the traveling public, and TSA that were not due to this rule. Consequently, in the Initial Regulatory Impact Analysis for this rule, TSA is reporting the AIT-related costs that have already occurred (years 2008–2011), but TSA considers the additional cost of this rulemaking to be years 2012–2015. By reporting the costs that have already happened and estimating future costs in this manner, TSA will have considered and disclosed the full eight-year life cycle of AIT deployment.

TSA reports that the net cost of AIT deployment from 2008–2011 has been $841.2 million (undiscounted) and that TSA has borne over 99 percent of all costs related to AIT deployment. TSA projects that from 2012–2015 total AIT-related costs will be approximately $1.5 billion (undiscounted), $1.4 billion at a three percent discount rate, and $1.3 billion at a seven percent discount rate. During 2012–2015, TSA estimates it will also incur over 98 percent of AIT-related costs with equipment and personnel costs being the largest categories of costs. Table 4 below reports the costs that have already happened (2008–2011) by cost category, while Table 5 shows the additional costs TSA is attributing to this rulemaking (2012–2015). Table 6 shows the total cost of AIT deployment from 2008 to 2015.

TABLE 4—NET COST[73] SUMMARY OF AIT DEPLOYMENT FROM 2008–2011 BY COST COMPONENT

[Costs already incurred in $ thousands—undiscounted]

Year	Passenger opt outs	Industry utilities	TSA costs				Total
			Personnel	Training	Equipment	Utilities	
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$52,535.3
2009	32.2	5.7	15,618.6	88.0	42,563.6	20.4	58,328.5
2010	262.2	158.2	247,566.7	5,332.8	119,105.4	241.4	372,666.6
2011	1,384.2	186.7	284,938.7	15,354.4	55,567.2	269.1	357,700.2
Total	1,685.6	356.3	562,813.0	21,164.7	254,661.3	549.6	841,230.6

TABLE 5—COST SUMMARY (NET COST OF AIT DEPLOYMENT 2012–2015) BY COST COMPONENT

[AIT costs in $ thousands]

Year	Passenger opt outs	Industry tilities	TSA costs				Rapiscan removal	Total
			Personnel	Training	Equipment	Utilities		
2012	$2,716.5	$325.7	$375,866.9	$12,043.0	$116,499.3	$473.0	$0.0	$507,924.4
2013	3,991.7	329.3	280,844.3	4,277.5	51,588.8	324.4	1,809.6	343,165.7
2014	4,238.7	312.0	263,677.6	4,190.5	51,397.8	317.7	0.0	324,134.2
2015	5,611.8	300.3	278,580.2	4,144.2	68,052.6	365.7	0.0	357,054.9
Total	16,558.7	1,267.3	1,198,969.0	24,655.2	287,538.5	1,480.9	1,809.6	1,532,279.2
Discounted 3%	15,265.0	1,178.9	1,118,459.3	23,810.2	269,233.7	1,380.7	1,705.7	1,431,033.5
Discounted 7%	13,766.6	1,075.8	1,024,344.7	22,048.8	247,810.4	1,263.8	1,580.6	1,311,890.7

[72] On December 21, 2012, TSA terminated part of its contract with Rapiscan for the Convenience of the Government because it could not meet development related issues in regards to ATR by the Congressionally-mandated June 2013 deadline. As a result of the contract termination, Rapiscan will pay for the removal of all units still in the field.

[73] TSA removed costs related to WTMD that would have occurred regardless of AIT deployment to obtain an estimated net cost for AIT.

TABLE 6—COST SUMMARY (NET COST OF AIT DEPLOYMENT 2008–2015) BY COST COMPONENT

[AIT costs in $ thousands—undiscounted]

Year	Passenger opt outs	Industry utilities	TSA costs				Rapiscan removal	Total
			Personnel	Training	Equipment	Utilities		
2008	$7.0	$5.7	$14,689.1	$389.5	$37,425.2	$18.8	$0.0	$52,535.3
2009	32.2	5.7	15,618.6	88.0	42,563.6	20.4	0.0	58,328.5
2010	262.2	158.2	247,566.7	5,332.8	119,105.4	241.4	0.0	372,666.6
2011	1,384.2	186.7	284,938.7	15,354.4	55,567.2	269.1	0.0	357,700.2
2012	2,716.5	325.7	375,866.9	12,043.0	116,499.3	473.0	0.0	507,924.4
2013	3,991.7	329.3	280,844.3	4,277.5	51,588.8	324.4	1,809.6	343,165.7
2014	4,238.7	312.0	263,677.6	4,190.5	51,397.8	317.7	0.0	324,134.2
2015	5,611.8	300.3	278,580.2	4,144.2	68,052.6	365.7	0.0	357,054.9
Total	18,244.4	1,623.6	1,761,782.0	45,819.9	542,199.9	2,030.4	1,809.6	2,373,509.9

This preamble (in the Background section above) has previously explained in detail the need for AIT and the Congressional direction to pursue AIT. In summary, terrorists continue to test our security measures in an attempt to find and exploit vulnerabilities. The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons. Below are examples of this threat:

- On December 22, 2001, on board an airplane bound for the United States, Richard Reid attempted to detonate a non-metallic bomb concealed in his shoe.
- On December 25, 2009, a bombing plot by Al Qaeda in the Arabian Peninsula (AQAP) culminated in Umar Farouk Abdulmutallab's attempt to blow up an American aircraft over the United States using a non-metallic explosive device hidden in his underwear.
- In October 2010, AQAP attempted to destroy two airplanes in flight using non-metallic explosives hidden in two printer cartridges.
- In May 2012, during the most recent terrorist plot thwarted, AQAP developed another non-metallic explosive device that could be hidden in an individual's underwear and detonated while on board an aircraft.

As evidenced by the incidents described in the above sections, TSA operates in a high-threat environment. Terrorists look for security gaps or exceptions to exploit. The device used in the December 25, 2009, attempt is illustrative. It was cleverly constructed and intentionally hidden on a sensitive part of the body to avert detection. If detonated, the lives of the almost 300 passengers and crew and untold numbers of people on the ground would have been in jeopardy.

Advanced Imaging Technology is proven technology which provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using metal detectors. In addition, risk reduction analysis shows that the chance of a successful terrorist attack on aviation targets generally decreases as TSA deploys AIT. However, the results of TSA's risk-reduction analysis are classified.

Passengers do not experience additional wait time due to use of AIT equipment because the x-ray screening of carry-on baggage constrains the overall screening process; they wait for their personal belongings regardless of which passenger screening technology is used.

In Tables 7 and 8 below, we present annualized cost estimates and qualitative benefits of AIT deployment. In Table 7, we show the annualized net cost of AIT deployment from 2012 to 2015. As previously explained, costs incurred from 2008–2011 occurred in the past and are not considered costs attributable to this proposed rule. However, given the life cycle of the AIT technology considered in this analysis is eight years; we have also added Table 8 showing the annualized net cost of AIT deployment from 2008–2015 (a full eight-year life cycle and includes the ''sunk costs'' from 2008 to 2011). Please note that while the *total costs* of AIT deployment for a full eight-year life cycle (2008–2015) are higher than the *total costs* of AIT deployment during the four-year period of 2012–2015, the *annualized* costs ($368,262.8 at seven percent discount) of the full eight-year cycle shown in Table 8 are actually lower than the *annualized* costs ($387,307.7 at seven percent discount) of the 2012–2015 deployment shown in Table 7. As previously shown in Tables 4 and 5, AIT deployment costs in 2008 and 2009 are relatively low compared with the later year AIT expenditures, resulting in lower annualized costs for the eight-year life cycle of 2008–2015. The costs are annualized and discounted at both three and seven percent and presented in 2011 dollars.

TABLE 7—OMB A–4 ACCOUNTING STATEMENT

[$ Thousands for 2012–2015]

Category	Primary estimate	Minimum estimate	Maximum estimate	Source citation (initial RIA, preamble, etc.)
BENEFITS				
Monetized benefits	Not estimated	Not estimated	Not estimated	Initial RIA.
Annualized quantified, but unmonetized, benefits	0	0	0	Initial RIA.

TABLE 7—OMB A–4 ACCOUNTING STATEMENT—Continued

[$ Thousands for 2012–2015]

Category	Primary estimate	Minimum estimate	Maximum estimate	Source citation (initial RIA, preamble, etc.)
Unquantified benefits	The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT technology that is capable of detecting both metallic and non-metallic weapons and explosives.			Initial RIA.
COSTS				
Annualized monetized costs (discount rate in parenthesis)	(7%) $387,307.0 (3%) $384,986.7		Initial RIA.	
Annualized quantified, but unmonetized, costs	0	0	0	Initial RIA.
Qualitative costs (unquantified)	Not estimated			Initial RIA.
TRANSFERS				
Annualized monetized transfers: "on budget"	0	0	0	Initial RIA.
From whom to whom?	N/A	N/A	N/A	None.
Annualized monetized transfers: "off-budget"	0	0	0	Initial RIA.
From whom to whom?	N/A	N/A	N/A	None.
Miscellaneous analyses/category	**Effects**			**Source citation (initial RIA, preamble, etc.).**
Effects on state, local, and/or tribal governments	None			Initial RIA.
Effects on small businesses	No significant economic impact anticipated. Prepared Initial Regulatory Flexibility Analysis			Initial Regulatory Flexibility Analysis.
Effects on wages	None			None.
Effects on growth	None			None.

TABLE 8—OMB A–4 ACCOUNTING STATEMENT

[$ Thousands, 2008–2015, eight-year lifecycle]

Category	Primary estimate	Minimum estimate	Maximum estimate	Source citation (initial RIA, preamble, etc.)
BENEFITS				
Monetized benefits	Not estimated	Not estimated	Not estimated	Initial RIA.
Annualized quantified, but unmonetized, benefits	0	0	0	Initial RIA.
Unquantified benefits	The operations described in this proposed rule produce benefits by reducing security risks through the deployment of AIT technology that is capable of detecting both metallic and non-metallic weapons and explosives.			Initial RIA.
COSTS				
Annualized monetized costs (discount rate in parentheses)	(7%) $368,262.8 (3%) $326,410.1			Initial RIA.
Annualized quantified, but unmonetized, costs	0	0	0	Initial RIA.
Qualitative costs (unquantified)	Not estimated			Initial RIA.
TRANSFERS				
Annualized monetized transfers: "on budget"	0	0	0	Initial RIA.
From whom to whom?	N/A	N/A	N/A	None.
Annualized monetized transfers: "off-budget"	0	0	0	Initial RIA.
From whom to whom?	N/A	N/A	N/A	None.

TABLE 8—OMB A–4 ACCOUNTING STATEMENT—Continued

[$ Thousands, 2008–2015, eight-year lifecycle]

Category	Primary estimate	Minimum estimate	Maximum estimate	Source citation (initial RIA, preamble, etc.)
Miscellaneous analyses/category	**Effects**			**Source citation (initial RIA, preamble, etc.).**
Effects on state, local, and/or tribal governments	None			Initial RIA.
Effects on small businesses	No significant economic impact anticipated. Prepared IRFA			IRFA.
Effects on wages	None			None.
Effects on growth	None			None.

As alternatives to the preferred regulatory proposal presented in the NPRM, TSA examined three other options. The following table briefly describes these options, which include a continuation of the current screening environment (no action), increased use of physical pat-down searches that supplements primary screening with WTMDs, and increased use of ETD screening that supplements primary screening with WTMDs. These alternatives, and the reasons why TSA rejected them in favor of the proposed rule, are discussed in detail in Chapter 3 of the regulatory evaluation located in this docket, and summarized in Table 9.

TABLE 9—COMPARISON OF REGULATORY ALTERNATIVES

Regulatory alternative	Name	Description
1	No Action	Under this alternative, the passenger screening environment remains the same as it was prior to 2008. TSA continues to use WTMDs as the primary passenger screening technology and to resolve alarms with a pat-down.
2	Pat-Down	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting a pat-down on a randomly selected portion of passengers after screening by a WTMD.
3	ETD Screening	Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD.
4	AIT Screening (NPRM)	Under this alternative, the proposed alternative, TSA uses AIT as a passenger screening technology. Alarms would be resolved through a pat-down.

C. Regulatory Flexibility Act Assessment

The Regulatory Flexibility Act (RFA) of 1980 requires that agencies consider the impacts of their rules on small entities. For purposes of the RFA, small entities include small businesses, not-for-profit organizations, and small governmental jurisdictions. Individuals and States are not included in the definition of a small entity. TSA has included an Initial Regulatory Flexibility Analysis within the Initial Regulatory Impact Analysis.

This NPRM proposes to codify the use of AIT to screen passengers boarding commercial aircraft for weapons, explosives, and other prohibited items concealed on the body. The only additional direct cost small entities incur due to this rule is for utilities, as a result of increased power consumption from AIT operation. TSA identified 102 small entities that could have potentially incurred additional utility costs due to AIT; however, TSA reimburses the additional utility costs for five of these small entities. Consequently, this rule would cause 97 small entities to incur additional direct costs. Of the 97 small entities affected by this proposed rule, 96 are small governmental jurisdictions with populations less than 50,000. A privately-owned airport is considered small under SBA standards if revenue amounts to less than $30 million. TSA identified one small privately-owned airport.

The small entities incur an additional utility cost as a result of increased power consumption from AIT operation. To estimate the costs of the deployment of AIT on small entities TSA uses the average kilowatt hour (kWh) consumed per unit on an annual basis at federalized airports. Depending on the size of the airport, TSA estimates the average additional utility cost to range from $815 to $1,270 per year while the average annual revenue for these small entities ranges from $69.5 million to $133.1 million per year. Consequently, TSA estimates that the cost of this NPRM on small entities represents approximately 0.001 percent of their annual revenue. Therefore, TSA's Initial Regulatory Flexibility Analysis suggests that this rulemaking would not have a significant economic impact on a substantial number of small entities.

D. International Trade Impact Assessment

The Trade Agreement Act of 1979 prohibits Federal agencies from establishing any standards or engaging in related activities that create unnecessary obstacles to the foreign commerce of the United States. Legitimate domestic objectives, such as safety, are not considered unnecessary obstacles. The statute also requires consideration of international standards and, where appropriate, that they be the basis for U.S. standards. TSA has assessed the potential effect of this rulemaking and has determined that it will have only a domestic impact and therefore no effect on any trade-sensitive activity.

E. Unfunded Mandates Assessment

The Unfunded Mandates Reform Act of 1995 (UMRA) is intended, among other things, to curb the practice of imposing unfunded Federal mandates on State, local, and tribal governments. Title II of the Act requires each Federal agency to prepare a written statement assessing the effects of any Federal mandate in a proposed or final agency rule that may result in a $100 million or more expenditure (adjusted annually for inflation) in any one year by State, local, and tribal governments, in the aggregate, or by the private sector; such a mandate is deemed to be a ''significant regulatory action.''

This rulemaking does not contain such a mandate. The requirements of Title II of the Act, therefore, do not apply and TSA has not prepared a statement under the Act.

F. Paperwork Reduction Act

The Paperwork Reduction Act of 1995 (PRA) (44 U.S.C. 3501 *et seq.*) requires that TSA consider the impact of paperwork and other information collection burdens imposed on the public and, under the provisions of PRA sec. 3507(d), obtain approval from OMB for each collection of information it conducts, sponsors, or requires through regulations. The PRA defines ''collection of information'' to be ''the obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinion by or for an agency, regardless of form or format…imposed on ten or more persons.'' 44 U.S.C. 3502(3)(A). TSA has determined that there are no current or new information collection requirements associated with this proposed rule. TSA's use of AIT to screen passengers does not constitute activity that would result in the collection of information as defined in the PRA.

G. Executive Order 13132, Federalism

TSA has analyzed this proposed rule under the principles and criteria of E.O. 13132, Federalism. We determined that this action would not have a substantial direct effect on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government, and therefore would not have federalism implications.

H. Environmental Analysis

TSA has reviewed this action for purposes of the National Environmental Policy Act of 1969 (NEPA) (42 U.S.C. 4321–4347) and has determined that this action will not have a significant effect on the human environment.

I. Energy Impact Analysis

The energy impact of the notice has been assessed in accordance with the Energy Policy and Conservation Act (EPCA), Public Law 94–163, as amended (42 U.S.C. 6362). TSA has determined that this rulemaking is not a major regulatory action under the provisions of the EPCA.

List of Subjects in 49 CFR Part 1540

Air carriers, Aircraft, Airports, Civil aviation security, Law enforcement officers, Reporting and recordkeeping requirements, Screening, Security measures.

The Proposed Amendment

For the reasons set forth in the preamble, the Transportation Security Administration proposes to amend Chapter XII, of Title 49, Code of Federal Regulations, as follows:

PART 1540—CIVIL AVIATION SECURITY: GENERAL RULES

■ 1. The authority citation for part 1540 is revised to read as follows:

Authority: 49 U.S.C. 114, 5103, 40113, 44901–44907, 44913–44914, 44916–44918, 44925, 44935–44936, 44942, 46105.

■ 2. In § 1540.107, add paragraph (d) to read as follows:

§ 1540.107 Submission to screening and inspection.

* * * * *

(d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.

Issued in Arlington, Virginia, on March 20, 2013.

John S. Pistole,

Administrator.

[FR Doc. 2013–07023 Filed 3–22–13; 4:15 pm]

BILLING CODE 9110–05–P

DEPARTMENT OF COMMERCE

National Oceanic and Atmospheric Administration

50 CFR Part 665

[Docket No. 130103006–3243–01]

RIN 0648–BC89

Fisheries in the Western Pacific; 5-Year Extension of Moratorium on Harvest of Gold Corals

AGENCY: National Marine Fisheries Service (NMFS), National Oceanic and Atmospheric Administration (NOAA), Commerce.

ACTION: Proposed rule; request for comments.

SUMMARY: This proposed rule would extend the region-wide moratorium on the harvest of gold corals in the U.S. Pacific Islands through June 30, 2018. NMFS intends this proposed rule to prevent overfishing and to stimulate research on gold corals.

DATES: Comments must be received by April 25, 2013.

ADDRESSES: You may submit comments on this document, identified by NOAA–NMFS–2013–0002, by either of the following methods:

- *Electronic Submission:* Submit all electronic public comments via the Federal e-Rulemaking Portal. Go to *www.regulations.gov/#!docketDetail;D=NOAA-NMFS-2013-0002,* click the ''Comment Now!'' icon, complete the required fields, and enter or attach your comments.
- *Mail:* Send written comments to Michael D. Tosatto, Regional Administrator, NMFS Pacific Islands Region (PIR), 1601 Kapiolani Blvd., Suite 1110, Honolulu, HI 96814–4700.

Instructions: Comments sent by any other method, to any other address or individual, or received after the end of the comment period, may not be considered by NMFS. All comments received are a part of the public record and will generally be posted for public viewing on *www.regulations.gov* without change. All personal identifying information (e.g., name, address, etc.), confidential business information, or otherwise sensitive information submitted voluntarily by the sender will be publicly accessible. NMFS will accept anonymous comments (enter ''N/A'' in the required fields if you wish to remain anonymous), and will accept attachments to electronic comments in Microsoft Word, Excel, or Adobe PDF file formats only.

C

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Other: **NPRM - Passenger Screening Using Advanced Imaging Technology Signed Version**

For related information, **Open Docket Folder**

Comment

I refuse to be groped by stranges or have strangers look at pictures of me essentially naked. I refuse to fly commercial air carrier due to this absurd TSA practice. I would rather drive anyway since I do not have to risk being stranded at an airport or left on an aircraft for hours on the taxiway.

Any technology can be defeated, so the advanced imaging equipment only gives a false sense of security to the uninformed public. Stop wasting money on it. Stop groping people and looking at them naked. People are not livestock; leave them some dignity.

Comment Period Closed

ID: TSA-2013-0004-0114

Tracking Number: 1jx-84h4-5tzz

Document Information

Date Posted:
Apr 1, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

City:
Pickerington

Country:
United States

State or Province:
OH

C

Milton John Schick

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0162

Tracking Number: 1jx-84h4-kr36

Comment

Ever since TSA started using invasive and totalitarian methods of airport security in complete violation of the U.S. Constitution, I have stopped flying. I now drive myself everywhere. If someone in business or a government agency I deal with finds the extra time involved excessive, too bad. I tell them why, and if they can't accept that, we do NOT do business. No one has ever yet complained. I will NEVER fly again until Congress gets some backbone and forces TSA to PROFILE, whether anyone likes it or not. The Israelis don't seem to have a problem like this. I even personally know FBI agents who get hassled by TSA and one who actually pulled out his cell phone to ask his SAC for permission to arrest a TSA screener. TSA is incompetent and corrupt to the bone. I will NOT fly, under any circumstances what-so-ever, period. TSA needs to be abolished and then start over, with intelligence, in more ways than one.

Document Information

Date Posted:
Apr 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Milton Schick

Mailing Address:
7611 North Camino De Maximillian

City:
Tucson

Country:
United States

State or Province:
AZ

ZIP/Postal Code:
85704-2024

C

Mary Graham

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I can only say, I am so appalled by the tactics of the TSA I won't even fly anymore. We drive where we want to go, vacation close to home...

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0168

Tracking Number: 1jx-84hm-px9g

Document Information

Date Posted:
Apr 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Mary Graham

Country:
United States

Response to NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Document ID TSA-2013-0004-0001)
Jean L. Cooper
rev. 3/31/2013

My objections to the use of AITs (also called body scanners) fall into 4 categories: constitutional, ethical, medical, and practical.

Constitutional:
The use of AITs is in violation of the 4th amendment to the Constitution, which requires that a search of one's person or belongings must be authorized by a warrant, supported by probable cause, and limited in scope. The fact that one has purchased an airline ticket (or bus ticket or train ticket) is not probable cause for a search. Tough theoretically an "administrative search" requires no warrant, the Supreme Court, in U.S. v. Davis, 482 F.2d 893, 908, states that *"[an administrative search is allowed if] no more intrusive or intensive than necessary, in light of current technology, to detect weapons or explosives, confined in good faith to that purpose, and passengers may avoid the search by electing not to fly."* Is it a permissible administrative search when the TSA does not limit its search to weapons or explosives, but opens wallets to read the documents therein, reads the paperwork in briefcases or files, questions travelers about their medications, quizzes one about where and why one is traveling, views images of the traveler naked, and touches every part of the traveler's body, including her sexual organs? I say such a search is much "more intrusive or intensive" than necessary.

Ethical:
The activities of the TSA in regard to the AIT and pat-downs at the checkpoints in an airport are used to intimidate and control citizens of this country whose only transgression is wanting to travel by air. The checkpoint staff of the TSA treats travelers like criminals. We are yelled at, looked down on, and patronized by the TSA. It is proven that some members of the TSA staff steal belongings and money from our carry-on bags as well as our checked baggage. In fact, I am more worried about the TSA stealing my bags than anyone else who might have access to my bags.

The TSA staff takes advantage of their position of responsibility to harass and take advantage of those members of our society who often cannot defend themselves; I refer to the elderly, children, and disabled travelers. The pat-down is used as a punitive weapon against all travelers, delaying travelers on purpose so that they miss their flights and making the physical pat-down either twice as lengthy as a normal pat-down or more rough and painful. The reason? To make the traveler comply and go through the AIT instead of requesting the pat-down as is her right.

Persons sent to secondary screening, who opt out, or who have medical conditions that don´t allow them to use the scanners (insulin pumps, inability to stand still, inability to hold their arms above their heads, claustrophobia, etc) are subject to what is called a "pat-down", but is actually a full-body rub, including intimate areas, and the insertion of the officer´s hands into the passenger´s pants. The elderly are forced to remove adult diapers or disrobe. The disabled have their canes or wheelchairs taken away and are forced to attempt to walk or crawl through the AIT.

The TSA staff are also known to choose a greater percentage of young, attractive female travelers for pat-downs than a truly "random" choice would select. Female travelers are often told that there are no female TSA agents available for a pat-down, so they can either let a male agent touch their bodies or wait for an unknown length of time. In other words, these persons are subjected to what in any other place is recognized as sexual assault.

It is proven that there are convicted child abusers who work for the TSA, and whose job includes "patting-down" children. By requiring the child the undergo such sexual touching, the government is promoting "grooming," which gradually reduces the child's resistance to such behavior, training him to comply with the wishes of people who wish to do him harm. This is not only unethical; it is criminal.

Medical: There are two kinds of AIT machines. One is the Rapiscan backscatter X-ray machine, which gives off radiation that is known to cause cancer. It does not matter that it gives off a small amount -- X-ray radiation is cumulative over a lifetime. In addition, the X-rays are not limited to the person inside the machine; it is also spread a certain distance around the machine, thus exposing the TSA staff for periods of up to 8 hours per day. This is a public health disaster waiting to happen. The study that has been touted as showing the safety of the Rapiscan machine have been repudiated by Johns Hopkins. The Millimeter Wave machines, we are told, do not use ionizing radiation. However, no long-term testing has been done on these machines, so their health effects over a long period of time are not known. I do not wish to be a government guinea pig to test these machines.

Travelers with insulin pumps or other external medical devices have had their equipment damaged by going through these AIT machines.

Practical:
These AIT machines produce false positives 54% of the time, requiring a follow-up pat-down. These false positives include prosthetic breasts, ostomies, bandages, maxipads, adult diapers—even scars and body abnormalities such as bony knees seem to appear. Such a rate of false positives makes the results of these machines suspect. It's also been proven that the machines only detect items on the surface of the boy, thus missing items inside the body, under a false skin, or under skin folds. They miss items that the metal-detectors will find, resulting in false negatives. For that reason, the scanners are making it easier to bring guns on an airplane! In government tests of TSA efficacy, the TSA personnel have found only 30% of the items that the testers attempt to smuggle into the secure area. With such an error rate, how can these machines be considered a success?

We have been assured that the images produced by these machines cannot be saved and stored; however, that is a lie, proven by the fact that 35,000 such images created by a Rapiscan machine were released to the public from a courthouse in Florida.

The AIT machines are slow, require full removal of everything from pockets, belts, etc., separate persons from seeing belongings (giving the TSA agents and passersby ample opportunity to steal from our bags), separate adults from children, and require more man power than the metal detectors. The AIT machines create log jams and large crowds of people standing in one place, offering a perfect opportunity for an attack.

Conclusion:
Since the introduction of the AIT machines, I have reduced my flying to only those occasions when I can't drive. In fact, last year I drove across the country, from San Diego to Columbia, SC, rather than fly, so strong is my objection to the TSA checkpoints and their practices. When I must fly, I always opt out, since I would rather be patted-down than go through a machine with unknown health effects. If there is no opt out available from the AIT machines, I will stop flying altogether. I lock my carry-on bags to prevent TSA staff from stealing from them. I feel no sense of security at having the TSA harassing me. I do feel that we have lost our freedoms and that our Constitution has been crumpled and thrown away.

Submitted 3/31/2013 JLC

C

Fred

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

Stop the screening. It should be the first thing to go in the sequester. It is unconstitiutional to begin with, and is far in excess of what is necessary. The screeners do not catch more than 50% of the so called dangerous items that go through the screening, and someone who wants to take a prohibited item on the plane can usually get through with it. I have choosen not to fly, because of the screening, and will continue to drive to my destination, or not travel by air. With the invasion of the trains, they taking it to another level that is not needed.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0246

Tracking Number: 1jx-84h2-nnyh

Document Information

Date Posted:
Apr 3, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Fred

Barbara Sheridan

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0279

Tracking Number: 1jx-84k0-7gnk

Comment

As an American citizen, I am deeply offended each time I and my family members are required to stand, in a straddled position, with arms in the air and hands overhead, for screening our entire bodies each time we fly. The enemy has won because American public servant agencies now treat all Americans as potential criminals. Even the body pat-downs are ridiculous given they don't really provide any added protections we don't already receive from limiting carry-ons and screening our belongings and our passing through metal detectors. The added pat-downs and the new Advanced Imaging is a disgrace, sold by private sector interests to make money from general fear.

Furthermore, these imaging machines can cause physical damage and the TSA does not know the actual long-term effect the added exposure will have on countless citizens, especially those of childbearing age and children. In addition, the TSA has thus far been unable to guarantee all employees implementing the use of these machines are adequately qualified and able to operate them correctly. Putting any person at potential risk unnecessarily is unacceptable.

It is time government agencies stopped buying every new idea that comes down the pike and starts remembering who they actually serve and what is truly logical. And it is time Americans are treated respectfully again and we go back to requiring probable cause before citizens can be accosted in any way, instead of the current system where we are treated like herded cattle all under suspicion. I do not support the use of the advanced digital imaging at airports or any public space.

Document Information

Date Posted:
Apr 3, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Barbara Sheridan

Mailing Address:
2725 Telequana Drive

City:
Anchorage

Country:
United States

State or Province:
AK

ZIP/Postal Code:
99517

Allison J. Jones

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0327

Tracking Number: 1jx-84ki-hpel

Comment

In a Free Republic I cannot understand why the blatant practice of intimidation currently in use by TSA is necessary or even possible.

At the age of 75 I am planning a 1200 mile trip with an aging automobile that I am trying make last as long as possible due to a limited retirement income, the majority of which is Social Security.

I am completely discouraged at the amount of entanglements that are currently in use that I have absolutely decided that flying is no longer an option for me. I am far too old and easily stressed by all that has been incorporated just to be able to board a plane.

Thus the stress of flying is merely replaced by the stress of nursing an aging car. Flying for me personally was always a stress free experience but I am literally afraid to attempt such these days.

The "due diligence" currently espoused by TSA is completely an over reaction and largely a waste of taxpayer money based on the quality of employees alone as current news sources constantly remind me of.

Document Information

Date Posted:
Apr 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Allison Jones

Mailing Address:
120 Brisbon Hall Drive

City:
Richmond Hill

Country:
United States

State or Province:
GA

ZIP/Postal Code:
31324

Dan

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0342

Tracking Number: 1jx-84kv-4gsw

Comment

I object to the use of these devices on 4th amendment grounds. I have never committed a crime and being forced to endure the abuse of my civil liberties whenever I need to travel is a disgrace. I routinely opt out, which causes me significant costs due to the amount of extra time I need to budget for each trip.

I think the TSA needs to respect that we as US citizens have a right to travel freely across the US without constant and unwarranted surveillance, search, or seizure.

These devices are ineffective, dehumanizing, and are shining example of government waste and abuse.

I have often opted to drive or take a train instead of flying thus increasing the cost of my trip and also increasing my risk of death as flying is a safer alternative.

I would prefer for the TSA to be disbanded and security returned to the airlines, let each airline compete on the security it offers - I guarantee it would be less invasive and more cordial.

I would also like to mention that the request for comments should've happened years ago.

Document Information

Date Posted:
Apr 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Dan

Country:
United States

State or Province:
NY

C

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

Airport scanning devices are a waste of government resources and invasion of privacy. I always opt out of them and increasing government regulation and invasion of my privacy and personal rights have encouraged me to drive more often and fly less. I have NEVER been afraid for my life because of terrorism but am constantly aware of the government interfering in my travels. TSA scanning machines should be abolished.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0343

Tracking Number: 1jx-84kz-eyv8

Document Information

Date Posted:
Apr 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

The possession of a Boarding Pass does not constitute probable cause, nor is it consent.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0390

Tracking Number: 1jx-84lb-6p7d

Document Information

Date Posted:
Apr 8, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Michael Alan Muller

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0401

Tracking Number: 1jx-84lp-s4oc

Comment

I consider the use of full body imaging and the alternative (the "enhanced pat-down") to be invasive, offensive and a violation of Fourth Amendment rights. I have avoided air travel since the measures were adopted, preferring to travel great distances by car.

These measures have left me feeling as though I live in an occupied state. Though it was over a decade ago, I distinctly recall the shock I felt on the day of 9/11. I can honestly say that I have since endured far more stress as a result of the subsequent invasive security measures than from the attack itself.

Full body imaging has been shown to be ineffective at discovering concealed items (see http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners/) and is acknowledged to be ineffective for discovering explosives. In light of their extremely limited capabilities, I have never heard anything approaching a reasonable justification for the sacrifice of passenger time, personal privacy and basic civil rights that these machines and procedures entail.

I suggest that the agency remove the scanners and revert to the use of simple metal detectors. I hope to be able to exercise my right to travel again some day.

Document Information

Date Posted:
Apr 8, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Michael Muller

City:
Cold Spring

Country:
United States

State or Province:
NY

ZIP/Postal Code:
10516

C

Donna A. Harrison

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0478

Tracking Number: 1jx-84o1-3wyi

Document Information

Date Posted:
Apr 10, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Donna Harrison

Mailing Address:
521 N.E. Fairchild Street

City:
Topeka

Country:
United States

State or Province:
KS

ZIP/Postal Code:
66608

Organization Name:
Passenger

Comment

I remember a time when if you couldn't use your ticket you could just sell it in the classified section of the newspaper it didn't matter that it didn't have your name on it and your family could wait with you and see you off in the departing area.
Later they changed that to the name on the ticket had to match the name on your ID, and your family could wait with you and see you off in the departing area.
Now your family just drops you off at the curb and you feel like you have entered a communist country. I would say a prison and passengers are the criminals and the guards are assuming all the passengers want to kill them, but I've never been in prison or jail so I really can't compare. I've never been to a communist country either but I remember studying about them in school.
The last time I flew I tried to get the agent to admit to what the machine showed. The TSA Agent said it was sound waves that bounced off your skin and would pick up any metal objects. I had read up on it before boarding the plane and had already decided to opt out. I just wanted to see what I would be told. I didn't tell her that she obviously did not know what she was talking about and did little to instill any confidence in their process or any of them knowing what they were doing.
I think the scanning machines are too intrusive. I know this has changed but when they knew they would be able to see peoples bodies they should have been made to have a line for females and a line for males with a female watching females from one screening room and a male watching males from a separate screening room. I wonder how many people that scream more screening, more screening have actually ever been on a plane. I am glad for the opt out rule I will use it anytime I do decide to fly. The first time I am told it is mandatory to go through the scanners I will kiss luggage I may have checked goodbye and walk back to the parking lot and drive to my destination.

C

Donald Eugene Ryan

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0596

Tracking Number: 1jx-84t4-rpp5

Comment

I am writing concerning the TSA regulation on passenger screening. I am an elite plus flyer with Delta and am angered as an American every time I go through security. Here, I see my fellow citizens "assume the position" as if they are criminals in order to access transportation. Instead of looking for bad things, the TSA should be focused on finding bad people. The organization has repeatedly shown itself incompetent and unaware of its own rules (such as the note that laptops under 13 inches can remain in bags). Additionally, every policy the TSA undertakes is reactionary in nature, such as removal of shoes and full body scanners. These are nothing but security theater designed to make passengers feel safe (they don't) and massively inconvenience and embarrass law abiding citizens. TSA agents have noted that Fourth Amendment of the US Constitution doesn't apply to them. This shocking disregard for basic freedoms is an affront both to the framers of the Constitution and the citizenry it was created to protect.

I strongly recommend disbanding these advanced screening procedures and the TSA as well. This is a vast organization that has gone rogue and forgotten that its mission is to serve the traveling public, not harass and humiliate them. Interject some common sense into airport screening and cease with the police state-like procedures. The American public deserves better than this.

Document Information

Date Posted:
Apr 17, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Donald Ryan

Mailing Address:
300 Oak Street

City:
Mount Vernon

Country:
United States

State or Province:
OH

ZIP/Postal Code:
43050

Fax Number:
614-929-3525

C

T.A.

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0597

Tracking Number: 1jx-84t4-wlwy

Comment

I am a stroke survivor - TIA in 2010. I am a rape survivor. My neurosurgeon advised me, after his exhaustive research turned up no substantiated, verifiable data concerning the safety of the scanners, to avoid them. I am also on cell phone restrictions, and have to use a wired earpiece instead of the handset up next to my head. I have been treated like a criminal - no, let me be clear, I've been treated worse because to pat down a criminal at least police need JUST CAUSE for it to be a lawful search. The TSA agents have been awful, dismissive, and used the patdown as a punitive measure. They've drawn out a patdown that should take about 2 minutes into a 10 minute ordeal where they have stuck their fingers up under my bra, down past the waistband of my pants, with my belongings on the conveyor out of my sight and told I couldn't retrieve them until after. They make what should be a simple patdown a traumatic ordeal and they do it right where everyone can see it - and have said as much right in front of me. "This should discourage anyone else from trying this little trick." As if it's A TRICK and not MY RIGHT to refuse a scan by a machine with no verifiable safety data.

The TSA does not exist to keep the planes safe. If safety was the concern, there would be decently paid guards with proper crowd surveillance training like Israel has. This is a farce, with improperly trained bullies and thugs running the show. It is a waste of taxpayer money and the TSA should be abolished. Removing the scanners would be a step in the right direction.

I'm voting with my wallet. I don't fly unless necessary. If I want to go somewhere for vacation, I take a train or drive, because I'm not willing to put myself in the hands of people who bully and try to railroad me through machines my doctor has strictly said to stay away from.

Document Information

Date Posted:
Apr 17, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
T A

City:
Minneapolis

Country:
United States

State or Province:
MN

ZIP/Postal Code:
55404

Martin A. Dyckman

The is a Comment on the **Transportation Security Administration** (TSA) Other: **NPRM - Passenger Screening Using Advanced Imaging Technology Signed Version**

For related information, **Open Docket Folder**

Comment

I recognize the necessity to screen airline passengers for those who are bent on harm. However, I consider the imaging technology to be unacceptably degrading--regardless of whether the viewer sees only an outline image of the person being inspected. It's the act of submission to that inspection that is degrading and dehumanizing--standing in a glass bubble with your arms raised in an act of virtual surrender, after undergoing the nuisance of emptying everything, whether metallic or not, from one's pockets. This humiliating exercise is a significant factor in my decisions as to whether to drive or fly to a destination.

Comment Period Closed

ID: TSA-2013-0004-0599

Tracking Number: 1jx-84t4-sj7n

Document Information

Date Posted:
Apr 17, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Martin Dyckman

Mailing Address:
355 Fox Run Road

City:
Waynesville

Country:
United States

ZIP/Postal Code:
28785

C

James L. Bareuther

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

The employment of advanced technology scanners should be expanded not diminished. The efficacy of scanners speed up the security screening process , ensure a consistent procedure and are not intrusive. Those who submit that the scanners are "not a comfortable experience" obviously do not have implantations (hips, knees, etc.) nor have they submitted to the non-scanner vetting process with their "friendly" TSA agent. As someone with over 2 MM miles on several airlines and therefore a "frequent traveler", I am hopeful that the current procedures remain and , as noted at the outset, scanners are mandatory at all security checkpoints in high volume airports.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0614

Tracking Number: 1jx-84te-vinb

Document Information

Date Posted:
Apr 17, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
James Bareuther

Country:
United States

State or Province:
CA

ZIP/Postal Code:
93921

Re: TSA-2013-0004-0001 or Federal Register Number 2013-07023

Summary
The TSA's summary to the proposed rule is outright deceptive and indicates willful misrepresentation of the facts, choice and options that it and the public face. Some clear and obvious counter arguments to their claims are set out below.

Airline security check points have become overly invasive and deprive people of their privacy, self-respect, dignity, and security of person. This is intensified by a workforce that can only be described in general terms as poorly trained, poorly managed, have a propensity for criminal behavior, show poor customer service skills, comport themselves poorly, and one can only infer are some of the least qualified people to hold any type of job. To subject oneself, and ones loved ones to TSA operated checkpoints is an exercise in self-restraint as both the "rules" and people acting on them, are capricious, arbitrary, vindictive, and lacking of common sense.

While the TSA has many issues, the front line use of AIT is an invasion of privacy, a poor use of time and resources, a potential health hazard, and an undue burden on those with certain conditions that "alert" every time - ensuring an even more invasive pat down. These tactics, and the way in which they are employed, have no place in an open and free society.

Specific issues with the proposed rule:

I(b) Executive Summary - Summary of The Major Provisions

"The threat to aviation security has evolved to include the use of non-metallic explosives, non-metallic explosive devices, and non-metallic weapons."

> To purport that non-metallic threats to aviation security are somehow newly "evolved" is clearly untrue, as the threat of plastic explosives and ceramic weapons has been in the public domain for the past 30-years (and even fodder for Hollywood movies). We should not be misled into believing there is a "new" threat.

"AIT currently provides the best available opportunity to detect non-metallic anomalies (5) concealed under clothing without touching the passenger and is an essential component of TSA's security layers."

> While this statement may be true technically [in reference to the use of AIT as the best way to detect non-metallic objects] - it may not be true when one weighs certain aspects of cost-benefit analysis differently. Amputation of a gangrenous limb may be the most certain way to ensure the spread of infection - but as a patient one could argue if that is truly the "best" course of action given other courses of treatment. There may be a place for AIT at the airport, perhaps as a

secondary screening device, but it is far from clear that AIT is necessary as a primary screening tool, as well as the fact that it is either the "best" or "essential."

Given the anecdotally high rate of false positives “alerts” from AIT, the touching component is often quite necessary. Should every senior wearing a diaper, woman wearing a maxi pad, or person with an injury wearing a bandage be forced an invasive and humiliating interaction with a government agent?

"Congress has authorized TSA to procure and deploy AIT for use at security checkpoints."

I cannot speak to this point, other than to say that because something has been authorized by congress hardly means that it is the right thing to do, let alone legal.

"TSA implemented stringent safeguards to protect the privacy of passengers undergoing AIT screening when AIT units were initially deployed and enhanced privacy even further by upgrading its millimeter wave AIT units with automatic target recognition (ATR) software. An AIT unit equipped with ATR creates a generic outline, not an image of a specific individual, and eliminates the need for operator interpretation of an image. TSA is removing all units that are not equipped with ATR from its checkpoints by May 31, 2013. (6)"

This statement is hard to read while at the same time suppressing an eye roll. A cursory Google search of "nude body scanners" will produce multiple articles detailing the lack of "stringent safeguards" of passenger privacy - which additionally begs the question of whether any technology that produces a naked image for government agents as prerequisite for flying can be construed as protecting one's privacy. The fact that the TSA is removing the machines that are not equipped with ATR now, after having installed them without public comment should not be met with a pat on the back, but rather a slap on the wrist for having employed them in the first place. Furthermore, it is unclear what the false positive rate is for ATR software. I suspect however that the software produces a tremendous amount of false positives; if the system were flawless I'm sure the TSA would trumpet its effectiveness - yet I'm sure any demands for the accuracy of such a technology will be met with resistance and the invocation of sensitive security information. However given the number of pat down resolutions for alerts by ATR software and the fact that not one would be terrorist has been apprehended at a check point would point to either an absurdly high false positive rate or a massive overestimation of the threat.

Additionally, for an agency beset with criminal behavior as evidenced by the continual arrest of TSA agents for numerous criminal acts while both on and off the job, can the flying public really be expected to trust such an agency with respecting and protecting their privacy.

"The safety of the two types of AIT equipment initially deployed was tested by TSA and independent entities and all results confirmed that both the backscatter and millimeter wave technologies are safe because the x-ray or radio waves emissions are well below applicable safety and health standards, and are so low as to present a negligible risk to passengers, airline crew members, airport employees, and TSA employees. (7)"

Again, this is far from settled, one need only execute a cursory Internet search to find multiple credible objections to the safety of both backscatter and millimeter wave technology. Without long term studies of the effects of such technology one can never be sure of its safety. Furthermore, this comment only applies to the specified use of such technologies. What are the potential effects if AIT machines were to malfunction, become "out of spec", or suffer from poor or improper maintenance? This important issue remains unaddressed, while evidence exists that these situations have already occurred.

"TSA has provided a detailed explanation of AIT procedures on its web site at www.tsa.gov/ait-how-it-works (which allows opt out procedures for passengers) and posted signs at airport checkpoints to notify passengers about AIT and alternative screening procedures. The level of acceptance by passengers has been high; the vast majority of passengers do not object to AIT screening."

First, I would say that the TSA's explanation are far from detailed and could objectively be classified as basic. Furthermore, as any regular traveler knows most frontline TSA employees are often unfamiliar with these procedures and they are often implemented arbitrarily or differently at different checkpoints and airports.

To say that the level of acceptance of AIT is high is a truly outrageous claim. When an air traveler is presented a choice, go through an AIT machine or be delayed in their travels, and suffer an invasive and often retaliatory pat down, the fact that people elect AIT should come as no surprise - but does not constitute acceptance or that passengers do not object. To reiterate if one is presented with the choice of a slap in the face or baseball bat to the knees as a perquisite of traveling, the fact that people consistently elect to be slapped in the face does not mean that people accept it or do not have objections. Additionally, frequent fliers (who represent the bulk of airline miles flown) consistently rate the performance of the TSA poorly. As opposed to public opinion polls that include the bulk of Americans that don't fly or fly only occasionally.

The public is offered a dilemma not a choice.

"TSA's experience in using AIT confirms that it is effective in detecting small, non-metallic items hidden underneath passenger clothing that could otherwise escape detection. When an item is detected, additional screening must be performed to determine whether the item is prohibited."

Perhaps AIT is effective in finding small non-metallic items, though there seems to be ample antidotal evidence that these machines may be defeated using certain tactics. However, even if these machines can find small non-metallic items under passenger clothing the TSA has not demonstrated that these machines are finding prohibited items let alone prohibited items that passengers intended to use for nefarious purposes.

Should we really spend billions of dollars - subject millions to invasive and demeaning pat downs, wasting countless hours in order to find receipts in people's back pockets and ace bandages around people's knees?

Furthermore, people with medical conditions may alert the AIT every time - creating a class of people for whose flying necessitates an invasive pat down every time they fly.

Jeffress B. Hailand

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0686

Tracking Number: 1jx-84v4-8x3c

Comment

I do NOT submit to the body scanners, and feel I am being "punished" by waiting an excessive amount of time, and, being subjected to a more than onerous search. I would rather drive . I have little confidence they provide any more security than do the metal detectors. Jeff Hailand

Document Information

Date Posted:
Apr 22, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Jeffress Hailand

Mailing Address:
225 S. Meramec

Mailing Address 2:
#528

City:
Clayton

Country:
United States

State or Province:
MO

ZIP/Postal Code:
63105

Fax Number:
314.863.8835

Organization Name:
Law Office of Jeffress B. Hailand

Submitter's Representative:
same

Passenger Screening Using Advanced Imaging Technology

Summary of Proposed Rulemaking

The Transportation Security Administration (TSA) is proposing to revise its civil aviation security regulations to clarify that TSA may use advanced imaging technology (AIT) to screen individuals at security screening checkpoints. This proposed rule is issued to comply with a decision of the U.S. Court of Appeals for the District of Columbia Circuit, which ordered TSA to engage in notice-and-comment rulemaking on the use of AIT for screening. The Court decided that TSA should provide notice and invite comments on the use of AIT technology for primary screening.

Introduction

Since the September 11, 2001 terrorist attacks on the United States, the Federal government has responded by taking steps to protect the nation by strengthening airline security, securing the borders and implementing controversial policies that can help protect Americans. As part of the Federal Government initiatives to improve airline security, the Transportation Security Administration was created as a response to the September 11 attacks to provide airport security for the traveling public in the United States.

Since its inception in 2001, the TSA has used various methods that have been deemed controversial by the public in screening passengers. These methods include pat downs, frisking and the use of the controversial advanced imaging technology (AIT) also popularly known as the full body x-ray scanner. The TSA's use of the body scanner to screen airline passengers has been the most controversial for a number of reasons. Firstly, critics of this technology argue that the use of the x-ray scanner may be violating citizen's Fourth Amendment rights. Other critics worry about the health implications, reported radiation emission and the risk of cancer for frequent air travelers passing through the scanner.

On July 15, 2011, the D.C. Circuit Court of Appeals ruled that the agency had violated the Administrative Procedures Act by implementing body scanners as a primary screening method without first undertaking public notice and comment rulemaking. The Court ordered the agency to "promptly" undertake the proper rulemaking procedures and allow the public to comment on the body scanner program.

Comment

The author of this comment appreciates the arguments from both the proponents and opponents of the x-ray body scanner. However, the author supports the TSA's deployment and use of the x-ray scanner in screening passengers for the sake of protecting lives and properties. Since the September 11, 2001 attacks and America's subsequent response using military force in certain countries, the enemies of the United States (both domestic and foreign) have made several attempts to detonate explosives on U.S carriers. To prevent these attacks, the TSA has been forced to evolve and develop new ways to detect potential attacks on the homeland and deter the perpetuators of this attack who are mostly sophisticated in their craft.

- **Invasion of Privacy as a Concern**

While it is fair to acknowledge the arguments of the opponents of these x-ray scanners who argue that the use of the scanner may constitute an invasion of citizen's privacy. It is also fair to state that the TSA has consistently showed that the scanner does not violate privacy rights. In a response to the "invasion of privacy" allegation, the TSA argued that they have implemented strict measures to protect passenger privacy which is ensured through the anonymity of the image and that these technologies cannot store, print, transmit or save the image, and the image is automatically deleted from the system after it is cleared by the remotely located security officer. The TSA's response shows that every traveler's body images and privacy rights are being treated with care and are not violated as most civil liberty groups would make people believe. Also, to address citizen's concerns about the possible invasion of their privacy, the TSA has made it known to passengers that they may opt out of the x-ray scanner screening and submit to an "enhanced" pat-down. This enhanced pat-down is an option for citizens who are uncomfortable passing through the x-ray scanner for whatever reason. All these show that the TSA has made genuine attempt over the years to allay people's fear and to prove that the TSA is not focused on breaching citizen's fourth amendment rights.

A neutral party may sympathize with the civil libertarians argument about the TSA's use of the body scanners as an example of the Federal Government's excess in dictating to its citizens. As a matter of fact, this argument may have merit because in recent times the government has overplayed its hands, breached and intruded on citizen's rights without cause (for instance: the wiretap surveillance clause in the PATRIOT ACT, etc.) However, the TSA's use of x-ray body scanners at airports should not be treated as another example of government overreach; neither should the TSA's action be deemed as an invasion of privacy. The reason why the TSA's actions is not an invasion of privacy as explained in the previous paragraphs is because firstly the images are anonymous to the screener, secondly, the TSA has made efforts to explain to the public that the images are automatically deleted from the system and also because the TSA has given an "opt out" option to those who may now want to go through the scanner. Hence it is fair to state that all this steps the TSA has taken shows that there is no sinister, willful and deliberate attempt at invading people's privacy as critics may suggest.

Effectiveness of the X-ray Body Scanner

The effectiveness of the x-ray body scanner has been controversial as the scanner itself. While critics of the scanner have described the technology as a hit or miss, U.S counter-terrorism officials and other airline security experts have hailed the scanner as effective. A vivid example of the efficacy of the scanner was published in a TSA blog titled *"TSA Week In Review: Non Metallic Martial Arts Weapon Found with Body Scanner."* According to this publication, a non-metallic martial arts weapon called a "Tactical Spike" was discovered in the sock of a passenger in Pensacola, Florida after being screened by the scanner and In December, 2011, a loaded .38 caliber firearm in an ankle holster was discovered during the screening of a passenger at Detroit Metropolitan Airport. Hence, it is fair to state that the versatility of this scanner in detecting both metallic and non-metallic concealed items without physical contact makes it more effective than metal detectors as a tool to protect transportation security.

Airport security experts and counter-terrorism officials have also unequivocally stated that the December 2009 Christmas bombing attempt on a Detroit bound U.S airliner would have been prevented if the suspect had passed through the x-ray body scanner. One of these airline security experts, Evert van Zwol, head of the Dutch Pilots Association stated that the full-body scanner "could have been helpful in this case, absolutely." Another expert, Joe Reiss, vice president of marketing for American Science & Engineering Inc., also stated that the x-ray scanners "provide the best protection for the widest range of threats."

Conclusion

While the author of this comment understands civil libertarians angst at the TSA's use of these scanners, still, it baffles the author of this comment that the critics of these scanners have consistently failed to grasp or consider the determination and sophistication of those who would like to commit havoc on U.S airliners and citizens. An example of such determination was evident in the way the convicted bomber in the 2009 Christmas Day bombing attempt concealed explosives in his underwear. According to reports, the Christmas Day bomber did not pass through an x-ray body scanner in Amsterdam before boarding the plane to the United States. If the bomber had passed through this scanner, would the scanner have alerted authorities and would it have stopped the bomber from boarding the plane? According to counter-terrorism officials, the answer is most likely yes.

Lastly, even if the TSA were to stop using the x-ray scanners as civil libertarian suggests, the fact is that there is no alternative technology out there that can assist in detecting explosives and other harmful objects that can be used to harm travelers. In the absence of anything better than the scanner, it would be a bit naïve and dangerous to phase out the x-ray body scanner in this dangerous world where terrorism (both domestic and foreign) has grown into a borderless and faceless phenomenon.

Another reason why phasing out the body scanners may be an impossible task is because according to public opinion polls, a majority of Americans support the presence and use of these scanners at our airports, hence it is fair to say that the x-ray scanners have come to stay. An example of these polls is a CBS poll conducted in the wake of the failed Christmas Day bombing, in the CBS poll almost three quarters of the American public said they were in favor of full body x-ray scanners at airports. Another Washington Post-ABC poll also conducted in 2010 stated that nearly two-thirds of Americans support the new full-body security-screening machines at the country's airports, as most say they put higher priority on combating terrorism than protecting personal privacy. What these polls reflect is the willingness of Americans to elevate public safety above any concern of personal privacy. The popularity of these scanners also shows that majority of fair minded Americans recognize that we live in a dangerous world where terrorism, airplane hijackings and other vices have come to stay at least for the considerable future. And as long as these vices thrive in our society, the TSA is fully justified in using these x-ray body scanners to protect air travelers. Supported by a clause in the 9/11 Commission report which states that *"Congress should provide funding and the TSA should move as expeditiously as possible to support, the installation of explosives detection trace portals* *or other applicable technologies at more of the nation's commercial airports,"* it is fair to state that the TSA's use of the AIT technology at the nation's airports would stretch into the future.

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0774

Tracking Number: 1jx-84wh-biip

Document Information

Date Posted:
Apr 23, 2013

RIN:
1652-AA67

Show More Details

Comment

As a result of the burdensome and intrusive airport screenings that have been put in place over the last few years, I would like you to take note of the following points:

1) I travel by air as infrequently as possible. I drive to my destination whenever possible, even when it involves driving across the entire country and taking several days. This is specifically in response to the intrusive security screenings and the terrible airline service that are now the norm.

2) I avoid the scanners under all circumstances, even when it means having to be delayed and be subjected to a demeaning pat down search by TSA personnel. This occurs very rarely as it is rather easy to simply take the line that uses the ordinary metal detector and avoid the whole body scanners.

I believe that if I am taking these steps, there are very likely large numbers of people who are quietly and without attention also acting in the same way. Our actions do not show up in surveys or statistics but are and will continue to be a very real side affect of the policy of intrusive airport screenings. This affect should be taken into account when deciding to continue or to enhance these policies.

Todd Edward Heimann

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-0916

Tracking Number: 1jx-84wi-hodc

Comment

This is excessive spending to make people "feel" safe. It is an inconvenience and another layer of crap to travel. After 9/11 people's whole attitude has changed. I'd rather that money be spent on getting pilots trained and armed or more air marshals. This is an invasion of privacy as the full body scanners that are already in place. I hate air travel, primarily because of the show made out of being safe, when I personally feel anything but due to the excessive oversight of the government. I know a few TSA agents and their stories are maddening. Turn the whole TSA over to the private sector and quit trying to control every facet of travel. I used to fly, but now I drive whenever even slightly practical. I look at more than just cost and time. I believe my personal safety is my responsibility, not some scanner. I feel awful everytime I step into a body scanner. I don't trust that someone isn't chuckling or that the images aren't stored or that anything I'm being told is even true. Let it go, spend the money where it will matter. Thank you.

Document Information

Date Posted:
Apr 23, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Todd Heimann

Mailing Address:
3601 Meadow Avenue

City:
Cincinnati

Country:
United States

State or Province:
OH

ZIP/Postal Code:
45211

Ben Fox

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1039

Tracking Number: 1jx-84wd-lpgh

Comment

Completely oppose. This technology has been proven not to provide any security to airports or their passengers. It is costing significant funding, hurting the airline industry. It is more humiliating, causing me to drive when possible, further hurting the airline industry. Please remove this worthless technology.

Document Information

Date Posted:
Apr 24, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Ben Fox

City:
Richmond

Country:
United States

State or Province:
KY

C

Gayle M.

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1439

Tracking Number: 1jx-84wo-j3bn

Comment

Thanks to invasive searches conducted on innocent people without probable cause I now drive whenever possible. Yes, it may take me longer to get there, but at least I won't have to worry about being sexually assaulted in the name of "security."

Document Information

Date Posted:
May 7, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Gayle M

C

Michael Gingrich

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I stopped flying due to screenings of various types. I refuse to submit myself to use of advanced imaging technology. I either drive or take bus or train, even though its sometimes very time inconvenient.

This practice is invasive, unsafe, and does nothing to increase security. Stop treating our bodies like they are government property.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1460

Tracking Number: 1jx-84wo-llyx

Document Information

Date Posted:
May 7, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Michael Gingrich

Mailing Address:
Box 7208

City:
Fort Worth

Country:
United States

State or Province:
TX

ZIP/Postal Code:
76111

Government Agency Type:
Federal

Government Agency:
TSA

C

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1490

Tracking Number: 1jx-84xf-x6n0

Document Information

Date Posted:
May 7, 2013

RIN:
1652-AA67

Show More Details

Comment

Full body scanners cross a line that should never have been crossed, and shame on you for not recognizing the importance of this. You have made the process of flying so repulsive that, when I have a choice, I now choose to drive instead of flying. Please, for the sake of your agency's credibility, do not reinstate those awful machines.

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I do not fly any more since these scanners have gone into effect. I'd rather drive than lose my dignity.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1617
Tracking Number: 1jx-84wf-ybwr

Document Information

Date Posted:
May 13, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

To:
Docket Management Facility,
U.S. Department of Transportation,
1200 New Jersey Avenue SE.,
West Building Ground Floor,
Room W12-140,
Washington, DC 20590-0001

From:
Kaitlin Duck Sherwood
157-2901 W. Broadway
Vancouver, Canada V6K 2G8

Re: TSA-2013-0004 comments

To whom it may concern:

I am writing to comment on TSA-2013-0004.

I am a US Citizen, living in Canada. I have reason to go to the US frequently to visit friends and family and/or for my work as a software professional. About once every two years, I take a trip overseas.

I have been boycotting the TSA for about three years now (and plan to continue) due to what I consider its government-sponsored sexual assault. I either drive, take the train, or choose airlines which make no stops in the US. Once, I took a private plane.

I do not believe that there will ever be a hijacking in the US again. The fault was not with security screening procedures, but with airline policy that directed airline personnel to comply with hijeackers' demands. Now, the flight crew will not stand for it. (For that matter, the passengers won't either.)

Furthermore, I am not convinced that the scanners are safe. Perhaps they are safe when properly maintained and calibrated, but TSA has not convinced me that they are competent in their maintenance and calibration.

Finally, the machines are expensive. That money could be spent on far better things. If you *must* spend it on something security-related, spend it on improved sensors at freight terminals. If you *must* spend it on something related to *airline* security, spend it on improved sensors for baggage. Even better, spend it on cameras to monitor baggage screeners so that valuables don't go missing from checked luggage quite so often, so that people will check more of their luggage and make the security lines move more quickly.

Sincerely,
K. Sherwood
Kaitlin Duck Sherwood

Lloyd L. Jordan

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1643

Tracking Number: 1jx-84x5-pwil

Comment

"I will not fly until TSA ceases and desists hands on full body and belongings searches, scanner body searches," and you can quote me on that. "I'd rather drive," It makes the Airlines lose money. It is bad for: tourism, creates public embarrassment, produces images of naked children, exposes workers and co-workers to higher cancer risks, High fliers at higher risk for cancer, and other nonsensical criteria that invalidate the existence and use of these devices.

Document Information

Date Posted:
May 16, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Lloyd Jordan

Mailing Address:
417 Southview Avenue

City:
Cincinnati, Ohio

Country:
United States

ZIP/Postal Code:
45219

C

Chris Doyle

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1737

Tracking Number: 1jx-84wm-sqi0

Comment

I have never and will never submit to this invasion of privacy, and it is a major factor in my travel decisions. I have taken trains and cars rather than be screened at an airport for domestic trips. When I do fly, I always take the patdown option, which cannot possibly be an efficient use of your resources and I'm sure drives up my ticket price. Please stop this ridiculous charade and focus on effective security methods that do not invade my privacy. "They that give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety."

Document Information

Date Posted:
May 16, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Chris Doyle

City:
Chicago

Country:
United States

State or Province:
IL

C

W. Hughes

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1741

Tracking Number: 1jx-84wm-phyl

Comment

The possibility of being scanned by the passive scanners (so-called "nude body scanners") has driven me away from flying. If I can drive somewhere in 12 hours or less I will choose to do it. I live very close to the Atlanta airport (ATL) and choose to use their rental cars instead of their airplanes.

This type of invasive scanning is not appropriate. The abuses of the extremely underpaid, overworked TSA agents have been well-documented, including taking the very detailed essentially naked pictures of passengers off the computer they use to monitor the scans.

There are much better ways to deter or prevent terrorists. Swap the technology for humans. Use the methods adopted by Israel (so-called "Israelification") which employs multiple layers of personnel trained in spotting "trouble." They achieve this by simply asking questions and observing behavior. Israel has had great success in preventing terrorist attacks of their airports and airplanes.

Yes, it will probably cost more. We should spend more if we're serious. What we have now is security theater.

Not only are the pat-downs and scans invasive and inappropriate, they're also ineffective. I can conceive of many ways to bypass them, and I'm not interested in causing any "trouble." I would expect that someone who had that as a goal would be able to think of more.

Please get rid of these scanners.

Document Information

Date Posted:
May 16, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
W. Hughes

City:
College Park

Country:
United States

State or Province:
GA

ZIP/Postal Code:
30337

Melissa E. Teates

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1823

Tracking Number: 1jx-84yp-epoi

Comment

If the federal government continues to use the Advanced Imaging Technology, then is must make the machines available for third-party research. The evidence provided thus far has not proven the safety of these screening machine for humans.

I no longer fly unless there is no other chose, because I opt-out when a scanner is in use for screening. The current pat down procedure is an affront to our civil rights. I drive, bus, or use the train for traveling whenever possible. Or just do not travel.

These theater that the TSA puts on does not make us safer and it is tyranny plain and simple. The worst part is we pay for this treatment. Go back to common sense screening (metal detector, random pat downs that are not abusive, and commonsense).

Document Information

Date Posted:
May 20, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Melissa Teates

City:
Falls Church

Country:
United States

State or Province:
VA

Abraham Richards Burnett

The is a Comment on the **Transportation Security Administration** (TSA) Other: **NPRM - Passenger Screening Using Advanced Imaging Technology Signed Version**

For related information, **Open Docket Folder**

Comment

I do not mind reasonable flight safety. This includes metal detectors and other non-invasive non-toxic security procedures. However the invasive pat downs and potentially hazardous health effects of the body scanner have driven me to refuse to fly for any reason. My health and my dignity are more important than my ability to efficiently travel domestically or abroad. Until the TSA stops violating our bodies and rights with these illegal pat downs (essentially assault) and unsafe scanners I and my family will stay home or drive.

Comment Period Closed

ID: TSA-2013-0004-1886

Tracking Number: 1jx-84wp-7p5i

Document Information

Date Posted:
May 21, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Abraham Burnett

Mailing Address:
4277 West Babcock Street

Mailing Address 2:
Apt 8

City:
Bozeman

Country:
United States

State or Province:
MT

ZIP/Postal Code:
59718

C

Kaye Beach

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1901

Tracking Number: 1jx-84z4-7g5f

Document Information

Date Posted:
May 21, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Kaye Beach

Mailing Address:
4019 Kent St.

City:
Norman

Country:
United States

State or Province:
OK

ZIP/Postal Code:
73072

Comment

- Travel is a right. It is not a privilege to be granted or denied by the government.
- Over the last several years I have chosen to drive rather than fly because of the TSA's trauma inducing groping and naked scanners costing me thousands.
- Searches or other conditions required for the exercise of our right to travel are subject to "strict scrutiny" and the burden of proof is on the TSA to show that they are actually effective and for a permissible purpose and that they are the least restrictive alternative that will serve that purpose.
- The TSA's current and proposed "rules" are unconstitutionally vague. It is impossible for the average traveler to figure out what is and isn't prohibited, or what is and isn't forbidden, at TSA checkpoints.

Rebecca Downing

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-1976

Tracking Number: 1jx-84z9-gaq5

Comment

The body scanners are not safe and I won't use one. Since they have been installed, I have elected NOT to fly at least 5 times. My family drove instead even though it cost us a bit more. When I flew earlier this year, passengers were randomly chosen to go through either the metal detector or the full scanner. Out bound, I went through the metal detector but when returning I was selected for the scanner. When I opted out I was spoken to very loudly by the TSA employee who directed to the search area for pat down. Although the lady who conducted my search was very polite, the whole procedure was unnecessary and an invasion of my privacy. This activity costs all of us way too much for any potential benefit. The airlines and airports lost money when I chose NOT to fly. This does not make us safer. We accept certain risks when we fly but this is more than I accept.

Document Information

Date Posted:
May 21, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Rebecca Downing

Mailing Address:
218 North Avenue

City:
Aptos

Country:
United States

State or Province:
CA

ZIP/Postal Code:
95003

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2074

Tracking Number: 1jx-84wq-k5hy

Comment

Haven't flown since the TSA rolled out the body scanners because I believe having government employees view people's naked bodies without a warrant is an unreasonable search. If I choose to fly in the future I will drive to Canada and fly to my international destination. I will not fly domestically until the TSA stops with the naked body scanners and the invasive pat-downs. I shudder to think of the millions of people who have been sexually assaulted or abused only to now have those traumatic experiences brought back because the federal government says it is safer this way.

The TSA and the body scanners are a great microcosm of the idiocy of the federal government. Ineffective and expensive solutions that trample on millions of people's rights on a daily basis.

Document Information

Date Posted:
May 22, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Country:
United States

State or Province:
OR

Grejdi Gjura

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2109

Tracking Number: 1jx-84x5-hd9a

Comment

My travel has gone down significantly ever since these scanner have started being used. I feel violated and ashamed when asking to not go through them. In addition I don't feel any safer than I would have when there were just metal detectors. Now that I have a kid, I can't even imagine taking her through these unnecessary lines, leading me to just travel by train and car.

Document Information

Date Posted:
May 22, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Grejdi Gjura

Mailing Address:
326 Broadway, Unit 14

City:
Somerville

Country:
United States

State or Province:
MA

ZIP/Postal Code:
02145

Robin Whitlock

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2169

Tracking Number: 1jx-8551-ulf4

Comment

I am against the AIT machines. I've stopped flying since they were introduced...my family of five drove 19 hours to Florida rather than be exposed to the radiation of the machines, or an invasive patdown.

Trauma on the way to Disney? No thanks.

Please, bring common sense into the conversation about airline security.

I do not believe those machines are safe at all.

Document Information

Date Posted:
May 22, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Robyn Whitlock

Mailing Address:
1616 Redpoll Court

City:
Naperville

Country:
United States

State or Province:
IL

ZIP/Postal Code:
60565

Karen Julie Lewis

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I returned home to Ct. today after leaving Orlando Florida yesterday afternoon. We DROVE both ways. The major reason for driving was the use of AIT in airports. I flew to New Orleans the beginning of the month, and because of flight changes I had no recourse except to go through the total body scanner or miss my flight.
I have written my congressmen/woman about my feelings of AIT's and full body patdowns. My feeling is we should return back to metal detectors as a primary screening technology and conducting explosive trace detection tests on random passengers.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2197

Tracking Number: 1jx-84wf-o5nj

Document Information

Date Posted:
May 23, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Karen Lewis

Mailing Address:
8 Morningstar Drive

City:
Seymour

Country:
United States

State or Province:
CT

ZIP/Postal Code:
06483

C

Vincent Wilkinson

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2288

Tracking Number: 1jx-84wn-mcsr

Comment

Due to the regulations in place as well as the actions of the TSA, I now refuse to travel by air and simply drive wherever i need to go. I did need to go to Singapore for work but otherwise have driven to Oregon, Texas, New York, California, etc. Body searches and especially imaging equipment do nothing to make me feel safer not are they safe to the public health. I simply refuse to be exposed to them and as long as the airlines are good with less flyers then continue with this system. Otherwise we need to investigate better alternatives.

Document Information

Date Posted:
May 28, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Vincent Wilkinson

City:
Midvale

Country:
United States

State or Province:
UT

ZIP/Postal Code:
84047

C

Marianne Cherrier Burns

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2397

Tracking Number: 1jx-84x4-cfb0

Comment

I am against the mandatory use of these body scanners as it is an invasion of personal privacy. Metal detectors and profiling would take care of this. A background check and a list of no risk flyers should be implemented. This is a ridiculous over reaction to a problem that simple profiling would take care of.

Document Information

Date Posted:
May 29, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Marianne Burns

Mailing Address:
4873 Mohr Avenue

City:
Pleasanton

Country:
United States

State or Province:
CA

ZIP/Postal Code:
94566

C

Bobbie Kent

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2442

Tracking Number: 1jx-85a4-rlmu

Comment

I find the circus at our airports to be appalling - not just because we are being unConstitutionally stripped and then sprayed with radiation and now millimeter waves, but also because the know-nothings operating this equipment (which would ordinarily be classified as 'medical equipment') typically appear to have been hired from the absolute lowest rung of our employment pool.
Why, if this is really about "securing' our country, are we not hiring genuine security professionals, with years of proper law enforcement training, and the adjunct education that would ensure their absolute familiarity with medical devices such as insulin pumps, feeding tubes, prosthetics, ostomys and the like? It's unfathomable to me that these laymen not only question these medical appliances but then actually touch them, possibly contaminating them, and the traveler - or worse breaking something, spilling, losing the medication and so on. I mean seriously - ? - we're good with this? All of these things - from the scanners to the intense 'examinations' performed by these laymen fall into the category of activities that should be conducted by true professionals - if at all. I am disrpirited by my fellow Americans, not just for acquiescing to all this, but for actually endorsing it. Whenever I have to fly now I have a sick feeling in my stomach for days in advance and can rarely enjoy the trip itself as I know what awaits me for the return.
I think if all Americans were subjected to having strangers place their hands inside the waistbands of their pants in order to commute to work and such, they might wake up to these abject abuses.
Three times with strangers hands inside my waistband was enough for me. I drive everywhere now. Sorry airlines. No matter how good a job you do, the fact that my first encounter with your "product" is one in which I am assumed to be a criminal and then processed like a felon into jail by minimum-wage hacks, is not my idea of either enjoyable or "safe."

Document Information

Date Posted:
May 29, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Bobbie Kent

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2542

Tracking Number: 1jx-85e0-awsp

Document Information

Date Posted:
May 30, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

City:
Worth

Country:
United States

State or Province:
IL

Comment

I feel that the invasive technique currently being used is unnecessary. The people who are doing the screening are not professionals, even if you slap a uniform on them. There is inconsistency in the enforcement of policy that is stated on the website.The TSA screeners are unprofessional. Yellin at passengers, treating them like idiots, stealing their personal items is a Federal agency out of control. There is no proof that these machines aren't harmful yet we use them anyway. Go back to the way it was before. It worked fine. Metal detectors, explosive trace detection screening & unenhanced pat downs if there is an alarm. There is absolutely NO proof that all this humiliation the flying public endures in the US has stopped a terrorist act. TSA parades out all the knives & other items confiscated but I'm not impressed. Also the theft of personal property. I'm sorry but I do NOT want to have my possessions out of my sight for a minute. The lack of response from this agency is unacceptable. People's rights are violated & nobody addresses the issues. The TSA feels they are untouchable. Nobody should be untouchable.
Metal detectors, explosive trace detection screening & unenhanced pat downs if there is an alarm. Please return to a better way of screening passengers. Give us back our dignity. Because of a minority of people, the enitre flying public is being held hostage & treated like criminals. I would love to return to flying to my vacation destinations but until the government reins in the TSA & uses a safer & unembarrassing method of security, I will continue to curtail my travels by air. I know there are many people who feel the same way. Boycott the airports & drive.Hopefully this will catch on & the airlines will lose money & pressure the government to get realistic in their screening approach.

Wade Allen

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2702

Tracking Number: 1jx-84x0-blnn

Comment

The use of full body scanners should be stopped. Immediately. They are a piece of security theater designed to infringe upon our rights without providing any real security. The same goes for the alternative pat downs.

The only real positive benefits of either of these practices are slowing airline traffic and providing a jobs program for TSA employees.

The excuse provided for the need for these programs - to "prevent another 9/11" has already been solved without the use of either of these programs. The locked cockpit door in combination with the change in the normal procedure to follow during a hijacking was all that was either necessary or effective.

Before the introduction of these new violations of our rights, I preferred to fly instead of drive half way across the country. Now I avoid flying whenever possible. Every person who is at all interested in their personal rights should do the same.

Document Information

Date Posted:
Jun 3, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Wade Allen

Country:
United States

State or Province:
NC

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2721

Tracking Number: 1jx-85d8-3y7b

Document Information

Date Posted:
Jun 3, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Country:
United States

State or Province:
VT

Comment

I will never go through a body scanner. No one is going to see me naked. Plus, I've read the radiation is worse than was expected. There has to be a better way to find evil doers.

I would rather see the creation of special access passes. I would be willing to have a thorough back ground check that would give me a card/passport with a certain level of access. One that would allow me to go back to regular bag x-rays and metal detector. I was born in the U.S, held a long time job, no criminal record. I am a 0 threat. Frequent fliers as in Business people should be able to bypass the heightened security.

On the lowest level of pass there would be the full check, - body scan or pat down. This would include people with criminal records, mental illness (if only this was info was avail)
Any non-citizen.

I've read so many horror stories with TSA agents giving people a hard time - including senior citizens and children.
This must stop.
It's such a hassle to fly these days, I either stay home or drive myself.
The last time I flew was on Southwest and it seemed like a cattle car.
It looks like the days when flying was enjoyable are gone. I remember hot meals, free gifts, and leg room.

Kate

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2740

Tracking Number: 1jx-85hx-2o1u

Document Information

Date Posted:
Jun 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Kate

Country:
United States

State or Province:
PA

Comment

I am 100% against the virtual strip search body scanners that the TSA has utilized in airports. Ever since these machines started being used I have not traveled via airplane. I refuse to allow anyone to see me virtually naked without a search warrant. I am a criminal justice major, and I have done my research. There are no other circumstances in which this type of situation would be legal.
I have read articles that speak about minors going through the scanners, and my question is how is that not considered child pornography? It does not matter if the image is saved or deleted; the mere viewing of a nude image of a minor is an act of child pornography.
The implementation of these machines have severely impacted my life, because if I wish to travel anywhere without feeling violated I have to drive... even if that means a 2 day trip out of state to see family. I suppose the TSA's argument would be that I could opt out of the body scanner... no thank you! Not only do I not want anyone seeing a virtual nude image of me, but I also do not wish to be molested. I do not want anyone touching any part of my body (over clothing or not) that I only let my significant other touch.
Not to mention, how can I be assured that the images produced by the scanners won't end up in the wrong hands? What guarantee do I have that the images are immediately deleted?
Lastly, what do these machines do to keep us safe? A blogger was able to get through the machine with a metal box because it was on the side of his body.
It's time TSA starts focusing on real ways to pick out terrorists instead of making every single person feel humiliated and violated. Try learning some behavioral observation techniques. But get these machines out of the airports so I can start traveling again!

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I would like to see the full body scanners removed from all airports. Beyond the health risk and privacy concerns, I do not see any improvement to security that these scanners offer. I do not feel that our airport security has been improved, despite the additional inconviences imposed on travelers. I personally have stopped flying to any location in the United States for personal trips and I opt to drive for any business trip that is within 8-9 hours driving due to the increased inconvience of flying. My frustration with the TSA and the policies of the last few years has discouraged me from flying altogether and I don't find it surprising that our airlines are struggling for this very reason.

I was an avid traveler and used to prefer flying. I'm sure I'm not the only person who has stopped flying because of TSA policies and procedures.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2785

Tracking Number: 1jx-84x5-4ko1

Document Information

Date Posted:
Jun 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

C

E. Kelly

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-2798

Tracking Number: 1jx-85nw-r9bn

Comment

I believe I should be free to travel around my own country without being searched. I believe the imaging is an unreasonable search of me and against my constitutional right against such. The imaging is an infringement of my right to privacy. I am not a terrorist threat and in no way could I be considered such. The searches are one step on a road to further infringement of my rights. I do not live in a police state and do not want to be treated as if I do. When I travel back to the US from other countries, I do not have to take off my shoes, go through an imaging machine, nor be treated like a terrorist. We have evolved from a "war on terror" to a "war OF terror." The TSA merely frightens us into thinking that we are constantly under threat. I have chosen to drive my car or take Amtrak on a few trips rather than fly because of the TSA security theater. I hesitate to even mention the train because I don't want the TSA to get involved in train passenger screening. Please stop the imaging at airports.

Document Information

Date Posted:
Jun 4, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
E Kelly

City:
Houston

Country:
United States

State or Province:
TX

ZIP/Postal Code:
77005

Josh Schreibman

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I do not think any person under the age of 18 should be exposed to these machines. Forcing children into these scanners is to force parents to allow strangers to look at their children naked, and that is totally unacceptable.

I would rather drive to my destination than subject my family to government-mandated child pornography.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3066

Tracking Number: 1jx-84x1-vdvh

Document Information

Date Posted:
Jun 5, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Josh Schreibman

Mailing Address:
220 Pineapple Street

City:
Satellite Beach

Country:
United States

State or Province:
FL

ZIP/Postal Code:
32937

Daniel Linder

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3196

Tracking Number: 1jx-85kw-hr61

Comment

I have not flown since the imposition of AIT. I cannot consent to what I believe to be a breach of my Constitutional rights. It saddens me to see travel demoted to "privilege" from right, subject to my consenting to endless idiotic restrictions, none of which seem to ever have actually caught a terrorist. I have driven everywhere since AIT went into effect, including 2 Winter round trips from CA to IL, and one round trip from CA to FL to see the final Shuttle launch. All that time on the road subjected me to additional costs and danger over flying.

The TSA seems to be effective at humiliating the elderly, the infirm, women, children, and foreigners, and appear to be quite adept at finding drugs, but none of this relates to their mandate of keeping the traveling public safe. The scanners slow down lines, give off too many false positives, humiliate the traveling public where the scanners are set to show anatomical details vs the "cartoon outline", and seem to routinely fail internal checks against detecting test weapons. There must be less invasive methods of passenger screening.

The TSA's current and proposed “rules” are unconstitutionally vague. I can’t tell what is and isn’t prohibited, or what is and isn’t forbidden, at TSA checkpoints, and I understand that every checkpoint and airport is different due to the lack of training and generally low quality of TSA staff. I shouldn't have to get arrested to find out whether something is against the law or not.

In short, the TSA is a disaster and shouldn't be given such broad powers and especially should not be given additional expensive equipment that will just wind up in the garbage like the chemical detecting air puff machines and the backscatter x-ray machines.

Document Information

Date Posted:
Jun 6, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Daniel Linder

Mailing Address:
6466 Hollis St., Unit 228

City:
Emeryville

Country:
United States

State or Province:
CA

ZIP/Postal Code:
94608

C

VSM

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3218

Tracking Number: 1jx-84x2-3kp8

Comment

It's invasive and does nothing to help security.I go through the pat down,even though it's time consuming and embarrassing,but the alternative is worse. Have stopped about half my flights,and drive instead.
If it becomes FORCED with no pat down,I'll stop flying completely.Especially with facetime,internet,it's less needed anyway.

Document Information

Date Posted:
Jun 7, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
V M

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3303

Tracking Number: 1jx-850g-1kwg

Document Information

Date Posted:
Jun 10, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Comment

ID: TSA-2013-0004-0001. The AIT systems are both unnecessary and unconstitutional and should not be used other than for exceptional circumstances (and as allowed by the constitution). Locked cockpit doors and passenger awareness have done the most to mitigate the threat to aviation. The TSA methods have done the opposite, at least for me since I now avoid flying at all costs, preferring to drive for three days than to have to deal with the TSA and their unconstitutional (and mostly useless) methods.

[P] The head of the TSA said that their actions are permitted because they perform "public safety searches". Apparently he's never read the constitution (which he swore to protect and defend) which makes no such distinction - all searches must have a warrant.

[P] I'd like to emphasize that the heads of the TSA, DHS, and the USA all swore to protect and defend the constitution. Protecting anything else is secondary because the constitution itself defines the USA - it *is* the USA. These people need to read it, understand it, and adhere to its guidance as they all swore to do.

The pre-9/11 security was plenty. The 9/11 events occurred because the airlines were too cheap to lock the cockpit doors, yet Congress has allowed them to deny their responsibility for the events of that day. Subsequent attempts have been thwarted by passengers, and *not* TSA. We need to return this country to "the land of the free and the home of the brave", not the land of millions of cowards being frisked daily to make them feel better.

[P] The TSA has also been a huge waste of money, stopping no terrorists but annoying, and worse, millions of people using their unconstitutional methods. That money is better spent elsewhere, such as highway safety. The roads kill far more each month than terrorists have all together. Use some good sense and invest where needed (and allowed).

[P] Support and defend the Constitution of the United States of America! You promised.

C

Joanne Frances Gladney-Naumer

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I've never had to use the Advanced Imaging Technology because I quit flying! There is plenty to see in the USA and road trips are the way my parents did it. Actually fun getting back into slower and less-hectic traveling!!

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3318

Tracking Number: 1jx-859o-11ts

Document Information

Date Posted:
Jun 11, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Joanne Gladney-Naumer

Mailing Address:
900 Coal Bank Road

City:
St. Louis

Country:
United States

State or Province:
MO

ZIP/Postal Code:
63138

Organization Name:
retired

Mary Kennedy

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3427

Tracking Number: 1jx-850g-z88v

Comment

Please restore our 4th amendment rights in our airports. I have stopped flying since this invasive technology started popping up. Last October i would have flown but chose to drive 1500 miles each way, instead of giving up my rights. In December I would have flown again, but chose again to drive 900 miles each way to visit family. I am a law abiding, tax paying citizen and resent losing my rights and being treated like the lowest common denominators in our society. THERE HAS TO BE A BETTER, SMARTER WAY. I will NEVER send my two year old daughter through one of those machines, OR submit her to an invasive grope by TSA. How do I explain to her that it's OK for THIS person to touch her there, but NOBODY else? I'm not sending those mixed messages to her.

Document Information

Date Posted:
Jun 11, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Mary Kennedy

Mailing Address:
P.O. Box 634

City:
Sugar Land

State or Province:
TX

ZIP/Postal Code:
77487

C

Vicki Warthen

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3465

Tracking Number: 1jx-84yd-ez21

Comment

I strongly object to using this technology for routine passenger screening. It is invasive and not scientifically proven to be either safe or more effective than previous screening methods. It also slows down the screening process. This technology is already in use and has caused me to find alternative travel methods (car; train) to avoid flying whenever possible.

Document Information

Date Posted:
Jun 11, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Vicki Warthen

City:
Cedarville

Country:
United States

State or Province:
IL

ZIP/Postal Code:
61013

Tom

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

The current TSA screening is invasive, more protection than I feel is necessary, and certainly far more protection than I want. Unless the distance involved makes it impractical, this screening makes me much more inclined to drive. The requirement to remove even a tissue from a pocket, even to undergo an even more invasive pat-down, is an unacceptable imposition. But will politicians and bureaucrats, not to mention those who profit financially from this system, ever have the courage to bring balance to the picture and risk criticism if something goes wrong?

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3559

Tracking Number: 1jx-8514-s6qa

Document Information

Date Posted:
Jun 12, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Tom

City:
Atlanta

Country:
United States

ZIP/Postal Code:
30338

Allyson Ramage

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3585

Tracking Number: 1jx-8519-nfdm

Comment

Travel is a right, not a privilege to be granted or denied by the government.

Searches or other conditions required for the exercise of your right to travel are subject to "strict scrutiny". The burden of proof is on the TSA to show that they are actually effective for a permissible purpose (not just e.g. to catch drugs, which is not supposed to be the TSA's job) and that they are the least restrictive alternative that will serve that purpose.

I haven't flown because I find the virtual strip-searches and/or the groping by checkpoint staff intolerable and/or traumatizing. Instead of flying my son out of state to see his family 4 times a year, we now drive 1-2 times a year. The costs of this are much higher because I have to take time off work and pay for hotels and gas.

The TSA's current and proposed "rules" are unconstitutionally vague. You can't tell what is and isn't prohibited, or what is and isn't forbidden, at TSA checkpoints. If there are to be any requirements or prohibitions on what you can and can't do, the TSA needs to spell them out, publicly, so that you don't have to get arrested to find out whether something is against the law or not.

Document Information

Date Posted:
Jun 12, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Allyson Ramage

Mailing Address:
190 Waner

City:
Felton

Country:
United States

State or Province:
CA

ZIP/Postal Code:
95018

J. Hatfield

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

Try a web search for "study backscatter shreds dna" to find reasons why this technology should not be used.
I stopped flying because I didn't want to be groped or be forced to go through these machines. I drive now.

They are designing 'camera' units to do the same as people walk through hallways, I suspect I won't even be a tourist in the future.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3599

Tracking Number: 1jx-84w6-uh99

Document Information

Date Posted:
Jun 12, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
J Hatfield

Country:
Canada

State or Province:
Nova Scotia

C

S.L. Hunt

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

"They who can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety." --Benjamin Franklin.

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." -- Fourth Amendment, Bill of Rights, U.S. Constitution.

"If all 800 million people who use airports every year were screened with X-rays, then the very small individual risk multiplied by the large number of screened people might imply a potential public health or societal risk. The population risk has the potential to be significant." -- Dr. David Brenner, head of the center for radiological research at Columbia University in New York, to the London Telegraph.

The TSA is security theater, that makes the effort to pretend they're doing some good, when really all they do is make traveling all the more hectic, troubling, and draining. I can't recall any instances of the TSA actually foiling a terrorist plot. Because of the TSA and their scanners and invasive pat-downs, I will no longer fly anywhere. I drive, and if I can't get there by driving or by boat, then I won't go there.

These scanners are invasive, violate the 4th amendment, and are potentially hazardous to the health of everyone to passes through an airport.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3616

Tracking Number: 1jx-856d-khpt

Document Information

Date Posted:
Jun 13, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
S. Hunt

Country:
United States

State or Province:
LA

Kelly McConnell

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I have stopped flying altogether due to the heavy handed and invasive screening procedures instituted by the TSA. The current screening process is MUCH more time consuming and invasive than one encounters in other countries and seems to be MUCH less effective.

So, rather than consent to being groped in public or allowing myself to be exposed to unnecessary doses of radiation I have just stopped flying. If I cannot drive or take a train to my intended destination I don't go. I realize that I am lucky to have the flexibility to make those decisions, many people must travel and therefore do not have that luxury.

I also know that I am not alone in this regard and have to wonder just how much business the American airlines are losing because of it. I have personal knowledge of at least 5 other people that have stopped flying for the same reasons I have stated.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3699

Tracking Number: 1jx-85xx-oa31

Document Information

Date Posted:
Jun 17, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Kelly McConnell

Mailing Address:
11375 S.W. Erste

City:
Tigard

Country:
United States

State or Province:
OR

ZIP/Postal Code:
97223

I was a longtime frequent flier who traveled domestically and internationally for family and business reasons. However, that all came to a screeching halt when TSA changed the screening procedures to require a person's right to air travel to be contingent upon him/her submitting to a full body scan with unknown health risks or a full body pat down wherein every part of the body will be rubbed, mashed, and prodded including my genitalia.

For me, traveling by air is a necessity to visit with my family and to earn an income. If I do not fly, I can do neither. As a result of these procedures which were rammed down our throats, I am no longer able to fly. Because of the full body scanners and the full body pat downs making it impossible for me to fly, I lost 90% of my income and forever lost time with my family.

Last month, I received a call that I feared. My Uncle was dying and the family was called to gather immediately so that we could be with him as he passed. Instead of focusing on my Uncle and his needs, my primary concern was TSA. I live 1400 miles away. My only option was to fly, in order to get there in time.

Why is TSA part of my decisions concerning the death of a family member? This is the question I had to answer: Would my Uncle, a Navy Veteran, want me to cast off my freedom, for which he was willing to give up his life, in order to for me be with him in his last moments? After much agonizing, I came to the conclusion that I would be spitting in the face of his sacrifice and in my own, if I answered the question any other way than no.

So I drove the 2800 mile roundtrip through thunderstorms, through the plains, through power outages, and through the mountains. All the while, I was tormented with not be able to do an everyday activity because of TSA. In the end, I arrived after my Uncle had passed. To further throw salt into my wounds, I had to leave immediately after the funeral because I had to drive back in order to make the return trip. The only way in which to attend my Uncle's funeral in the 3 days' time, I was allotted was to fly. There was no other alternative. It was and is physically impossible for me to make the drive across country and back in three days. In the end it means, that TSA has taken away my right to travel.

Currently, if I need to fly I have to either be scanned by a machine which has unknown health risks and have naked photos taken of me (before the generic image can be produced the naked photo must be taken) or I have to be patted down from head to toe including the touching, prodding, and massaging of my genitalia. I will have to reveal my most private medical conditions to TSA officers who are not trained in medicine.

Moreover, the full body scans and full body patdowns require that an American Citizen subject herself or himself to a level of degradation and submission that is unacceptable and prohibited by the US Constitution. It is unreasonable to search and seize my body and my property just because I am seeking to go from point A to point B. I am suspect because I am engaging in the everyday activity of having family relations, earning an income by working a job, seeking education, obtaining medical care. etc. If I attempt to object to the TSA procedures or assert any of my rights, TSA bans me from flying. That means cannot go on a job interview, complete my job responsibilities, interview for college, visit my family, go on a vacation, obtain the medical care of my choice, run a business, run a campaign etc. This is a most violent attack on the rights and freedoms of United States.

The full body scanners and full body patdowns are a psychological and physical attack on an individual. TSA officers are accountable to noone. In order to travel one must relinquish all control over one's body to the TSA and can do nothing to protect herself/himself. To have to restrain yourself from your natural instincts to move away from harmful physical contact, to avoid having naked photos taken of you, and to avoid health risks, is nothing less than a terrifying torture: the most egregious affront to basic human dignity.

This is the exact opposite of freedom. In order to fly, TSA forces me to be taken apart psychologically and taken apart physically. My freedom of movement is completely restricted; and I haven't been convicted of any crime. I am in a virtual prison: having no right to travel. For what reason do I have to surrender my rights just to be a free human being in America? My rights and freedoms have no price. TSA's response to terrorism to terrorize America. Does that make any sense?

TSA does not have the right to tell me what to do with my body? Nor does TSA have the right to have total control over my body just because I am traveling. Moreover, the millimeter full body scan do not work at least 54% of the time. It makes no sense to use machines that emit radiation of any sort (ionizing or tetrahertz) when they do not even work and are harmful to the health of humans. Of note is TSA's consistent and adamant refusal to allow independent testing of the full body scanners. For this reasons, travelers cannot not make a fully informed choice about the health risks of the full body scanners.

There are significantly less intrusive, less costly, and effective alternatives such as good old police work and dogs. Why has TSA steadfastly refused to use them?

TSA's decision to use full body scanners or to subject a human being to a terrorizing head to toe pat down including massaging, probing, and rubbing a persons entire body, their medical devices, and genitalia is the height of utter disdain for our right to life, our right to liberty, our right to privacy, our right to travel, our right to engage in commerce, and our right to be free from unreasonable searches and seizures.

The full body scanners and full body patdowns have created a decrease in travel which is detrimental to a healthy economy. One cannot operate a business in America without flying. In today's world, one cannot go on a job interview, earn an income, attend a funeral, spend time with family, go on vacation, without flying. There is no alternative to flying.

It is impossible to be in New York one day and California the next without flying. It is impossible to be present in New Orleans on Tuesday and Washington D.C. on Wednesday. So why does the TSA get to take my business away from me? If people are not permitted to freely travel without having to undergo a full body scan or pat down, people do not engage in business, do not hire employees, do not have money to spend in the marketplace, etc. Overall, the entire US economy takes a direct hit and cannot survive.

TSA must return to the use of metal detectors as the primary method of screening. Alarms should be resolved by the use of a metal detector wand. Advanced imaging technology should not be used on human beings. Common medical devices such as insulin pumps, hip and knee replacements, prosthetics, etc. should not trigger a full body patdown. Furthermore, no patdowns should be used without probable cause.

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3769

Tracking Number: 1jx-85yo-rcit

Document Information

Date Posted:
Jun 18, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Comment

I refused to go through a scanner at ONT, and as a result, was physically brutalized by a screener and left with bruises on my leg and arm. All I wanted to do was go to my grandmother's funeral. It took several phone calls to both TSA, ONT, and both my senate and House of representative to receive a response. The response was not timely. I have chosen to drive over 40,000 miles in the past two years, skip family gatherings, and avoid special events rather than subject myself to any kind of physical brutality at the hands of the increasing police state. I do not sign my name because I am still afraid. I have been successfully terrorized by my own government, and I refuse to be cowed into submitting to untested machines. I am not your lab rat. I am a citizen with rights. I am terrified not of a random attack, but of my government and the increasingly brutal security apparatus that has sprung out of the post 9/11 panic. I have rights. I have a right to be secure in my person, and being forced to verbal threats and physical bruising for questioning the constitutionality of a scanner and refusing to go through it runs counter to all the fairy tales I was told as a child about my rights as a citizen. I have lost faith in the United States as a result of the brutalization and callous indifference of the TSA and US Congress regarding my specific petition and complaint.
See attached file(s)

Attachments (5)

Exhibit 1

View Attachment: JPG PDF

Exhibit 2

View Attachment: JPG PDF

Exhibit 3

View Attachment: DOC PDF

Exhibit 4

View Attachment: JPG PDF

Exhibit 5

View Attachment: JPG PDF

The following events occurred on Friday, July 8, 2011 between 0745 and 0815. I took Southwest flight 1183 from ONT to MCI.

I put my possessions on the belt. The man in front of me kept alarming the metal detector. When I suggested that he take off his watch after his third attempt, a female screener told me to step to the side. My things were going through the machine, so I refused to lose line of sight on my possessions. She said that I still had to step to the side. I refused to go through the scanner; I have had several moles removed for being precancerous, so I had no intention of risking any more exposure to radiation. The screener tried to force me to stand right next to the machine, and I refused, as standing next to it defeats the purpose of avoiding extra radiation and exposure. I said "I won't be raped to fly."

I was finally allowed to step through the gate and start going towards my belongings and to maintain my line of sight when another female screener came up behind me and said she was going to do my pat down, but she suddenly started shoving me towards the belt. As I felt her hand start shoving me hard on my right shoulder, I stepped forward, turned around and said "You will NOT touch me without my consent." She called for a supervisor. A male screener started rifling through my belongings while they were still on the belt; I said "I have the right to maintain a line of sight on my things." The supervisor let me point out which things were mine and we walked to the screening area.

The negligence of the first female screener who shoved me put me in a heightened state of anxiety. I was already shaking. I rapidly told the supervisor (who never gave me her name, she only ever identified herself as "the supervisor"). I told her I would rather strip naked than go through the machine and that I didn't want to do a pat down because I had been raped in college and a pat down would be extremely traumatic. She said we could go to a private screening room. I said "I won't go to any rape room with you," as I have read several accounts of very abusive treatment in the private rooms and considering that I had been shoved only moments before, I was not leaving the public's view. She said she would have me arrested if I took off my clothes; I was well aware of that, but her tone and attitude became increasingly abusive and controlling. I asked if I could have paperwork to fill out after the pat down; she said I could have it. I nodded and said "I consent to the pat down under duress."

I told her again that I had been raped in college and that this was extremely traumatic. At some point, she pulled me up by my left arm with excessive force; this caused a bruise to appear on Wednesday, July 13, 2011. (Dr. Silvia Jones said that it could take several days for bruises to appear, especially when the trauma is deep and that I could expect other bruises to show up later as well.) I have enclosed pictures of this injury as well.

A male screener behind me looked me in the eyes, snapped his gloves behind my head and licked his lips lasciviously as I stood up to assume the position for the pat down. I maintained his gaze and said, "You will not touch me without my consent." I told the supervisor that I just wanted to go to my grandmother's funeral. She started pressing her thumb very violently and with excessive pressure into my left leg. I began to whimper from the pain of having her continually dig and grind her thumb into my knee. I began shaking more, as her negligent and violent actions made me begin to have flashbacks to having my legs spread apart violently (almost with the same amount of pressure that she was using) at the knees and being raped shortly thereafter. I was shaking more and more, and she was violently and intentionally causing me physical pain and I whimpered again and started crying. She said that she would start with my back. She finished my back. I had my eyes closed and I was trying to get through the pat down. She never told me that she would move to my chest; she never told me that she would start examining my breasts. I started shaking more and whimpering louder as the flashbacks became more and more vivid. She hissed "Just let me finish the pat down" as she started touching my breasts. When I was raped in college, my rapist told, "Just shut up and let me finish" as he caressed my breasts. I was having my breasts touched with absolutely no notice and I was already traumatized from being shoved. I began having a panic attack and started sobbing loudly as the screener's hands became my rapist's hands on my breasts. She stopped and called the cop.

She and the male screener who had snapped his gloves and licked his lips began to talk about how they "should have called the cops from the beginning and had [me] arrested". I groveled, "Please, just let me bury my grandma. Please, just let me go to her funeral." The supervisor "You have two choices," she said, "consent to the pat down or leave the airport." She went on about how "on the way home they won't be as understanding as I am." I felt threatened. She started talking about how I could be arrested and that she would make sure I was if I didn't cooperate and consent to the pat down.

The cop came. The female supervisor willfully lied to him and said "She was using abusive language and interfering with the screening process." Crying out from a panic attack and sobbing is not abusive language. At no time did I use obscenities or foul language with the supervisor. I realized in that moment when she lied to the cop that she would go through with her threat to not let me fly to my grandmother's funeral if I told the cop about how she had been hurting me earlier or the shoving from the other screener. I was still panicking, and I was terrified that the cop would have no power to get me on my flight. The cop asked me some questions. Another male passenger put his hand on my shoulder and said "We all go through this."

When the cop was in front of me and another male clerk thought the cop was blocking my line of sight, he started to go through my things, thinking I couldn't see him. I said "You will not touch my things without my presence or consent. Are you trying to steal from me? I have a right to see you go through my things. Don't do it because you see the cop is blocking my line of sight."

With the cop observing, the pat down was less violent and abusive. The wrenching and shoving into my knees stopped and she did not apply the same amount of abusive pressure on my legs during the rest of the pat down; however, she never ever said what she was going to touch—she just touched me. She never told where her hands were going, making the experience even more traumatic.

The male clerk who tried to go through my stuff admitted to the cop to "just touching your sweater." They were looking for my boarding pass, but they tried to go through my things without my consent or permission. They would not give me the paperwork that I asked for in the beginning.

I finally left the pat down area, vividly remembering a second rape where my rapist tried to drown me in a slow draining bathtub. I was covered with sweat and shaking. Looking for my gate, a different male passenger came up to me and said, "What a waste of time." I asked, "Are you mad at me?" He said, "No, it was a waste of your time and theirs."

I wrote up only part of my experience on an online forum, as to not lose the more important details. On Saturday, I noticed a very dark bruise on my left leg where I had been violently pinched and grabbed by the female supervisor who was negligent in her duties. The bruise was approximately two and a half to three inches long. Due to my grandmother's funeral, I did not take a photo that day. Due to the shoving, the abusive holding of my leg and the threat of arrest, I wanted to forget the whole thing happened. However, on Sunday, when I cleared security uneventfully in MCI, and I looked and saw the deep bruise on my leg, I decided that the abuse and threats were unwarranted and that I needed to document it. Enclosed are two photos of the bruise.

I spent the weekend having panic attacks, waking up with full sweat, and reliving the rapes. I began scratching the back of my ears, scratching my arms, grinding my knuckles into the palms of my hands and pulling hair as an unconscious, physical manifestation of the anxiety caused by the brutality and abuse I suffered from the negligent actions of the TSA agents at ONT airport Friday morning.

I landed at ONT on Sunday evening, and I asked for a supervisor. I wanted the paperwork I had been denied on Friday. The supervisor brought the paperwork and asked for my name and number. I did not want to give that information to him because I sincerely feared and still fear retaliation if I fly out of ONT and report what happened to me. I relented and gave him that information and left the airport.

On Monday, July 11, 2011, I went to the doctor. I had her record my bruises and I recounted how the anxiety had become almost unmanageable and made me get to the point where I had decided on my top three ways of committing suicide. I began reliving both the brutal treatment that left a bruise that is still dark and visible on my left leg four days later (Tuesday, July 12, 2011) and my college rapes. I was sobbing and panicking in the office. Due to my state of agitation, the doctor (Dr. Jones) made an emergency appointment with the psychiatrist. I then spoke to the psychiatrist for half an hour, and had to make a follow up appointment.

The negligent and abusive actions of several TSA clerks at ONT on Friday, July 8, 2011, has resulted in me having cascading panic attacks, needing several more appointments for mental health, needing to increase what was a sub-clinical dose of Lexapro to a much higher dose to just manage to get through the day, having vivid recalls of both the college rapes and the violent treatment of my left leg during the pat down, having a deep tissue bruise that is still visible and dark almost four days later, having a lower quality of life, and a loss of work productivity.


BURT'S BEES
Honey
LIP BALM
.15 oz. (4.25 g)
Ingredients: Beeswax, sunflower oil, coconut oil,
lanolin, comfrey root, fragrance, tocopheryl acetate
& tocopherol (vitamin E)

Tom Ritter

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3814

Tracking Number: 1jx-85z0-bum1

Document Information

Date Posted:
Jun 19, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Tom Ritter

ZIP/Postal Code:
07030

Comment

I vehemently disgaree with the AIT in use by the TSA. I'm not convinced it's safe & more importantly we can't subject it to public studies to *determine* if it's safe. I'm very convinced it has made traveling by plane a chore that people try to avoid, and hurts US air travel.

I know, for certain, that I have taken trains, driven, and not taken trips to avoid flying, and I know several of my friends and family members have as well. Traveling in the US or to the US is an ordeal that many simply try to avoid, and these devices are a big reason why.

They're ineffective for what they try to do, and there are youtube videos showing you how to bypass them either via body cavities or tricking the machines' background. I've seen the TSA regurally switch to metal detectors, or send people through metal detectors when they opt out, because it's faster. These machines cause NWK's lines to get so long it overflows the cutbacks they have for security lines and actually overflows across walkways and they have to have airline staff stand there and direct people to wait and then go.

And finally, they are extremely intrusive to people's privacy. There are reports online of TSA agents making fun of someone during their training on the device because of the size of his penis, of masectomy and colonoscopy patients being embarressed and forced to explain themselves in public, and domestic violence and harrassment victims are forced to be seen naked or groped. It prompts an air of suspicion amoung passengers ("What did he do...."). I know because I opt out of them, and the comments and looks I get at security are some of the worst - so bad you don't even want to try and comment back.

They're of dubious safety, and we can't test them; they're ineffective and expensive, they reduce the number of people flying and stunt the growth of the US air industry, and they're extremely invasive to people's privacy. These machines are wholly inappropriate for US air travel.

C

Nick B.

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3830

Tracking Number: 1jx-85z4-ekbd

Comment

I find the TSA screening procedures absurd and a major violation of privacy. In addition, the "pat down" given when opting out of the body scanners is barely short of molestation. It is uncomfortable and embarrassing, and made worse when reports surface that the procedures are not any more effective than before the body scanners and pat downs were initiated.

I am talking about articles such as this: http://www.propublica.org/article/just-how-good-are-the-tsas-body-scanners

In which congressmen themselves are lobbying against the use and efficacy of the TSA as a whole, and the controversy associated with Michael Certoff (the person behind much of the lobbying to get the body scanners established in the first place) now profitting from their use - detailed here: http://www.brasschecktv.com/videos/tsa-nonsense-and-abuse/investigate-michael-chertofffor-fraud-and-corruption.html

I have tried to avoid flying as much as possible since these changes were put into effect, opting instead to drive most places less than 12-15 hours away. I think controlled trials should be done to determine the actual efficacy of the TSA as a whole, as well as its body scanners and pat down procedures, compared to traditional metal detectors. Thus far all of the anecdotal evidence points to there being little to no difference other than the current methods inflicting more physical and psychological stress on passengers.

Document Information

Date Posted:
Jun 19, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Nick B

Country:
United States

C

Marc N. Evans

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-3980

Tracking Number: 1jx-84wa-tov9

Comment

With respect to TSA-2013-0004, I would like to inform the reviewers that prior to the installation of full body scanners I was flying at least twice per month, often bringing my family with me on these business trips, both national and international. As a direct result of the scanners I and my family have discontinued flying and will continue to avoid these devices for as long as they are in place. Don't misunderstand me, e.g. I am happy to participate in good screening practices, so long as long-term health impacts are well quantified and publically disclosed. I even support deep background checking, which I also participated in. Until a time when potential health impacting devices are removed from the screening process, I will largely avoid travel, but when required, I will drive, use a train, or use other modes of transportation.

Thank you for listening.

Marc Evans

Document Information

Date Posted:
Jun 20, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Marc Evans

Mailing Address:
265 Country View Ln

City:
Arlington

Country:
United States

State or Province:
VT

ZIP/Postal Code:
05250

June 19, 2013

Commentary on:

NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Document ID TSA-2013-0004-0001)

My recommendation is to revert to Regulatory Alternative 2, which supplements usage of the Walk-Through Metal Detector (WTMD) with pat-downs. There are several reasons that have brought me to this recommendation over today's standard of using Millimeter Wave Advanced Imaging Technology (AIT) with Automated Target Detection (ATD) for the primary screening method. First, the Millimeter Wave AIT's ATD software has a high false positive rate and is of questionable effectiveness. Second, the AIT requires more staffing over the traditional WTMD. Third, using AIT as the primary screening method slows down lines.

In my own travels, I have experienced a 66 percent false positive rate with the Millimeter Wave AIT's ATD software. This means that despite the fact that I followed the TSA's instructions and divested everything from my body as instructed, two-thirds of the time the ATD software still alarmed, or highlighted, portions of my body on the monitor showing my scan results. This means that I had to receive a pat-down despite the fact that I did not pose a threat to aviation security. Had I used the WTMD, I would not have alarmed since I had removed all metal objects from my body and the WTMD does not experience the same issue with false positives like the AIT's ATD software does.

It is true that the AIT is a better alternative for individuals who always alarm the WTMD, as the AIT allows for a targeted pat-down. This makes the pat-down experience less invasive and traumatizing for these individuals. However, the majority of passengers would not typically alarm the WTMD, so an ATD false positive results in an unnecessary pat-down and a screening experience that is more invasive than necessary.

The number of false positives can also have the effect of lulling TSOs into a false sense of security. In other words, I believe that the TSOs operating the AIT are being desensitized to ATD alarms because there are so many of them that turn out to be false positives. Many of my targeted pat-downs after using the AIT have been very "half-hearted," and had I actually been concealing a prohibited item, I do not think it would have been discovered. This issue undermines the AIT's effectiveness.

Next, operation of the AIT requires more Transportation Security Officers (TSOs) than only using the WTMD. In order to operate an AIT, two TSOs, a male and a female, are needed. A WTMD only needs one TSO. Since not all passengers are eligible to use the AIT, the WTMD still has to be staffed alongside the AIT. Since the deployment of the AIT units, this has resulted in an increase of two additional TSOs per WTMD/AIT combination. This has resulted in an increase of staffing at checkpoints, which has resulted in larger payroll costs.

Sometimes, the TSA does not even have enough staff to operate the AIT units and reverts back to the using only the WTMDs. This results in AIT units that sit unused in checkpoints. Obviously, it is not cost effective for the AIT units to sit unused in checkpoints. In addition, if the purpose of the AIT's deployment is to screen for nonmetallic objects, the TSA is not carrying out that mission by using WTMDs over the AITs when understaffed.

At no point since the introduction of the AIT into regular usage in America's checkpoints has there been 100 percent screening of passengers by AIT. Between checkpoints or lanes that only have WTMD, AIT units that are not being used, and passengers who are ineligible for the AIT (families with children under 12 years of age, passengers carrying pets, passengers unable to stand with their arms raised above their head), there have always been several passengers who have still been able to use the WTMD. This renders every AIT unit useless. If someone wanted to smuggle a nonmetallic threat into the secure area of an airport, there are a variety of opportunities for them to do so. However, even with this loophole in existence for the past three years, it hasn't happened.

Finally, regular usage of the AIT has slowed down checkpoint lines. The most obvious example of this is simply the fact that the AIT cannot scan an individual unless they are standing completely still, while the WTMD can scan an individual as they walk at a comfortable pace. As stated previously, the AIT's number of false alarms also contributes to its low throughput. With the number of passengers proceeding through American's checkpoints on the rise, a faster security screening solution is needed, and WTMDs can handle the increased number of passengers.

Based on the reasons that I have discussed, I believe that elimination of the AIT is in America's best interest. WTMDs used as primary screening, with the addition of the random element of pat-downs as a substitute for the AIT, will provide an equivalent level of security while providing for better throughput of the checkpoints and less staffing. In addition, WTMDs can be purchased and maintained for a significantly lower cost than AIT units. I strongly urge you to choose Regulatory Alternative 2.

Thank you for your consideration.

National Center for TRANSGENDER EQUALITY

Jeremiah Gold-Hopton
30135

June 20, 2013

Dear TSA:

As a member of the LGBT and allied community, I am deeply concerned that the TSA's proposed rule does nothing to protect passenger privacy and merely expands the agency's power. Transgender travelers especially are put in fear of being outed, humiliated, and facing additional screening because of their appearance, physical characteristics, or necessary personal items.

As a transgender person, this situation has caused me to completely avoid plane travel since the TSA began requiring a body scan and/or a prison-style pat-down for all air passengers. Even when traveling very long distances, I have chosen to drive my car or take a train or bus because of what I have heard from other transgender people about their experiences with TSA body scans and pat-downs.

TSA should conduct a new cost-benefit analysis that fully considers the impact of both body scanners and pat-downs on traveler privacy.

I urge TSA to adopt Regulatory Alternative #3, using walk-through metal detectors and explosive trace detection instead of body scanners and pat-downs. Alternatively, TSA should consider additional regulatory solutions that reduce reliance on body scanners and prison-style pat-downs as primary screening methods.

To the extent TSA continues the use of body scanners and pat-downs, the final rule should codify minimum protections, including guaranteeing individual passenger image data is not retained; that all physical searches are conducted by officers of the same self-identified gender; that secondary screening will be conducted in private at passenger's election; that no passenger is required to expose sensitive areas under clothing to display any item; that searches to resolve an anomaly are no more intrusive then necessary to resolve the anomaly; that screeners receive training on working with diverse populations; and that no traveler will be subject to discrimination on the basis of gender identity.

Sincerely,
Jeremiah Gold-Hopton

anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4086

Tracking Number: 1jx-84xj-dlqh

Document Information

Date Posted:
Jun 24, 2013

RIN:
1652-AA67

Show More Details

Comment

Dear Sir or Madam:

I recall quite clearly a trip our family made some number of years ago (post 9/11) to Montana. On our return home, my belt buckle triggered the airport security detector, and I was grilled by the TSA security agent in Great Falls, MT. So here you have a 40-something year old male American citizen, his wife, and his two young children wearing "dude ranch" shirts: obvious terrorists. The TSA agent apparently thought so.

You simply cannot operate in this manner. I am an American citizen. I pay taxes. I have volunteered five or more hours a week for the last 10 years. I have no criminal record; my last citation was a parking ticket over 20 years ago.

And yet, once I set foot in an airport, I am treated as a suspect, to be herded along with all the others through gates and checkpoints.

I will submit to such treatment only under duress. Which, incidentally, means I won't be flying unless absolutely necessary. I prefer to drive; unless I cross a national border, I am not subjected to such an abitrary and capricious exercise of authority.

If your goal is to destroy commercial air travel in this country, you are doing a damn fine job of it.

I understand that non-Americans can and should be questioned prior to allowing their entry into this country. But American citizens have the right of free travel in this country. We do when driving; why should we not when flying?

I would also point out that those of financial means are essentially exempt from onerous TSA "authority": private and charter aircraft are simply not subject to the same rules. Dealing with the TSA is entirely the province of middle class flyers, and affects American citizens more than anyone else.

Robin Douglas Kunzler

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I think that we should do away with the body scans they are too invasive and the TSA agent have been know to share this with friends and other sexual deviants. If it becomes mandatory I will drive instead of fly.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4103

Tracking Number: 1jx-85zi-ndr5

Document Information

Date Posted:
Jun 25, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Robin Kunzler

Mailing Address:
4826 S. 4075 W.

City:
Roy

Country:
United States

State or Province:
UT

ZIP/Postal Code:
84067

C

Margaret E. Hopper

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4120

Tracking Number: 1jx-85z9-uj4y

Comment

Gentlemen,

I once traveled by air. No longer. After a serious wreck, my trachea closes and I need water to reopen it. Airlines won't allow me to carry water on, and many other freedoms are gone, too.

It's no longer worth the effort to fly. I drive where I can and 4 years ago took a bus trip to Missouri for business. You have penalized air travel needlessly. These 'rules' don't make us any safer and myth is securely in place. You harass and terrify children and the elderly to prove how 'fair' you are, while letting true terrorists travel unchallenged as long as they behave while on board.

I suspect that even you refuse to travel by air under the conditions you foisted on the American public. Somehow, you are favored and above the rest of the people you bully under
false pretenses. How nice for you.

These new regulations are even more scandalous, if possible.

There are better ways to handle security, but this Mickey Mouse seems to be the order presently. We no longer trust you and we reserve our respect for those who make more sense. It seems that any freedoms that can be destroyed are, and no one is taking responsibility.

Has it occurred to you that your freedoms could also be lost?

Margaret Hopper

Document Information

Date Posted:
Jun 25, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Margaret Hopper

Mailing Address:
600 East 38th

City:
Silver City

Country:
United States

State or Province:
NM

ZIP/Postal Code:
88061

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4172

Tracking Number: 1jx-8637-xy4t

Document Information

Date Posted:
Jun 25, 2013

RIN:
1652-AA67

Show More Details

Comment

TSA scanners, and in fact most of the airport screening process, seem to be intended to be as intrusive, inconvenient and offensive as possible, projecting an appearance of security while offering little or no actual security.

The TSA has shown a willingness to subject travelers to technology that has a higher risk than any threat that might reasonably be posed by terrorists.

In response, I've chosen to completely avoid flying. I'm not alone in choosing to drive to destinations where I otherwise might have flown. That's not good for the airlines or tourist industry, and imposes additional burdens on the highway system.

In my view, approving further (or continued) invasions of privacy along the lines of the existing and proposed scanning technology is indefensible.

June 24, 2013

Re: **Docket No. TSA-2013-0004, Passenger Screening Using Advanced Imaging Technology**

Transgender Law Center ("TLC"). TLC is a public interest legal organization founded in 2002 and based in San Francisco that works to change law, policy, and attitudes so that all people can live safely, authentically, and free from discrimination regardless of their gender identity or expression. We envision a future where gender self-determination and authentic expression are seen as basic rights and matters of common human dignity. TLC has a particular interest in this proposed rule because we have been contacted by a number of transgender travelers who have experienced discrimination, harassment, and humiliation as a result of TSA's airport screening procedures.

While we appreciate the steps TSA has made to address concerns from the LGBT community, these concerns cannot fully be resolved within the agency's current approach to screening. The NPRM is fatally flawed, nonresponsive to the concerns identified by the Court of Appeals, and especially problematic for vulnerable traveler populations such as transgender people. Instead, the NPRM is merely a rubber stamp of unlimited authority to use privacy-invasive screening techniques. We are deeply troubled that TSA's cost-benefit analysis completely ignores real passenger privacy interests that are impacted by the proposed regulatory approach, and that the NPRM proposes neither any change in current policy nor even to codify the minimal passenger protections in current agency practice. We urge the agency to conduct a new cost-benefit analysis that fully considers the ways in which, notwithstanding existing mitigation measures, passenger privacy is in fact impacted by the current screening approach. We further urge you to adopt proposed regulatory alternative #3 (walk-through metal detectors supplemented with explosive trace detection) or, alternatively, to consider additional regulatory alternatives to reduce reliance on body scanners and prison-style pat-downs. Finally, to the extent that any final rule incorporates *any* use of body scanners and/or prison-style pat-downs, it must at a bare minimum codify protections for passengers that are already part of TSA practice.

There can be no doubt that TSA has a public trust problem, that the existing airport screening approach does impact traveler privacy, and that it disparately impacts transgender travelers among other traveler groups. We urge you in the strongest possible terms to issue a fair and well-considered final rule that provides more than a rubber stamp.

Transgender Travelers Are Disparately Affected by TSA's Invasive Screening Approach

An estimated nearly 700,000 adults in the United States, or 0.3% of the adult U.S. population, are transgender.[1] While estimates of the population of transgender children and adolescents are lacking, this population is also significant. In a national survey conducted in 2008-09, more than one in five transgender adults reported having been harassed or disrespected at the airport.[2] Since the implementation of the current regime of routine scanning and pat-downs, LGBT organizations have continued to be contacted with stories of harassment, rudeness, being singled out for additional screening, and other potentially discriminatory treatment of transgender children and adults and their loved ones. In addition, LGBT organizations continues to hear from many travelers that they are afraid of going to the airport,

---

[1] G. Gates, *How Many People Are Lesbian, Gay, Bisexual and Transgender?,* WILLIAMS INST. ON SEXUAL ORIENTATION LAW, UCLA (Apr. 2011), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Gates-How-Many-People-LGBT-Apr-2011.pdf.

[2] J.M. GRANT, L.A. MOTTET, J. TANIS, J. HARRISON, J.L HERMAN, M. KEISLING, INJUSTICE AT EVERY TURN: A REPORT OF THE NATIONAL TRANSGENDER DISCRIMINATION SURVEY, 130 (2011).

uncertain of how they will be impacted by current screening techniques or treated by Transportation Security Officers (TSOs), and in some cases are unwilling to fly as a result.

For example, we were contacted by a transgender male attorney who was returning from a legal conference when he was stopped and informed by TSA screeners that a body scan had revealed an anomaly that necessitated a physical search of his genital region. The man explained that he was transgender and had had genital reassignment surgery, the prosthetic for which had shown up on the scan. Nevertheless, he was required to remove his clothing and undergo a humiliating and invasive search of his genital region to confirm that he did not pose a security risk. We were also contacted by a transgender woman whose breast prosthesis appeared during a TSA body scan, and who was subsequently subjected to a physical "pat down" of her breasts. Airport scanners are simply unable to distinguish between "materials" that are contraband, and the social and medical prostheses some transgender people use to modify their bodies in order to have them correspond to their gender identities. As a result, transgender people risk being subjected to uniquely humiliating and degrading treatment every time they fly.

While we recognize and appreciate the modest steps TSA has taken to improve screening procedures, staff training, and traveler education with regard to this population, transgender people will always be disparately impacted by any system based on routine scrutiny of the contours of passengers' bodies under their clothes, whether by body scanners, prison-style pat-downs, or the current combination of both. Transgender people's unique bodily sensitivities, common use of sensitive prosthetics, high rates of past physical and sexual trauma, and pervasive experiences of harassment and other discrimination in all area of social life, make the routine use of even modified scanners, when paired with intensive pat-downs as the only alternative option or form of resolution, a very serious imposition on individual privacy, comfort, and well-being.

TSA's Cost-Benefit Analysis Completely Ignores Passenger Privacy Interests

The ruling of the Court of Appeals directing the agency to undertake this rulemaking was premised on a simple conclusion: "Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT [advanced imaging technology] scanner intrudes upon his or her personal privacy in a way a magnetometer does not."[3] Yet the NPRM and accompanying Initial Regulatory Impact Analysis fail to acknowledge any impact whatsoever on the privacy of the traveling public. Instead, the IRIA simply claims that the privacy protections noted by the Court of Appeals, together with the Congressional mandate for automated target recognition (ATR) software, have "adequately addressed privacy concerns."[4]

Yet while these steps are laudable, they are not reflected in the actual rule TSA has proposed. Nor do these measures eliminate all privacy impacts on the public. Even with most of these measures in place, the ruling of the Court of Appeals was premised on a real privacy impact from body scanners. While the ATR mandate is a positive step, it also does not eliminate all privacy impacts. The agency tacitly admits as much by stating in its Initial Regulatory Impact Statement that it "anticipates future advancements to AIT in … privacy protection" and by stating that its proposed regulatory approach has the "Potential for negative public perception on… privacy concerns"[5] Indeed, as the Congressional Research Service has noted, respondents in a 2010 survey identified privacy more than twice as often as delay as a primary concern with AIT.[6]

[3] EPIC v. DHS, 653 F.3d 1, 6 (D.C. Cir. 2011).
[4] IRIA at 101.
[5] IRIA at 110, 119.
[6] U.S. Congressional Research Service. Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening (7-5700; September 12, 2012), by Bart Elias.

First and most importantly, the use of body scanners as a primary screening method is inseparable from the use of highly intrusive physical pat-downs. These screening techniques are inextricable because (1) TSA relies on the alternative option of pat-downs to mitigate the privacy impact of the scanners themselves, and (2) TSA relies on the use of pat-downs to resolve many, if not most, anomalies identified by ATR. While TSA regularly cites the high rate at which passengers opt for scanning over pat-downs, this rate demonstrates not that passengers view scanners as non-intrusive, but rather that most view the alternative of a prison-style pat-down as *even more intrusive*.[7] Accordingly, pat-downs are an essential part of the operation of body scanners, and the privacy impacts of the use of pat-downs in conjunction with body scanners must be assessed in this rulemaking. Additionally, ATR does not eliminate the privacy impact of body scanners themselves. Even with this software, scanners generate and analyze data representing the contours of passengers' bodies underneath their clothing, and use this data to highlight areas of passengers' bodies that may then be subject to a pat-down.

For these reasons, an adequate regulatory impact analysis would not only identify measures the agency has taken to mitigate privacy concerns, but would also identify remaining privacy impacts on passengers, estimate the total privacy impact, and weigh this impact alongside the other costs and benefits of the proposed regulatory action. Other agencies routinely include privacy impacts on the public in their analysis of regulatory costs, and it is unacceptable for the agency not to do so in the case of a program impacting millions of members of the traveling public.

TSA Should Adopt Regulatory Alternative #3 or Consider Additional Regulatory Alternatives that Reduce Reliance on Body Scanners and Prison-Style Pat-Downs

We strongly urge the Department to adopt proposed regulatory alternative #3 as described in the NPRM (walk-through metal detectors supplemented with explosive trace detection), or alternatively, to consider additional regulatory alternatives that reduce reliance on body scanners as a primary method of checkpoint screening. Because of the intrusive, time-consuming, costly and controversial nature of body scanners, as well as persistent questions about their ability to detect the most significant threats and to avoid false positives, body scanners are not appropriate for use as a primary method of checkpoint screening.

We note that while the NPRM oddly describes the proposed regulatory alternatives in all-or-nothing terms, TSA's historical practice has been to use a mix of screening methods providing a layered approach and a certain amount of variability. Accordingly, we expect that TSA's actual regulatory alternatives actually include using both body scanners and pat-downs on a more limited basis to supplement the use of metal detectors and explosive trace detection. Curiously, the NPRM completely ignores the possibility of redeploying already-purchased scanner devices on a more limited basis, such as for random or secondary screening. Given the intrusive, time-consuming, and controversial nature of body scanners, they would be more appropriate for these more limited uses than as a primary screening method.

The Final Rule Must, at a Bare Minimum, Codify Existing Passenger Protections

Despite the significant privacy implications noted by the Court of Appeals, the proposed rule does not incorporate *any* limitation on the use of body scanners or pat-downs – not even the minimal requirements already incorporated in TSA policy and practice or mandated by Congress. If TSA ultimately chooses to maintain use of the body scanners, the final rule must, at a bare minimum, incorporate these existing protections. Because public trust is fundamental to the viability of airport screening, these protections

[7] See DHS v. EPIC, 653 F.3d 1, 10 (D.C. Cir. 2011) (pat-down alternative "allows [the traveler] to decide which of the two options … is *least* invasive" (emphasis added)).

must be codified in regulation as opposed to less formal operating procedures that are less transparent and more readily modified. These include at least the following:

1. No human viewing of individual passenger images
2. No retention of individual passenger image data
3. Providing passengers with clear notice of choices
4. All physical searches to be conducted by officers of the same self-identified gender
5. All secondary screening to be conducted in private at passenger's election, and with a witness of passenger's choice
6. No passenger required to expose sensitive areas under clothing to reveal prostheses, medical devices, or other items
7. Physical searches to resolve an anomaly detected by scanning to be no more intrusive then necessary to resolve the anomaly
8. Training for TSOs to include working with diverse traveler populations
9. Nondiscrimination on the basis of race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, parental status, or gender identity

1. Automated Target Recognition Mandate

Congress has mandated that all body scanners employ ATR software, and it would be irrational for the final rule to authorize the use of scanners without this fundamental requirement. If they are to be used, the final rule must define scanners not only as technology that allows screening without physical contact, but also as technology that allows screening without human viewing of individuals passenger images.

2. No Retention of Individual Passenger Image Data

TSA has stated that, with the use of ATR, individual passenger image data is neither viewed nor retained. The assurance that such data are not retained was central to the reasoning of the Court of Appeals in *EPIC v. DHS.*[8] Nevertheless, many passengers reasonably fear that their individual body image could be retained and viewed at a later time. If ATR is to be used, the final rule should define scanners as technology that allows screening without subsequent retention of individual passenger image data.

3. Clear Notice of Passengers' Choices

As previously stated, provision of prison-style pat-downs as an alternative to body scanners is grossly inadequate because most travelers experience these pat-downs as *even more invasive* than scanners. The proposed rule omits even this inadequate requirement.

Passengers must be provided clear notice of the choices they are given by TSA. TSA's current practice of providing this information in small print on an 11" x 14" poster, in a crowded checkpoint area where passengers are rushed to load their belongings into bins, is far from adequate to gain the informed consent needed to make this choice meaningful. The "high level of acceptance" of the scanners cited in the NPRM is rather evidence of the inadequate notice of alternatives currently provided. As the Court of Appeals noted, "Many passengers . . . remain unaware of this right [to opt out].[9] The final rule must require that

[8] 653 F.3d 1, 4, 10.
[9] *Id.* at 3.

information about passengers' screening choices be prominently posted, in plain language and in large type, at all checkpoints.

4. Physical Searches Conducted by Officers of Same Self-Identified Gender

The current use of body scanners is inseparable from the use of thorough physical pat-downs as an alternative as well as secondary screening measure. TSA's deployment of scanners cannot work without the use of pat-downs as a secondary method, and TSA's justification for use of scanners hinges on the use of pat-downs as an alternative. The inextricable link between these two, tandem checkpoint screening methods is underscored by the panel opinion of the Court of Appeals, which emphasized the importance of the pat-down alternative in mitigating the personal intrusion caused by the scanners.[10]

Accordingly, if TSA is to codify use of scanners it must also codify basic protections for the use of pat-downs. Among the most basic, minimal protections is TSA's long-standing requirement that, absent exigent circumstances, all pat-down searches be conducted by officers of the same self-identified gender as the traveler (rather than the gender listed on identification or the gender an officer assumes the traveler was assigned at birth).

5. Physical Searches Conducted in Private and with Chosen Witness at Passenger's Election

Also among the minimal protections long provided by TSA is that physical searches and other secondary screening be, at the passenger's election, conducted in a private location and with a witness of the passenger's choosing. This is also a basic expectation of passengers that must be reflected in the final rule.

6. Limitation on Requirement to Lift or Remove Clothing

Another key protection currently established in agency policy, which must appear in any final rule authorizing body scanners, is a minimal zone of privacy protection or travelers with personal medical devices or prostheses or other items under clothing that must be identified during screening. This includes not requiring passengers to lift or remove clothing in sensitive areas to reveal a prosthetic or medical device or any other item, and instead allowing travelers, when necessary, to conduct a self pat-down of the item, followed by an explosive trace detection sampling of the hands. In the context of the routine, invasive pat-downs on which the current screening approach depends, not to codify this minimal limitation would be shocking. If TSA is to authorize the use of intrusive routine pat-downs and body scanners, this fundamental protection must be included in any final rule.

7. Additional Limits on "Resolution" Pat-Downs

In addition, current TSA policy provides for "resolution" pat-downs to be limited in appropriate cases to only those areas of the body where an anomaly was detected by a body scan. If a body scan has identified an anomaly only in the area of a passenger's head or arm, for example, it is simple common sense that further screening limited only to that area will be sufficient in most cases to resolve the anomaly. If no threat object is identified in area highlighted by the scanner, any further physical screening is an unnecessary invasion of privacy and a waste of time. Any final rule that authorizes body scanners must codify a requirement that "resolution" pat-downs be limited to the area of an anomaly wherever possible.

8. Comprehensive Training for TSOs including Working with Diverse Passenger Populations

[10] *Id.* at 3, 10.

TSA has publicly committed to substantially expanding training for TSOs, including training on working with diverse passenger populations, many of which are disparately or uniquely impacted by aspects of TSA's current screening techniques – such as transgender and gender non-conforming people, people with disabilities, religious minorities, older travelers, and families with children. Robust training on these topics is essential to public trust in the screening process, and should be explicitly required by any final rule.

9. *Traveler Civil Rights Policy*

TSA's Traveler Civil Rights Policy should also be codified in any final rule, and should be expanded to include nondiscrimination on the basis of gender identity. Again, this goes to public trust in the screening process.

The Final Rule Must Use Clearly Defined Terms

In addition to completely lacking passenger protections, the proposed rule uses vague, confusing terms that fail to adequately define the agency's authority for the use of body scanning technology, or to give sufficient notice to the public of the technologies' purpose or impact on travelers.

Most notably, the proposed rule authorizes the use of "screening technology used to detect concealed anomalies" without providing any definition or context for the vague term "anomalies." As commonly defined, an anomaly is "something different, abnormal, peculiar, or not easily classified."[11] This extremely broad and amorphous term could potentially incorporate not only foreign objects that could be put to a potentially dangerous use an aviation environment, but absolutely any item, garment, or even features of the traveler's own body that are deemed to be unusual in any way. The use of this vague, undefined term fails to establish appropriate objectives and limits for security screening and invites abuse. Checkpoint screening should be expressly limited to the detection of prohibited foreign items that pose special risks of creating physical danger in the aviation environment. TSA has been unable or unwilling to publicly confirm whether current ATR software may or may not misidentify atypical bodily characteristics as anomalies. Codifying the limits of screening objectives in this way is essential to public trust.

Conclusion

We recognize the difficult job that TSA faces in protecting the nation's transportation systems and, most importantly, its travelers. We strongly believe that TSA can fulfill its security mission while respecting the rights and dignity of all passengers, and we look forward to continued dialogue and collaboration with your agency.

[11] *Merriam-Webster's Dictionary,* http://www.merriam-webster.com/dictionary/anomaly.

C

Michelle Patterson

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4226

Tracking Number: 1jx-8638-4lmy

Comment

I am a middle-age Caucasian female who works for the government - nothing about me suggests anything nefarious nor a tendency to be paranoid. And yet I find the advanced screening machines to be offensive at best, a waste of money to be sure, and the most profound rights violation. I fly about five times per year and have always refused to go through those machines; I will continue to do so. Being made to "assume the position" when rational observation and wise analysis can provide much better security is the epitome of excess and poor planning. It certainly makes road trips a lot more enticing, even though that means renting a car for me.

Document Information

Date Posted:
Jun 25, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Michelle Patterson

Before the

TRANSPORTATION SECURITY ADMINISTRATION

Arlington, V.A., 22202

	)	
In the Matter of	)	
Notice of Proposed Rulemaking	)	Docket No. TSA–2013–0004
For Passenger Screening Using	)	
Advanced Imaging Technology	)	
	)	

COMMENTS OF

THE COMPETITIVE ENTERPRISE INSTITUTE

AND

ROBERT L. CRANDALL

FORMER CHAIRMAN & CEO OF AMR AND AMERICAN AIRLINES

June 24, 2013

Prepared by:

Marc Scribner, Fellow in Land-use and Transportation Studies, Center for Economic Freedom

mscribner@cei.org

Ryan Radia, Associate Director, Center for Technology & Innovation

rradia@cei.org

Competitive Enterprise Institute

1899 L St N.W., 12th Floor

Washington, D.C. 20036

Phone: (202) 331-1010

1. Executive Summary

The Competitive Enterprise Institute (CEI) is a non-profit, non-partisan public interest organization dedicated to promoting consumer well-being by empowering individuals to make their own choices in a free market. Founded in 1984, CEI participates in cases involving civil liberties, public safety, overregulation, and governmental checks and balances.[1] CEI also filed an *amicus curiae* brief on behalf of a diverse coalition of organizations and individuals in the judicial proceeding that led to TSA's publication of the proposed rule.[2]

Robert L. Crandall is the former Chairman and CEO of AMR and American Airlines, and a current frequent flyer.

On March 26, 2013, TSA proposed a rule regarding passenger screening using advanced imaging technology after a federal appeals court ordered the agency to do so in 2011. In conducting this rulemaking, however, TSA has flouted the 2011 court order by proposing a rule that does not comport with the federal law that governs agency rulemaking. TSA has also failed to demonstrate that the proposed rule's benefits exceed its considerable costs.

2. Argument

a. Agencies Must Conduct Notice-and-Comment Rulemaking Before Imposing Substantive New Regulations Under Administrative Procedure Act

The Administrative Procedure Act ("APA") governs how administrative agencies of the United States federal government create regulations.[3] In general, when an agency seeks to regulate, it must engage in the rulemaking process described by section 553 of the APA.[4] Under Section 553, an agency must, among other things, publish a notice of its proposed rulemaking in the Federal Register and accept written comments from interested persons

[1] *See Competitive Enterprise Institute v. NHTSA*, 956 F.2d 321 (D.C. Cir. 1992) (challenge to agency rule that ignored impact on safety); *Free Enterprise Fund v. Public Co. Accounting Oversight Bd.*, 130 S.Ct. 3138 (2010) (co-counsel for petitioners); *Sackett v. EPA*, 132 S.Ct. 1367, 1375 (2012) (citing CEI *amicus* brief).

[2] Brief for Competitive Enterprise Institute et al. as Amici Curiae Supporting Petitioner, *In re EPIC* (D.C. Cir. July 19, 2012) (No. 12-1307), *available at* http://cei.org/sites/default/files/CEI%20TSA%20Amici%20Brief%20in%20Support%20of%20EPIC's%20Petition%20for%20Writ%20of%20Mandamus.pdf.

[3] 5 U.S.C. §§ 551-59 (2012) [hereinafter APA].

[4] 5 U.S.C. § 553 (2012).

about the rulemaking.[5] The agency must take these comments into consideration before adopting a final rule.[6]

Not all agency actions are subject to the APA's rulemaking requirements. In general, an agency's "interpretative rules, general statements of policy, or rules of agency organization, procedure, or practice" are exempt from the rulemaking requirement.[7] An agency may also forgo APA rulemaking when it finds "for good cause . . . that notice and public procedure [about a proposed regulation] are impracticable, unnecessary, or contrary to the public interest."[8]

When an agency seeks to make new substantive rules that will bind the general public, however, it must follow the APA's procedural requirements.[9] An agency's substantive, "legislative-type" rules "affect[] individual rights and obligations" and thus have "the force of law."[10] Conversely, an agency's "interpretive" rules "merely remind[] parties of existing duties," while statements of general policy enable agencies to announce their "tentative intentions for the future without binding themselves."[11]

b. When TSA Commenced AIT Scanning of Passengers, It Exercised Quasi-Legislative Authority Without Following APA's Rulemaking Requirements

In July 2011, the U.S. Court of Appeals for the District of Columbia Circuit ordered the Transportation Security Administration ("TSA") to "promptly" commence APA rulemaking regarding the agency's use of Advanced Imaging Technology ("AIT") scanners in U.S. airports.[12] The appeals court held that when TSA announced plans to deploy AIT scanners in airports nationwide,[13] the announcement "purport[ed] to bind"

---

[5] *Id.* § 553(b)-(c)

[6] *Id.* § 553(c)

[7] *Id.* § 553(b)(A)-(B)

[8] *Id.*

[9] *Chrysler Corp. v. Brown*, 441 U.S. 281, 302 (1979) (holding that agencies must conform with Congress's procedural requirements when exercising quasi-legislative powers pursuant to statutory authority); *Am. Hosp. Ass'n v. Bowen*, 834 F.2d 1037, 1044 (D.C. Cir. 1987).

[10] *Chrysler Corp.*, 441 U.S. at 302 (citing *Morton v. Ruiz*, 415 U.S. 199, 232-36 (1974)).

[11] *Am. Hosp. Ass'n*, 834 F.2d at 1046 (citing *Pacific Gas & Electric Co. v. FPC*, 506 F.2d 33, 38 (D.C.Cir.1974) (internal quotations omitted)).

[12] *EPIC v. DHS*, 653 F.3d 1, 12 (D.C. Cir. 2011), *available at* http://www.cadc.uscourts.gov/internet/opinions.nsf/B3100471112A40DE852578CE004FE42C/$file/10-1157-1318805.pdf.

[13] *See* Joe Sharkey, *Whole-Body Scans Pass First Airport Tests*, N.Y. TIMES, Apr. 7, 2009, at B6,

the traveling public.[14] Rules that bind the public are by definition substantive and "legislative." [15] Therefore, because TSA's plans to implement AIT scanners appeared to bind the public, the agency should have conducted notice-and-comment rulemaking pursuant to the APA, yet failed to do so.[16] TSA argued that its statement regarding AIT scanners was procedural, or alternatively, either an interpretive rule or a general statement of policy—and, therefore, exempt from the APA's rulemaking procedure. But the court disagreed, concluding that the AIT rule constituted a substantive legislative rule.[17]

In an attempt to comply with the D.C. Circuit's 2011 order, TSA published a notice of proposed rulemaking ("NPRM") in the Federal Register on March 26, 2013 regarding passenger screening using advanced imaging technology.[18] TSA proposed adding the following language to its current passenger screening regulations at 49 C.F.R. Part 1540.107:

> (d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.[19]

This brief, open-ended proposal is a far cry from the clear, informative rule the D.C. Circuit ordered TSA to promulgate.

c. TSA's Proposed Rule Merely Restates a Vague Principle Without Notifying Passengers of Their Rights and Obligations

When the D.C. Circuit ordered TSA to conduct this rulemaking, the court emphasized that "the purpose of the APA would be disserved if an agency with a broad statutory command . . . could avoid notice-and-comment rulemaking simply by promulgating a comparably broad regulation . . . and then invoking its power to interpret that statute and

available at http://www.nytimes.com/2009/04/07/business/07road.html.

[14] *Id.* at 7-8 (citing *Gen. Elec. Co. v. E.P.A.*, 290 F.3d 377, 383-84 (D.C. Cir. 2002)).

[15] *Am. Hosp. Ass'n*, *supra* n. 9, at 1046.

[16] *EPIC, supra* n. 12, at 12.

[17] *Id.* at 5.

[18] Passenger Screening Using Advanced Imaging Technology, 78 Fed. Reg. 18287-302 (proposed Mar. 26, 2013) (to be codified at 49 C.F.R. Part 1540) [hereinafter NPRM], *available at* http://www.regulations.gov/contentStreamer?objectId=0900006481245267&disposition=attachment&contentType=pdf.

[19] *Id.* at 18296.

regulation in binding the public to a strict and specific set of obligations."[20]

Yet TSA's proposed rule does little to cure the defect identified by the court. Rather, the rule leaves passengers uncertain as to whether AIT screening is mandatory and as to which technologies TSA might someday deploy. Consider the proposed rule's single-sentence definition of advanced imaging technology (AIT): a "screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened." [21]

This definition of AIT encompasses myriad technologies, including not only millimeter-wave and backscatter scanners[22]—the two "whole-body imaging" technologies the TSA has deployed throughout U.S. airports in recent years—but also every other tool, extant or otherwise, that screens passengers without making physical contact with them. A magnetometer (metal detector) also meets TSA's definition of AIT, as the device can detect whether a passenger has a metallic object on their person.[23]

Why isn't this "pat down" option mentioned in the Code of Federal Regulations?

AIT also includes "trace-detection portals," colloquially known as "puffers," which blow air on passengers to search for explosives ("concealed anomalies").[24] Puffer units are far less invasive than whole-body imaging scanners, as they do not reveal any aspects of passengers' bodies beyond the presence of explosives (or lack thereof). From 2004 to 2006, TSA deployed 94 puffer units in 37 airports, but phased out the units in 2008 due to insufficient reliability and effectiveness.[25] Yet from the

---

[20] *EPIC*, *supra* n. 12, at 10.

[21] NPRM, *supra* n. 18, at 18296.

[22] *Id.* at 18294-95 (explaining millimeter wave and backscatter units).

[23] *See, e.g.,* Blogger Bob, *Advanced Imaging Technology Off To a Great Start* [sic], TSA Blog (Apr. 20, 2010), *at* http://blog.tsa.gov/2010/04/advanced-imaging-technology-off-to.html.

[24] Eric Lipton, *Screening Tools Slow to Arrive in U.S. Airports*, N.Y. Times, Sep. 3, 2006, *at* http://www.nytimes.com/2006/09/03/us/03research.html.

[25] JOINT MAJORITY STAFF REPORT, 112TH CONG., AIRPORT INSECURITY: TSA'S FAILURE TO COST-EFFECTIVELY PROCURE, DEPLOY AND WAREHOUSE ITS SCREENING TECHNOLOGIES 6 (May 9, 2012),

traveling public's perspective, TSA's proposed rule offers absolutely no guidance as to whether they will be subjected to puffers, magnetometers, whole-body imaging screeners, or any other distinct screening technology the agency might conceive.

In this proceeding, TSA proposes a "broad regulation."[26] Yet the agency also maintains a comprehensive set of policies detailing the nature of the scanners deployed at airports and the screening options from which passengers may select when entering an airport security checkpoint.[27] For example, the TSA website and signs posted near airport security checkpoints suggest that passengers may "opt out" of backscatter or millimeter wave screening, and instead opt for pat-down screening. The proposed rule, however, makes no mention of this "opt out" option. As the D.C. Circuit held, however, it is impermissible for TSA to promulgate an indefinite rule through APA rulemaking and subsequently adopt explicit policy statements and interpretive rules that outline passengers' obligations when traveling.[28]

d. TSA Fails to Justify its Proposed Rule on Risk-Based and Cost-Benefit Grounds

TSA purports to comply with federal requirements under which an agency may "propose or adopt a regulation only upon a reasoned determination that the benefits of the intended regulation justify its costs."[29] Although TSA rightfully factors the fiscal costs of deploying whole-body imaging (WBI) scanners into the aggregate cost estimate of the proposed rule, the agency omitted many other crucial elements of a proper cost-benefit analysis. For instance, the NPRM's assessment of costs associated with WBI scanner deployment exclusively considers accounting costs, while it ignores opportunity costs.[30] Accounting costs refer to mere expenses such as labor and equipment; opportunity costs, also known as economic costs, refer to the value of best alternative not undertaken in a given effort.

Nowhere does TSA attempt to estimate relevant economic costs of the NPRM, including

---

available at http://oversight.house.gov/wp-content/uploads/2012/05/5-9-2012-Joint-TSA-Staff-Report-FINAL.pdf.

[26] *See generally* NPRM, *supra* n. 18; *see also EPIC*, *supra* n. 12, at 10.

[27] *See* Bob Burns, *Opting Out of AIT (Body Scanners)*, TSA Blog (Nov. 19, 2012), *at* http://blog.tsa.gov/2012/11/opting-out-of-ait-body-scanners.html.

[28] *See generally EPIC*, *supra* n.12.

[29] NPRM, *supra* n. 17, at 18297 (citing Executive Order (E.O.) 12866, Regulatory Planning and Review (58 Fed. Reg. 51735, Oct. 4, 1993), as supplemented by E.O. 13563, Improving Regulation and Regulatory Review (76 Fed. Reg. 3821, Jan. 21, 2011)).

[30] NPRM, *supra* n. 17, at 18299.

costs stemming from passengers shifting from relatively safe modes of transportation to less safe ones—*e.g.*, from airliners to automobiles—due to the onerous security practices, time-consuming waiting lines, and missed flights that WBI scanners exacerbate.

TSA claims it has done its due diligence with respect to risk management. But, as the agency notes in the NPRM, "the results of TSA's risk-reduction analysis are classified."[31] To be sure, we recognize that TSA rightfully wishes to classify certain sensitive aspects of WBI scanners. But this does not justify the agency's refusal to release a redacted version, or at least a summary, of its risk-reduction analysis of WBI deployment. In proposing this rule, TSA is obligated to disclose whether WBI scanners are cost-effective in reducing risk, given that the invasiveness of WBI scanners and other security procedures are likely causing potential flyers to take to the far more deadly roads, which has led to an estimated 500 additional annual road fatalities due to this modal substitution.[32]

Professors John Mueller of Ohio State University and Mark G. Stewart of the University of Newcastle in Australia are noted experts in the subjects of aviation security risk management and cost-benefit analysis. In 2011, Oxford University Press published a book by Professors Mueller and Stewart, *Terror, Security, and Money: Balancing the Risks, Costs, and Benefits of Homeland Security*, in which Mueller and Stewart analyze the economics of TSA's passenger screening policies.

In the NPRM, TSA estimates the multi-year "2012-2015 total [WBI]-related costs will be approximately $1.5 billion (undiscounted), $1.4 billion at a three percent discount rate, and $1.3 billion at a seven percent discount rate"[33]—in other words, TSA's WBI cost estimate averages $375 million per year. Mueller and Stewart in their 2011 book provide an estimate of $1.2 billion annually.[34] A 2012 Congressional Research Service study confirms Mueller and Stewart's cost estimate.[35]

The discrepancy between TSA's cost estimate and recent independent estimates appears to largely be explained by assumptions related to the quantity of WBI scanners actually deployed in airports. Mueller and Stewart correctly note that WBI passenger screening

---

[31] *Id.*

[32] John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Costs, and Benefits of Homeland Security*, New York: Oxford University Press, 2011, at 148 (citing Garrick Blalock et al., *The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel*, 50 J. LAW. ECON. 731-755 (2007)).

[33] NPRM, *supra* n. 18, at 18289.

[34] Mueller and Stewart, *supra* n. 33, at 148.

[35] Bart Elias, "Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening," *CRS Report for Congress* R42750, Washington, D.C.: Congressional Research Service, Sep. 20, 2012, at 3.

would only be effective if TSA fully deploys 1,800 AIT scanners in all airport general passenger screening lines, as a potential terrorist intent on downing an airliner with body-borne explosives would need only to observe which airports or security areas lack WBI scanners to defeat the security measure. The significantly lower cost estimates contained in the NPRM fail to include an estimate of the number of WBI scanners TSA anticipates will be deployed, while other assumptions are neither explained nor even referenced by TSA in the NPRM or RIA.

After reviewing the literature, Mueller and Stewart concluded that (1) the expected cost of a successful attack that brings down an airliner is $26 billion,[36] and (2) universal deployment of WBI scanners reduces by an additional 8.6 percent the likelihood that a terrorist will succeed in downing an airliner with body-borne explosives.[37]

The benefits of WBI, as with any screening device, depend not only on the effectiveness of the technology in detecting threats, but also on the "baseline" annual attack probability—that is, the likelihood that a successful attack will occur in any given year absent WBI deployment. In other words, as the frequency with which terrorists attempt to smuggle body-borne explosives onto airliners increases, so too do the risk benefits of WBI.

To determine whether investing in a proposed safety enhancement passes the muster of a cost-benefit analysis, risk assessments typically employ the following basic equation:

$$\frac{Cost}{(Damage)(Risk\ Reduction)} \tag{1}$$

Based on Mueller and Stewart's estimate of annual WBI deployment costs ($1.2 billion), their estimated cost of a downed airliner ($26 billion), and the additional airliner loss risk reduction from WBI scanners (8.6 percent), they arrive at the annual attack probability:

$$\frac{1.2}{(26)(0.086)} \tag{2}$$

$$\frac{1.2}{2.236} = 0.537 = 53.7\%^{38} \tag{3}$$

In other words, the benefits of deploying WBI scanners justify the costs only if the baseline annual probability of a successful attack (absent WBI scanners) exceeds 53

[36] Mueller and Stewart, *supra* n. 33, at 149.

[37] *Id.* at 151.

[38] *Id.* at 152.

percent—or one downed airliner every two years. This analysis assumes TSA will fully deploy 1,800 WBI scanners, while TSA's cost estimates imply a significantly lower or slower rollout. Taken together, one must conclude the actual risk reduction of WBI deployment is far lower than the above estimate.

However, a doubling of both the estimated average loss of a successful body-borne explosive airliner attack ($26 billion to $52 billion) and the additional airliner loss risk reduction from WBI scanners (8.6 percent to 17.2 percent), the annual likelihood of a successful attack absent WBI scanners would need to exceed 13 percent—or about once every eight years. Outside of two coordinated detonations in the Russian Federation in 2004, there have been no documented successful body-borne explosive attacks bringing down airliners. Given the complete absence of successful body-borne explosive attacks downing airliners in developed countries at any time in history, this revised probability is still almost certainly too high to justify the costs of WBI deployment.

As Mueller and Stewart conclude:

> Since it appears that exceedingly few suicide terrorists with body-borne explosives have planned, yet alone attempted, to board an aircraft anywhere, the likelihood of a successful attack, absent body scanners, is unlikely to be anywhere near one every two years. By this criterion, the scanners fail a cost-benefit analysis quite comprehensively, and the $1.2 billion per year in taxpayer money might be used more productively elsewhere.[39]

Before critical public and independent expert review can take place, TSA must declassify the results of its AIT risk-reduction analysis. Again, references to specific threats or security practices can justifiably be redacted, but withholding the results in their entirety undermines both the legitimacy of the current aviation security regime and the public's right to meaningfully examine the costs and benefits of controversial and consequential technology currently deployed in airports.

3. Conclusion

For the reasons above, TSA should immediately reverse its decision to deploy WBI scanners in airports nationwide. Instead, TSA should adopt regulatory alternative 3,[40] whereby "Walk Through Metal Detectors" remain the primary passenger screening technology, augmented by Explosives Trace Detection. Until TSA is able to show the benefits of WBI exceed its costs, alternative 3 is the only prudent option.

---

[39] *Id.* at 152.

[40] NPRM, *supra* n. 17, at 18301.

Respectfully Submitted,

COMPETITIVE ENTERPRISE INSTITUTE

ROBERT L. CRANDALL

Prepared by:

Marc Scribner, Fellow in Land-use and Transportation Studies, Center for Economic Freedom

mscribner@cei.org

Ryan Radia, Associate Director, Center for Technology & Innovation

rradia@cei.org

Competitive Enterprise Institute

1899 L St N.W., 12th Floor

Washington, D.C. 20036

Phone: (202) 331-1010

C

Jeffrey A. Strauser

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4265

Tracking Number: 1jx-860e-u7in

Comment

I am totally against full-body scanners (nude-scanners) for many reasons. First is they are against the fourth amendment (despite some opinions by political anti- American judges). And it has been repeatedly proven (as most TSO's admit to) the full-body scanners don't work.
TSA illegally rushed into a $250 million dollar mistake that has violated the 4th Amendment, exposed passengers to unnecessary radiation, created child pornography, and led to countless women and children being humiliated, harassed, and raped (rape according to the FBI is penetration, however slight). The TSA continuously ignores court orders which makes the TSA a criminal organization.
My wife and my children no longer take our grandchildren on any flights in the U.S.. We now need to drive everywhere. We are the only country on planet earth where it is not safe for children to fly. We now need to fly out of Canada.
Now the totally corrupt TSA (I mean management, I know there are many honest TSO's who actually care about passenger safety, unlike Pistole or Napalatano) is removing and scrapping over 40 million dollars in nearly new X-ray porno scanners due to the lack of ATR and the severe cancer risk (which every cancer expert knew from the beginning). The TSA only got rid of the X-ray scanners when congress ordered them to do so. They still defied congress and took a full year more than legally allowed. According to the TSA they have authority to strip-search each and every passenger.
AIT was tested in prisons and had an over 50% failure rate. No country other than the US allowed the cancer causing X-ray porno-scanners in their airports. And most got rid of the MMW porno-scanners because they do not work. And they still take nude pictures of victims. The ATR is just a cover-up. I am sure there are still TSA perverts and US Senators somewhere who still ogle the naked pictures of children. However, the ATR is still a step in the right direction as it restricts the # of perverts

Document Information

Date Posted:
Jun 25, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Jeffrey Strauser

Mailing Address:
10243 Lakeside Boulevard

City:
Dunkirk

Country:
United States

State or Province:
NY

ZIP/Postal Code:
14048

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4414

Tracking Number: 1jx-8613-h7ay

Comment

Please know that my friends and family travel by car whenever possible due to the new TSA screening procedures used at airlines.
Not only is the imaging technology invasive, it is also
expensive
ineffective
unsafe
unnecessary
unconstitutional.
The people have spoken and we vote against the use of this technology.

Document Information

Date Posted:
Jun 26, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

C

C.J. Lindell

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4447

Tracking Number: 1jx-862g-kmc2

Comment

I am strongly opposed to the current security measures being used in airports, especially the use of AIT scanners. These scanners have been proven ineffective and are a gross violation of privacy, dignity and civil rights, subjecting innocent citizens to a highly invasive search without cause. The “enhanced” (i.e. punitive and abusive) pat-downs go WAY too far, cause serious trauma to abuse survivors and many others, and would be cause for immediate arrest if done by anyone outside the government. I was once a frequent traveler but have avoided airports whenever possible for the past four years, preferring a drive of several hours/days rather than be subjected to the unacceptable activities occurring at our airports today. This should NOT be happening in America. There is no way to 100% prevent the risks involved in flying or anything else, and I accept that as a fact of life. But this unnecessary assault by the U.S. government on the dignity and rights of its citizens IS preventable and should be ceased immediately.

Document Information

Date Posted:
Jun 27, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
CJ Lindell

City:
Los Angeles

Country:
United States

State or Province:
CA

Comment on NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Document ID TSA-2013-0004-0001)

Mark H. Lyon

The risk of death by terrorism in the U.S. is lower than 1 in 3.5 million. In fact, death by furniture is more likely than death by terrorism. Many of the processes used in the screening exercise are mere theater, designed to make people feel better about the security measures than in actually accomplishing the goal of increasing security. The only truly effective measures taken in the wake of the 9/11 attacks were strengthening cockpit doors and teaching passengers and crew that it is necessary to fight hijackers.

Unfortunately, the scanners slow the progress of passengers through the checkpoint, creating an even more attractive (and accessible) target for terrorism. If terrorists were truly prevalent in America, certainly one or more would have been clever enough to bring a firearm or explosive device and use it on the long lines of passengers waiting to be screened. None of the TSA's operations would prevent such an attack; the fact that one has not occurred is a testament to the scarcity of such bad actors in our society.

As an overweight person, it is clear to me that the TSA's body scanners and follow-up pat-down are easily circumvented. Because the scanners cannot see through skin, any area where the body overlaps - as happens in overweight people - can be used to conceal weapons, including those made of metal. Even when an individual opts out, the shamefulness of the process for TSA screeners can often result in a less-than-thorough screening, particularly of overweight people.

Without requiring individuals to also pass thorough a magnetometer, the body scanners are incapable of providing the same level of security against metallic objects as traditional screening. Items concealed in non-obvious places can easily be passed through the screening process that would otherwise have been stopped with the earlier technology.

TSA's body scanner rule is not sufficiently detailed to inform the public how scanners will be used and how the information collected will be stored and maintained. As one concerned about my privacy, but who is also sometimes required to fly, I do not wish to have unnecessary and inappropriate information collected and used in unknown ways.

Both before and after the proposed rule-making, passengers have been given almost no information about what search will be conducted. Attempts to collect this information, such as by observing or documenting the screening process, result in intimidation and threat. I personally experienced this at JFK Terminal 4 when I was threatened with arrest for taking a photograph of the baggage screening taking place in the public portion of the airport.

Surely the most basic element of consent is to know what one is consenting to. The proposed rule implies that passengers who submit to a body scanner will not be touched, but this is belied by the huge number of people who endure a manual search after passing through a body scanner. Under what conditions will passengers who use body scanners be touched? Will screeners lay their hands on our genitalia through our clothing if the body scanner shows an alarm? What is the alternative search procedure if passengers opt out of the body scanners? Will screeners lay their hands on our genitalia through our clothing if we opt out?

Because of the TSA's body scanner program, I have shifted a large proportion of my travel to driving trips. Driving is a far more dangerous proposition than flying, but I would rather take the risk of dying than let a complete stranger create nude images of me or touch my genitals. The TSA offends people and causes diversion from the airplanes to the roads, which means that the TSA causes 15 excess road deaths for every million passengers diverted. If just 1% of the 700 million annual would-be air passengers decide to drive instead of flying because of the body scanners, then the TSA's body scanner program will kill more than 100 people.

Pride Foundation

pridefoundation.org

June 24, 2013

Re: **Docket No. TSA-2013-0004, Passenger Screening Using Advanced Imaging Technology**

Pride Foundation is pleased to provide the following comments on the above notice of proposed rulemaking (NPRM). Pride Foundation is a donor-supported community foundation that inspires a culture of generosity by connecting and strengthening organizations, leaders, and students who are advancing equality for lesbian, gay, bisexual, transgender, and queer (LGBTQ) people and their families in the Northwest. We work with individuals, families, and organizations in Alaska, Idaho, Montana, Oregon, and Washington. Each of these states has differing policies related to gender identity, changing names and gender markers on identification. This can be a challenge for a transgender traveler, one who present as their gender identity, but may or may not have identification with a gender marker that is consistent with their identity and presentation. In addition, like many transgender people across the country, our transgender community members may not have access to or the financial means to afford medical transition.

We would also add that many of the airports in the states we represent are smaller in size and it is more likely that personnel, including TSA agents, and other travelers, may know each other. What someone may not know is that their fellow traveler is transgender. If a transgender traveler is forced to disclose their transgender status, because of wearing a prosthetic or the incongruity of one's body with that of their gender expression, which is often verbally labeled as an "anomaly" by TSA agent in the screening line, these actions may be putting that transgender traveler at risk for discrimination or violence. Three of the five states we operate in do not have statewide laws for non-discrimination protections for gender identity or sexual orientation. The impact of being outed could have a ripple effect, affecting one's employment, housing, and quality of life.

Additionally, what are the standards of confidently for TSA agents about disclosing personal information, much of which for a transgender traveler is personal medical information, among other agents or other airport personnel? The fear of being outed at the screening area of airport security is enough to stop some transgender people from flying, not only do they lose out, but so does the airline industry, the other commercial industries associated with airports, as well as the state and federal government that relies on the taxes collected.

While we appreciate the steps TSA has made to address concerns from the LGBT community, these concerns cannot fully be resolved within the agency's current approach to screening. The NPRM is fatally flawed, nonresponsive to the concerns identified by the Court of Appeals, and especially problematic for vulnerable traveler populations such as transgender people. Instead, the NPRM is merely a rubber stamp of unlimited authority to use privacy-invasive screening techniques. We are deeply troubled that TSA's cost-benefit analysis completely ignores real passenger privacy interests that are impacted by the proposed regulatory approach, and that the NPRM proposes neither any change in current policy nor even to codify the minimal passenger protections in current agency practice. We urge the agency to conduct a new cost-benefit analysis that fully considers the ways in which, notwithstanding existing mitigation measures, passenger privacy is in fact impacted by the current screening approach. We further urge you to adopt proposed regulatory alternative #3 (walk-through metal detectors supplemented with explosive trace detection) or, alternatively, to consider additional regulatory alternatives to reduce reliance on body scanners and prison-style pat-downs. Finally, to the extent that any final rule incorporates *any* use of body scanners and/or prison-style pat-downs, it must at a bare minimum codify protections for passengers that are already part of TSA practice.

There can be no doubt that TSA has a public trust problem, that the existing airport screening approach does impact traveler privacy, and that it disparately impacts transgender travelers among other traveler groups. We urge you in the strongest possible terms to issue a fair and well-considered final rule that provides more than a rubber stamp.

Transgender Travelers Are Disparately Affected by TSA's Invasive Screening Approach

An estimated nearly 700,000 adults in the United States, or 0.3% of the adult U.S. population, are transgender.[1] While estimates of the population of transgender children and adolescents are lacking, this population is also significant. In a national survey conducted in 2008-09, more than one in five transgender adults reported having been harassed or disrespected at the airport.[2] Since the implementation of the current regime of routine scanning and pat-downs, LGBT organizations have continued to be contacted with stories of harassment, rudeness, being singled out for additional screening, and other potentially discriminatory treatment of transgender children and adults and their loved ones. In addition, LGBT organizations continues to hear from many travelers that they are afraid of going to the airport, uncertain of how they will be impacted by current screening techniques or treated by Transportation Security Officers (TSOs), and in some cases are unwilling to fly as a result.

While we recognize and appreciate the modest steps TSA has taken to improve screening procedures, staff training, and traveler education with regard to this population, transgender people will always be disparately impacted by any system based on routine scrutiny of the contours of passengers' bodies under their clothes, whether by body scanners, prison-style pat-downs, or the current combination of both. Transgender people's unique bodily sensitivities, common use of sensitive prosthetics, high rates of past physical and sexual trauma, and pervasive experiences of harassment and other discrimination in all area of social life, make the routine use of even modified scanners, when paired with intensive pat-downs as the only alternative option or form of resolution, a very serious imposition on individual privacy, comfort, and well-being.

TSA's Cost-Benefit Analysis Completely Ignores Passenger Privacy Interests

The ruling of the Court of Appeals directing the agency to undertake this rulemaking was premised on a simple conclusion: "Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT [advanced imaging technology] scanner intrudes upon his or her personal privacy in a way a magnetometer does not."[3] Yet the NPRM and accompanying Initial Regulatory Impact Analysis fail to acknowledge any impact whatsoever on the privacy of the traveling public. Instead, the IRIA simply claims that the

---

[1] G. Gates, *How Many People Are Lesbian, Gay, Bisexual and Transgender?,* WILLIAMS INST. ON SEXUAL ORIENTATION LAW, UCLA (Apr. 2011), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Gates-How-Many-People-LGBT-Apr-2011.pdf.
[2] J.M. GRANT, L.A. MOTTET, J. TANIS, J. HARRISON, J.L HERMAN, M. KEISLING, INJUSTICE AT EVERY TURN: A REPORT OF THE NATIONAL TRANSGENDER DISCRIMINATION SURVEY, 130 (2011).
[3] EPIC v. DHS, 653 F.3d 1, 6 (D.C. Cir. 2011).

privacy protections noted by the Court of Appeals, together with the Congressional mandate for automated target recognition (ATR) software, have "adequately addressed privacy concerns."[4]

Yet while these steps are laudable, they are not reflected in the actual rule TSA has proposed. Nor do these measures eliminate all privacy impacts on the public. Even with most of these measures in place, the ruling of the Court of Appeals was premised on a real privacy impact from body scanners. While the ATR mandate is a positive step, it also does not eliminate all privacy impacts. The agency tacitly admits as much by stating in its Initial Regulatory Impact Statement that it "anticipates future advancements to AIT in privacy protection" and by stating that its proposed regulatory approach has the "Potential for negative public perception on privacy concerns"[5] Indeed, as the Congressional Research Service has noted, respondents in a 2010 survey identified privacy more than twice as often as delay as a primary concern with AIT.[6]

First and most importantly, the use of body scanners as a primary screening method is inseparable from the use of highly intrusive physical pat-downs. These screening techniques are inextricable because (1) TSA relies on the alternative option of pat-downs to mitigate the privacy impact of the scanners themselves, and (2) TSA relies on the use of pat-downs to resolve many, if not most, anomalies identified by ATR. While TSA regularly cites the high rate at which passengers opt for scanning over pat-downs, this rate demonstrates not that passengers view scanners as non-intrusive, but rather that most view the alternative of a prison-style pat-down as *even more intrusive*.[7] Accordingly, pat-downs are an essential part of the operation of body scanners, and the privacy impacts of the use of pat-downs in conjunction with body scanners must be assessed in this rulemaking. Additionally, ATR does not eliminate the privacy impact of body scanners themselves. Even with this software, scanners generate and analyze data representing the contours of passengers' bodies underneath their clothing, and use this data to highlight areas of passengers' bodies that may then be subject to a pat-down.

For these reasons, an adequate regulatory impact analysis would not only identify measures the agency has taken to mitigate privacy concerns, but would also identify remaining privacy impacts on passengers, estimate the total privacy impact, and weigh this impact alongside the other costs and benefits of the proposed regulatory action. Other agencies routinely include privacy impacts on the public in their analysis of regulatory costs, and it is unacceptable for the agency not to do so in the case of a program impacting millions of members of the traveling public.

TSA Should Adopt Regulatory Alternative #3 or Consider Additional Regulatory Alternatives that Reduce Reliance on Body Scanners and Prison-Style Pat-Downs

We strongly urge the Department to adopt proposed regulatory alternative #3 as described in the NPRM (walk-through metal detectors supplemented with explosive trace detection), or alternatively, to consider additional regulatory alternatives that reduce reliance on body scanners as a primary method of checkpoint screening. Because of the intrusive, time-consuming, costly and controversial nature of body scanners, as well as persistent questions

[4] IRIA at 101.
[5] IRIA at 110, 119.
[6] U.S. Congressional Research Service. Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening (7-5700; September 12, 2012), by Bart Elias.
[7] See DHS v. EPIC, 653 F.3d 1, 10 (D.C. Cir. 2011) (pat-down alternative "allows [the traveler] to decide which of the two options … is *least* invasive" (emphasis added)).

about their ability to detect the most significant threats and to avoid false positives, body scanners are not appropriate for use as a primary method of checkpoint screening.

We note that while the NPRM oddly describes the proposed regulatory alternatives in all-or-nothing terms, TSA's historical practice has been to use a mix of screening methods providing a layered approach and a certain amount of variability. Accordingly, we expect that TSA's actual regulatory alternatives actually include using both body scanners and pat-downs on a more limited basis to supplement the use of metal detectors and explosive trace detection. Curiously, the NPRM completely ignores the possibility of redeploying already-purchased scanner devices on a more limited basis, such as for random or secondary screening. Given the intrusive, time-consuming, and controversial nature of body scanners, they would be more appropriate for these more limited uses than as a primary screening method.

The Final Rule Must, at a Bare Minimum, Codify Existing Passenger Protections

Despite the significant privacy implications noted by the Court of Appeals, the proposed rule does not incorporate *any* limitation on the use of body scanners or pat-downs – not even the minimal requirements already incorporated in TSA policy and practice or mandated by Congress. If TSA ultimately chooses to maintain use of the body scanners, the final rule must, at a bare minimum, incorporate these existing protections. Because public trust is fundamental to the viability of airport screening, these protections must be codified in regulation as opposed to less formal operating procedures that are less transparent and more readily modified. These include at least the following:

1. No human viewing of individual passenger images
2. No retention of individual passenger image data
3. Providing passengers with clear notice of choices
4. All physical searches to be conducted by officers of the same self-identified gender
5. All secondary screening to be conducted in private at passenger's election, and with a witness of passenger's choice
6. No passenger required to expose sensitive areas under clothing to reveal prostheses, medical devices, or other items
7. Physical searches to resolve an anomaly detected by scanning to be no more intrusive then necessary to resolve the anomaly
8. Training for TSOs to include working with diverse traveler populations
9. Nondiscrimination on the basis of race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, parental status, or gender identity

1. Automated Target Recognition Mandate

Congress has mandated that all body scanners employ ATR software, and it would be irrational for the final rule to authorize the use of scanners without this fundamental requirement. If they are to be used, the final rule must define scanners not only as technology that allows screening without physical contact, but also as technology that allows screening without human viewing of individuals passenger images.

2. No Retention of Individual Passenger Image Data

TSA has stated that, with the use of ATR, individual passenger image data is neither viewed nor retained. The assurance that such data are not retained was central to the reasoning of the Court of Appeals in *EPIC v. DHS.*[8] Nevertheless, many passengers reasonably fear that their individual body image could be retained and viewed at a later time. If ATR is to be used, the final rule should define scanners as technology that allows screening without subsequent retention of individual passenger image data.

3. Clear Notice of Passengers' Choices

As previously stated, provision of prison-style pat-downs as an alternative to body scanners is grossly inadequate because most travelers experience these pat-downs as *even more invasive* than scanners. The proposed rule omits even this inadequate requirement.

Passengers must be provided clear notice of the choices they are given by TSA. TSA's current practice of providing this information in small print on an 11" x 14" poster, in a crowded checkpoint area where passengers are rushed to load their belongings into bins, is far from adequate to gain the informed consent needed to make this choice meaningful. The "high level of acceptance" of the scanners cited in the NPRM is rather evidence of the inadequate notice of alternatives currently provided. As the Court of Appeals noted, "Many passengers . . . remain unaware of this right [to opt out].[9] The final rule must require that information about passengers' screening choices be prominently posted, in plain language and in large type, at all checkpoints.

4. Physical Searches Conducted by Officers of Same Self-Identified Gender

The current use of body scanners is inseparable from the use of thorough physical pat-downs as an alternative as well as secondary screening measure. TSA's deployment of scanners cannot work without the use of pat-downs as a secondary method, and TSA's justification for use of scanners hinges on the use of pat-downs as an alternative. The inextricable link between these two, tandem checkpoint screening methods is underscored by the panel opinion of the Court of Appeals, which emphasized the importance of the pat-down alternative in mitigating the personal intrusion caused by the scanners.[10]

Accordingly, if TSA is to codify use of scanners it must also codify basic protections for the use of pat-downs. Among the most basic, minimal protections is TSA's long-standing requirement that, absent exigent circumstances, all pat-down searches be conducted by officers of the same self-identified gender as the traveler (rather than the gender listed on identification or the gender an officer assumes the traveler was assigned at birth).

5. Physical Searches Conducted in Private and with Chosen Witness at Passenger's Election

Also among the minimal protections long provided by TSA is that physical searches and other secondary screening be, at the passenger's election, conducted in a private location and with a witness of the passenger's choosing. This is also a basic expectation of passengers that must be reflected in the final rule.

6. Limitation on Requirement to Lift or Remove Clothing

[8] 653 F.3d 1, 4, 10.
[9] *Id.* at 3.
[10] *Id.* at 3, 10.

Another key protection currently established in agency policy, which must appear in any final rule authorizing body scanners, is a minimal zone of privacy protection or travelers with personal medical devices or prostheses or other items under clothing that must be identified during screening. This includes not requiring passengers to lift or remove clothing in sensitive areas to reveal a prosthetic or medical device or any other item, and instead allowing travelers, when necessary, to conduct a self pat-down of the item, followed by an explosive trace detection sampling of the hands. In the context of the routine, invasive pat-downs on which the current screening approach depends, not to codify this minimal limitation would be shocking. If TSA is to authorize the use of intrusive routine pat-downs and body scanners, this fundamental protection must be included in any final rule.

7. *Additional Limits on "Resolution" Pat-Downs*

In addition, current TSA policy provides for "resolution" pat-downs to be limited in appropriate cases to only those areas of the body where an anomaly was detected by a body scan. If a body scan has identified an anomaly only in the area of a passenger's head or arm, for example, it is simple common sense that further screening limited only to that area will be sufficient in most cases to resolve the anomaly. If no threat object is identified in area highlighted by the scanner, any further physical screening is an unnecessary invasion of privacy and a waste of time. Any final rule that authorizes body scanners must codify a requirement that "resolution" pat-downs be limited to the area of an anomaly wherever possible.

8. *Comprehensive Training for TSOs including Working with Diverse Passenger Populations*

TSA has publicly committed to substantially expanding training for TSOs, including training on working with diverse passenger populations, many of which are disparately or uniquely impacted by aspects of TSA's current screening techniques – such as transgender and gender non-conforming people, people with disabilities, religious minorities, older travelers, and families with children. Robust training on these topics is essential to public trust in the screening process, and should be explicitly required by any final rule.

9. *Traveler Civil Rights Policy*

TSA's Traveler Civil Rights Policy should also be codified in any final rule, and should be expanded to include nondiscrimination on the basis of gender identity. Again, this goes to public trust in the screening process.

The Final Rule Must Use Clearly Defined Terms

In addition to completely lacking passenger protections, the proposed rule uses vague, confusing terms that fail to adequately define the agency's authority for the use of body scanning technology, or to give sufficient notice to the public of the technologies' purpose or impact on travelers.

Most notably, the proposed rule authorizes the use of "screening technology used to detect concealed anomalies" without providing any definition or context for the vague term "anomalies." As commonly defined, an anomaly is "something different, abnormal, peculiar, or not easily classified."[11] This extremely broad and amorphous term could potentially incorporate not only foreign objects that could be put to a potentially dangerous use an aviation environment, but absolutely any item, garment, or even features of the traveler's own body that are deemed to be unusual in any way. The use of this vague, undefined term fails to establish appropriate objectives and limits for security screening and invites abuse. Checkpoint screening should be expressly limited to the detection of prohibited foreign items that pose special risks of creating physical danger in the aviation environment. TSA has been unable or unwilling to publicly confirm whether current ATR software may or may not misidentify atypical bodily characteristics as anomalies. Codifying the limits of screening objectives in this way is essential to public trust.

Conclusion

We recognize the difficult job that TSA faces in protecting the nation's transportation systems and, most importantly, its travelers. We strongly believe that TSA can fulfill its security mission while respecting the rights and dignity of all passengers, and we look forward to continued dialogue and collaboration with your agency.

Sincerely,

Kris A. Hermanns
Executive Director

[11] *Merriam-Webster's Dictionary,* http://www.merriam-webster.com/dictionary/anomaly.

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

As a past victim of sexual assault with a resulting PTSD diagnosis, I find the choice of being irradiated or patted down in the manner TSA agents must do in order to clear you if you opt out one I cannot make without being significantly retraumatized. I've had to cut down my flying to only critical trips, otherwise relying on the far less-safe transportation method of driving to avoid such incidents. While I *may* be able to comprehend such requirements were it to actually prove effective, the reactive security theater that has resulted from the September 11th attacks doesn't appear to be either cost-effective or effective in terms of results.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4553

Tracking Number: 1jx-863e-opdo

Document Information

Date Posted:
Jun 27, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4562

Tracking Number: 1jx-863e-3wru

Comment

I refuse to go through the scanners as it simply gives me the creeps. As for the pat-down, now that I am a parent, I cannot truly imagine the rage I would feel seeing my child treated like I have been. As such, when traveling, I will drive whenever possible, and leave my children at home when flying, because the pat downs are pure and simple sexual assault, and I cannot expose my children to that.

These procedures are shameful and degeneratong of our core societal values. Maybe if it ever ONCE prevented a terrorist plot, it would be defensible, but all it seems to do is prevent honest people from travelling honestly with their dignity intact.

Document Information

Date Posted:
Jun 27, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Anonymous

Country:
United States

State or Province:
IL

Amber Worth

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4565

Tracking Number: 1jx-8613-gtbv

Document Information

Date Posted:
Jun 27, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Amber Worth

Country:
United States

ZIP/Postal Code:
33701

Comment

"Dear TSA:

As member of the LGBT and allied community, I am deeply concerned that the TSA's proposed rule does nothing to protect passenger privacy and merely expands the agency's power. Transgender travelers especially are put in fear of being outed, humiliated, and facing additional screening because of their appearance, physical characteristics, or necessary personal items.

The harassment I've gone through at the hands of the TSA has made me scared for my life to the point I have stopped traveling by air to avoid going through the heckling and embarrassment caused by the screenings. Since I work in avionics, this has forced me to drive thousands of miles at a stretch, just to get to a job that I used to be able to fly to.

TSA should conduct a new cost-benefit analysis that fully considers the impact of both body scanners and pat-downs on traveler privacy.

I urge TSA to adopt Regulatory Alternative #3, using walk-through metal detectors and explosive trace detection instead of body scanners and pat-downs. Alternatively, TSA should consider additional regulatory solutions that reduce reliance on body scanners and prison-style pat-downs as primary screening methods.

To the extent TSA continues the use of body scanners and pat-downs, the final rule should codify minimum protections, including guaranteeing individual passenger image data is not retained; that all physical searches are conducted by officers of the same self-identified gender; that secondary screening will be conducted in private at passenger's election; that no passenger is required to expose sensitive areas under clothing to display any item; that searches to resolve an anomaly are no more intrusive then necessary to resolve the anomaly; that screeners receive training on working with diverse populations; and that no traveler will be subject to discrimination on the basis of gender identity.

Sincerely,
Amber Worth

C

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4576

Tracking Number: 1jx-863c-zabi

Comment

I wish to express my outrage about the Passenger Screening Using Advanced Imaging Technology. I not only object to the nude body images visible, but also to the TSA's "grope" policy if one chooses to "opt out". To date the TSA has not apprehended one single so called terrorist, but bullied, harassed, and treated the flying public with contempt. This is NOT the country I grew up in, as I see our rights systematically trampled on in the name of "safety". I have chosen never to fly again as long as the TSA exists as it does. I would rather drive 3000 miles to see my son graduate next year than subject my disabled wife and myself to the thugs wearing TSA uniforms.

Document Information

Date Posted:
Jun 27, 2013

RIN:
1652-AA67

Show More Details

THE SIKHCOALITION
the voice of a people

June 24, 2013

Ms. Chawanna Carrington
Project Manager, Passenger Screening Program
Office of Security Capabilities
Transportation Security Administration
701 South 12th Street
Arlington, VA 20598-6016

Re: TSA-2013-0004-0001 (NPRM: Passenger Screening Using Advanced Imaging Technology)

Dear Ms. Carrington:

As the largest Sikh civil rights organization in the United States, the Sikh Coalition has worked with the Transportation Security Administration (TSA) for several years to address persistent concerns about profiling based on suspect classifications—including race, ethnicity, religion, and national origin—at our nation's airports. In this context, we respectfully submit this comment to highlight deficiencies in TSA's proposed rule on the use of Advanced Imaging Technology (AIT) at our nation's airports. In short, in light of the experiences of Sikh American travelers, we believe that the proposed rule's description of the efficacy of AIT machines may be misleading, and that the proposed rule should be modified to allay concerns about profiling by TSA.

A. Background

The Sikh Coalition is concerned that TSA screeners are subjecting Sikh travelers to profiling based on suspect classifications. According to TSA's website, air travelers who wear religious headcoverings, including Sikh turbans, are subject to the "possibility of additional security screening, which may include a pat-down search of the head covering."[1] Additional screening is justified, according to the TSA, "if the security officer cannot reasonably determine that the head area is free of a detectable threat item,"[2] even after a traveler passes through a screening device without incident. In practice, however, instead of being subject to the 'possibility' of additional screening, Sikh travelers who wear turbans have been advised by TSA personnel that such screening is mandatory, resulting in 100 percent additional/secondary screening rates of Sikhs at many American airports.

Ironically, Sikhs continue to experience disparate rates of secondary screening despite the deployment of AIT machines nationwide. While the TSA's website states that AIT machines "safely [screen] passengers for metallic and nonmetallic threats including weapons, explosives and other objects concealed under layers of clothing without physical contact,"[3] and while the proposed rule repeatedly makes similar claims, Sikhs are routinely subjected to pat downs after clearing the machines without setting off an alarm. Senior TSA officials have even advised the Sikh Coalition that Sikhs should expect to undergo secondary screening, even after passing through AIT machines without incident.

---

[1] Transportation Security Administration, *Security Screening of Headcoverings*, *available at* http://www.tsa.gov/press/happenings/head_coverings.shtm.
[2] Transportation Security Administration, *Religious and Cultural Needs*, *available at* http://www.tsa.gov/travelers/airtravel/assistant/editorial_1037.shtm.
[3] Transportation Security Administration, *AIT: How it Works*, *available at* http://www.tsa.gov/ait-how-it-works.

National Office
50 Broad Street, Suite 1537
New York, NY 10004
t: 212.655.3095
f: 212.208.4611

Western Region Office
39055 Hastings Street, Suite 210
Fremont, CA 94538
t: 510.659.0900
f: 510.659.0903

Washington DC Office
PO Box 11258
Washington, DC 20008
t: 202.747.4944
f: 202.330.5574

In December 2011, the Sikh Coalition obtained an internal TSA memorandum (attached to this letter as an enclosure) through a Freedom of Information Act (FOIA) request. According to the memorandum, which was written in June 2009, TSA actively considered several auditing options to address concerns about profiling based on suspect classifications. Despite the feasibility of several auditing options, TSA never pursued an audit of its screening practices, anticipating instead that the deployment of AIT machines would mitigate concerns about profiling. According to the memorandum's author:

> In closing, the way ahead for the TSA is to determine what strategic option(s) to implement during the interim period of time it takes to deploy advance[d] passenger screening technologies. It's my opinion that advance[d] screening technologies, beyond those deployed today, will reduce or possibly eliminate perceptive profiling associated with our passenger screening process and policies.[4]

Contrary to the memorandum author's projection, the deployment of AIT machines has neither reduced nor eliminated the disparate treatment of Sikh travelers at our nation's airports.

B. Recommendations

The disparate secondary screening of Sikh travelers who pass through AIT machines without incident is suggestive of two problems: (1) limitations on the efficacy of AIT machines, and/or (2) profiling based on suspect classifications at our nation's airports by TSA screeners. In order to address these issues, the proposed rule should be modified as follows:

- TSA should explicitly clarify whether and to what extent AIT machines can detect anomalies concealed under "layers of clothing." Sikh travelers are routinely subjected to secondary screening of their religiously-mandated turbans, even after passing through AIT machines without incident. It is difficult to reconcile TSA's repeated claims that AIT machines can penetrate "layers of clothing" with the experiences of Sikh travelers at our nation's airports.

- TSA should explicitly commit itself to undertaking a comprehensive, public, and independent audit of its screening practices to determine whether TSA screeners are subjecting travelers to profiling based on suspect classifications, including race, ethnicity, religion, and national origin.

The Sikh Coalition appreciates the opportunity to comment on the TSA's proposed rule and looks forward to working with TSA to ensure that travelers are not subjected to civil rights violations, which undermine national security, at our nation's airports. Please accept our gratitude for your consideration.

Respectfully submitted,

Rajdeep Singh
Director of Law and Policy
(202) 747-4944 | rajdeep@sikhcoalition.org

Enclosure

---

[4] *Available at* http://bit.ly/130EjDI.

U.S. Department of Homeland Security

Freedom of Information Act Office
Arlington, VA 20598-6020

Transportation Security Administration

DEC - 5 2011

3600.1
FOIA Case Number: TSA09-0800

Mr. Arjun Sethi
Covington & Burling, LLP
1201 Pennsylvania Ave., NW
Washington, D.C. 20004-2401

Dear Mr. Sethi:

This is in response to your Freedom of Information Act (FOIA) request dated August 24, 2009, in which you requested "a copy of the memorandum written by Mark Lendvay assessing the need for the TSA to implement an auditing mechanism to monitor racial profiling. This memorandum would include, among other things, assessments of various audit proposals, including those presented by Professors Jack Glaser and Steven Raphael from the University of California, Berkeley and by researchers at the Vera Institute".

Your request was processed pursuant to the FOIA, 5 U.S.C. § 552.

A search was conducted within the Transportation Security Administration (TSA) and responsive documents (43 pages) were located. Seventeen pages are being released to you in their entirety. Nine-teen pages in their entirety and portions of 7 pages are being withheld pursuant to Exemptions (b)(3), (b)(4), (b)(5) and (b)(6) of the FOIA. A more detailed explanation of these exemptions is outlined below.

<u>Exemption (b)(3)</u>

This information reveals Sensitive Security Information (SSI) and is exempt from disclosure under Exemption (b)(3), which permits the withholding of records specifically exempted from disclosure by another Federal statute. Title 49 U.S.C. Section 114(r) exempts from disclosure SSI that "would be detrimental to the security of transportation" if disclosed. The TSA regulations implementing Section 114(r) are found in 49 CFR Part 1520.

Exemption (b)(4)

We have determined that portions of the responsive documents are exempt from disclosure under Exemption (b)(4) and must be withheld in order to protect the submitter's proprietary interests. Exemption (b)(4) protects trade secrets and commercial or financial information obtained from a person that is privileged or confidential. The courts have held that this subsection protects (a) confidential commercial information, the disclosure of which is likely to cause substantial harm to the competitive position of the person who submitted the information and (b) information that was voluntarily submitted to the government if it is the kind of information that the provider would not customarily make available to the public. Based on our review of documents deemed responsive to your request, and in consultation with the submitters of research proposals, we have determined the information to have been voluntarily submitted. Accordingly some information has been withheld from release on the basis that it is the type of information the submitters would not customarily release to the public.

Exemption (b)(5)

Exemption (b)(5) protects from disclosure those inter- or intra-agency documents that are normally privileged in the civil discovery context. The three most frequently invoked privileges are the deliberative process privilege, the attorney work-product privilege, and the attorney-client privilege. Of those, we have determined that some of the information in the documents you have requested is appropriately withheld under the deliberative process privilege, the general purpose of which is to "prevent injury to the quality of agency decisions." Specifically, three policy purposes consistently have been held to constitute the basis for this privilege: (1) to encourage open, frank discussions on matters of policy between subordinates and superiors; (2) to protect against premature disclosure of proposed policies before they are actually adopted; and (3) to protect against public confusion that might result from disclosure of reasons and rationales that were not in fact ultimately the grounds for an agency's actions.

Exemption (b)(6)

Exemption (b)(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, we 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

The fees incurred to process your request do not exceed the minimum threshold necessary for charge and, therefore, there is no fee associated with the processing of this request.

Administrative Appeal

In the event that you may wish to appeal this determination, an administrative appeal may be made in writing to Kimberly Walton, Special Counselor, Office of the Special Counselor, Transportation Security Administration, 601 South 12th Street, East Building, E7-121S, Arlington, VA 20598-6033. Your appeal **must be submitted within 60 days** from the date of this determination. It should contain your FOIA request number and state, to the extent possible, the reasons why you believe the initial determination should be reversed. In addition, the envelope in which the appeal is mailed in should be prominently marked "FOIA Appeal." Please note the Special Counselor's decision on your FOIA appeal will be administratively final.

If you have any questions pertaining to your request, please feel free to contact the FOIA Office at 1-866-364-2872 or locally at 571-227-2300.

Sincerely,

Yvonne L. Coates
Director, Freedom of Information Act Office
Office of the Special Counselor
Transportation Security Administration

Enclosure

Transportation
Security
Administration

Date: June 16, 2009

To: Kimberly Walton
Special Counselor [redacted] (b) (6)

From: [redacted]

Subject: Final Report on Strategic Options to Consider on Racial Profiling and Slide Presentation

In accordance with my Development Assignment Profile that required me to: 1) reach out to external stakeholders and identify issues and concerns about secondary screening and allegations of racial profiling; 2) researching what measures other organizational entities have taken in response to such allegations; and 3) developing a formal recommendation as to the measures TSA should implement to address this matter, please find attached my formal recommendations based on meetings with our stakeholders and in-depth research performed on this issue.

The attached document contains eight (8) Strategic Options in which the TSA Senior Leadership Team could deploy, to include three formal proposals on data collection Efforts. These proposals were provided by University of California, Berkeley, VERA Institute of Justice and RAND Corporation.

Included with this report is a slide presentation that provides leadership with a Summary of the report.

In closing, the way ahead for the TSA is to determine what strategic option(s) to implement during the interim period of time it takes to deploy advance passenger screening technologies. It's my opinion that advance screening technologies, beyond those deployed today, will reduce or possibly eliminate perceptive profiling associated with our passenger screening process and policies.

Attachments (2)

www.tsa.gov

1

TSA Passenger Screening Program

Strategic Options to Consider

Racial Profiling Concerns

Submitted By:

[redacted]

Senior Leadership Development Program – 3

June 16, 2009

Table of Contents

3

TSA Passenger Screening Program

Strategic Options to Consider

Racial Profiling Concerns

Office of Special Counselor

Introduction:

Since federalization the Transportation Security Administration (TSA) has implemented a number of passenger screening procedures that continue to evolve. These procedures change as the threat to aviation continues, along with the Agency balancing race neutral screening policies with national security. An example of this is in August of 2007, whereby the TSA commenced screening of bulky clothing and passenger headwear. Prior to this date the TSA permitted passage through the screening process without either additional screening or removal of headwear. This change in security posture resulted in some religious (Sikhs in particular) groups experiencing increased secondary screening. Some believe that the increased secondary screening resulted in "perceptible racial profiling" and in particular, individuals who wear turbans such as the Sikh religious faith.

In response to the concerns expressed by various coalition groups the TSA adjusted their screening procedures in October of 2007. This adjustment permitted individuals wearing religious headwear to carry out ne of three screening options that includes passing through either a Trace Portal (Puffer) or Whole Body ımaging (WBI). However, even with adjustments to the Passenger Screening Checkpoint Standard Operating Procedures (SOP), the issue of "perceptible racial profiling" continues to exist today. The attached TSA Report Card prepared by the Sikh Coalition illustrates this ongoing concern among the Sikh community (**Attachment 1**).

The purpose of this document is to present the TSA Senior Leadership Team (SLT) with possible strategic options that could be implemented to: (1) address racial profiling concerns whether perceptive or actual; and, (2) Improve internal business controls as they relate to secondary screening procedures. Each option is presented below in granularity and offers the reader background information associated with the option. Although ultimately a highbred approach is suggested, a single course of action to address this sensitive and important area specifically pertains to screening technologies and the accelerated deployment of said equipment by the Agency.

Advancements in screening technologies would permit members of the traveling public to pass through the screening process without necessarily experiencing secondary screening. However, with advance technology, privacy becomes a consideration, not to mention how the TSA can adequately balance national security with public policy as exhibited in H.R. 2027 (Aircraft Passenger Whole-Body Imaging Limitations Act of 2009). The current challenge faced by the TSA is how to function during this interim period of time until the perfect screening technology is deployed for public use.

TSA Passenger Screening Program

Strategic Options to Consider

Racial Profiling Concerns

Office of Special Counselor

(b) (5) [redacted]

Attachments 2, 2A and 2B contain three proposed Research Prospectuses on data collection efforts. The first prospectus was submitted by the Goldman School of Public Policy, University of California - Berkeley who suggests reviewing checkpoint video as a methodology. The second prospectus was offered by the VERA Institute of Justice whose research methodology is to perform direct observational audits of the screening checkpoints, followed by reviewing video where available. (b) (4) [redacted] Although all research methodologies offer their own unique and independent benefits, it would appear that the VERA and RAND approaches are better aligned with TSA's expected outcomes.

(b) (5) [redacted]

7

WIF (b)(3), (b)(5)

TSA Passenger Screening Program

Strategic Options to Consider

Racial Profiling Concerns

performed in accordance with Section 222 of the Homeland Security Act in order to alleviate the concerns associated with this screening technology. Although privacy concerns surrounding the WBI continue to remain today, the Agency is on official record of proactively performing the PIA.

Unlike the above programs, the Passenger Screening Checkpoint SOP has not undergone a CLIA. It would appear that based on a review of H.R. 1 (Implementing Recommendations of the 9/11 Commission Act of 2007), Title VIII, Section 1062, the TSA could provide (optional Agency action) the SOP to the DHS for review since these security procedures pertain to national security. Performing a CLIA on the SOP would, in the opinion of the author, reduce some of the debate associated with secondary screening and ensure that the Agency is meeting the intent of the statute; albeit, optional. Although the debate about discriminatory practices and racial profiling would continue, a CLIA endorsement would further demonstrate an open and transparent government, something that the current Administration requires.

trategic Option Recommendation #2 to SLT:

Perform a CLIA on the Passenger Screening Checkpoint SOP then publically announce the effort and results.

[redacted]

During the May 8th meeting with the Sikh Organizations, Acting TSA Administrator Gale Rossides, was specifically asked whether or not a turban had ever been utilized to conceal an item [redacted] Such data could be delivered to Congress during

8

WIF (b)(3), (b)(5)

TSA Passenger Screening Program
Strategic Options to Consider
Racial Profiling Concerns

Office of Special Counsel

classified briefings and support the "political debate" on national security versus public policy as they relate to privacy considerations.

Strategic Option Recommendation #3 to SLT:

[redacted] (b)(3) 49 USC 114(r)

Strategic Option 4 – Operational Screening Audits:

A number of the organizations (stakeholders) commented that many airports do not apply the Passenger Screening Checkpoint SOP in a consistent manner. Rather, screening measures appear to be inconsistent when comparing airports. In fact, as illustrated in **Attachment 1**, some airports may not require secondary screening for an individual wearing a bulky item, whereas other airports reportedly perform 100% secondary screening of the same item. Discretionary application of the SOP on bulky clothing is difficult to measure, but not necessarily impossible for the TSA to consider. Another factor to consider here when reviewing network consistency is whether or not an airport has advanced screening technologies (i.e. Trace Portal or WBI) deployed, as is the case with SFO.

Since federalization of the screening process the TSA has performed a number of operational tests, some of which consist of: IED Checkpoint Drills, ADASP and Red Team testing. But, the Agency does not conduct performance audits in order to gage the performance aptitude of the screening process, or how our TSOs are directly carrying out the SOP. In particular, the TSA is not reviewing bulky clothing screening procedures and the execution of independent discretion by the Officer ranks. This is further illustrated by the recently developed and released Training Job Aid that focuses on bulky clothing.

Although the PASS Program has some operational criteria contained, it's noted that this primarily focuses on screening with a Hand Held Metal Detector (HHMD), Full Body Pat Down (FBPD), attendance, Online Learning Center (OLC) and collateral duties. Performance audits of the bulky clothing requirements could be performed at each airport by Expert Screening Training Instructors (ESTI) or Screening Training Instructors (STI), then recorded in a centralized database such as PMIS or PARIS. These ESTIs or STIs could be deployed to other airports in order to provide an objective review of the screening process. This approach is similar to how the Agency is currently managing the Passenger Screening Evaluations (PSEs) this fiscal year.

9

WIF (b)(3), (b)(5)

developed by the San Francisco Bay Area Airports (**Attachment 3**) in response to concerns of inconsistencies among SFO, OAK, SJC and SMF. Although not implemented at said airports as of yet, the observations items on the checklist are intended to be completed by a Transportation Security Manager (TSM), Supervisor Transportation Security Officer (STSO), ESTI or STI.

This option is similar to the previous option above in that an operational assessment of the screening process is performed. However, there is a specific focus on non-form fitting headwear, and not just religious headwear. Again, this information could be nationally entered into a centralized data system that would enable the Agency to review this screening procedure across the network.

Strategic Option Recommendation #5 to SLT:

Implement a Practical Skills Observation/Demonstration Checklist for Non-Form Fitting Headwear Screening and report findings throughout the network.

Strategic Option 6 – Expansion of Close Circuit Television at Passenger Screening Checkpoints:

A review of the (b)(3) 49 USC 114(r) [redacted] reveals that CCTV technology is lacking. Conversely, airports such as (b)(3) 49 USC 114(r) [redacted] have elaborate camera systems. The former airports have minimal camera coverage that results in challenges to local FSD staffs and the Agency as a whole as it relates to allegations of racial profiling.

Allegations of racial profiling and discriminatory screening practices, whether actual or perceptive, are not being recorded at airports lacking camera coverage. This results in the Agency having a difficult time of sorting out whether an allegation actual occurred or not. An ancillary consideration here also pertains to allegations of theft, damage, on-the-job injures and security breaches. Thus, a robust camera system would assist the Agency in investigating such allegations, mitigating security breaches and possibly reducing the number of passenger claims paid out on.

Therefore, it's suggested that the Agency expand its' efforts in this area and consider funding instruments such as Other Transaction Agreements (OTAs) and/or Memorandum of Agreements (MOA).

Strategic Option Recommendation #6 to SLT:

Accelerate and improve CCTV systems at airports that lack such technology today.

TSA Passenger Screening Program

Strategic Options to Consider

Racial Profiling Concerns

[redacted]

Conclusion:

he Officer ranks of the TSA are all hardworking men and woman who carryout their official duties and responsibilities both proudly and professionally. Said workforce is administered continued training that not only pertains to screening procedures, but also cultural awareness. This workforce is resilient and adoptable to the dynamics associated with aviation security and the continued threat we collectively face.

Historical information indicates that the issue presented here is not one of profiling or discriminatory practices by the TSA workforce. Rather, the issue directly correlates to our current screening policies as a result of a lack of advance screening technologies, combined with ongoing threat streams. These policies are required to overcome the security vulnerabilities in order to ensure a safe and secure air transportation system.

The challenge ahead for the TSA is what strategic option or options to implement during the interim period of time is takes to deploy advance passenger screening technologies.

Attachment 1

14

The Sikh Coalition
the voice of a people

The TSA Report Card

A Quarterly Review of Security Screenings of Sikh Travelers in U.S. Airports

Q1 2009

RoundUp: Oakland Airport Problems Persist

As we begin 2009, 100% secondary screening rates of Sikh travelers continue to be an issue at California's airports.

Of all the reports we have received, no Sikh turbaned traveler reported being spared a secondary screening at Oakland Airport. This is a continuation of the same problem we identified in our last quarterly report card.

We first brought this issue to the TSA's attention in October 2008. In response, a few of California's TSA administrators met with Sikh groups in early February 2009. Though TSA officials from Washington D.C. at that meeting reiterated that the policy is not intended to mandate turban screenings, no action has yet been taken to remedy the screening problem at Oakland. A follow up meeting to discuss the policy has been planned for the first week of May in Washington D.C.

In addition to Oakland Airport, frequent flyers through Sacramento Airport also noted 100% screening rates at that location. Both airports are among the top screening airports according to the Sikh Coalition's data.

Similar reports have also been received from Seattle, while officials in Dallas and Chicago airports told Sikhs that turban searches are mandatory.

Screening Sikhs by the Numbers:

	Q1 2009	Q1 2008
Sikhs sent for additional screening who reported feeling singled out	90%	64%
Sikhs who were not informed of their option to conduct a self-pat-down	23%	25%
Sikhs who were told that turban screening is a mandatory security measure	13%	23%
Screening complaints stemming from California airports	48%	49%
Sikhs who reported being subject to additional screenings at U.S. airports*	84%	71%

*Note that this number is based on self-reporting by Sikh travelers. As a result, since more people are likely to complain about unpleasant experiences at security, this percentage is likely weighted towards bad experiences.

Specific Incidents

1. A traveler leaving from **Oakland Airport** was subjected to a full body pat down after clearing the metal detector. The TSO then mentioned that the passenger "would be a good one" for another TSA officer to get trained on.
2. A Sikh passenger traveling through **Buffalo Airport** was screened by four separate TSA officers before being allowed to proceed. Although one had only wanted to check his loose sweatshirt, another instructed the first officer to screen the full body. Then, a third and fourth screener asked the passenger numerous questions about his trip, where he lived and his destination.
3. A passenger at **Phoenix Airport** was instructed to go through a full body scan machine in lieu of a TSO pat down .
4. A passenger traveling through **Dallas Airport** had cleared security but was called back by a separate TSO whose supervisor claimed that all turbans must be screened. "I can even pull you out of the boarding area, if I want to," the supervisor said.

Recommendations

1. Audit TSA screeners in the exercise of their discretion, to ensure that individual TSA employees are not engaging in racial profiling at U.S. airports.
2. Promptly address claims of mandatory or 100% secondary screenings for Sikh passengers at the airports where they arise.
3. Guide TSA screeners to inform Sikh passengers of all three of their options as soon as a passenger is identified for additional screening of their turban.
4. Involve Sikh civil rights groups in the development of cultural sensitivity training materials for TSA screeners.
5. Post information about the screening procedures in Punjabi.

Attachments 2, 2A and 2B

16

Research Prospectus:
Racial and Ethnic Profiling in Airport Security Screening with a Focus on Clothing and Headdress Searches

Associate Professor Jack Glaser and Professor Steven Raphael
Goldman School of Public Policy
University of California, Berkeley

At the request of
The Sikh Coalition

Draft: December 15, 2008

This investigation seeks to employ rigorous scientific and policy-analytic methods to investigate whether (and to what extent) or not racial and ethnic profiling has occurred in Transportation Security Administration screenings at American airports, resulting in unfair treatment of certain racial, ethnic, and religious groups.[1]

The question:

Are Turbaned Sikhs and others targeted by Transportation Security Officers (TSO's) for extra scrutiny and secondary searches at airport security screening checkpoints at a rate that is disproportionate to that justified by their behavior?

The background:

The Transportation Security Administration is tasked with, among other things, preventing terrorists from carrying out attacks involving airliners. To that end, their TSO's screen every passenger. Some passengers are given secondary screening that extends beyond passing through a metal detector and having items x-rayed. The secondary screening can involve additional electronic "wanding," physical pat-downs, screening by an electronic trace portal machine (puffer), clothing removal, additional questioning, and even strip searching.

The problem:

Based on numerous firsthand accounts and complaints, The Sikh Coalition believes that Sikhs who wear turbans in accordance with their religious mandate, are subjected to secondary screening at a dramatically disproportionate rate. At one point, it was explicit TSA policy to subject any passenger wearing a turban to secondary screening. This had a disparate effect on Sikhs. The TSA has reversed that policy. Nevertheless, reports to the Sikh Coalition indicate that Sikhs are still asked to have their turbans inspected more often than others wearing clothing

[1] We will use the term "racial and ethnic profiling" in this document to capture profiling based on religious group membership as well, particularly because it is likely that screeners and other observers often do not accurately recognize the actual religion of targeted minorities. The term "ethnic" will be used broadly to capture some non-racial physical, cultural, and religious categorizations.

17

that could just as easily conceal a weapon (e.g., Hasidic Jews, people wearing cowboy hats, people wearing baggy clothes).

If Sikhs are being targeted disproportionately, it implicates a civil rights violation. Furthermore, excessive targeting of Sikhs may even be at odds with security objectives because Sikhs would be singled out based solely on their appearance – a tactic that the TSA has agreed is a distraction in terms of promoting security. Targeting Sikhs based on misconceptions about religion and ethnicity may undermine security by drawing TSOs' attention and resources away from more likely threats and more direct and credible indicators of threat.

The research:

The study would involve objective reviews of TSO screening videos from a diverse sample of airports. Multiple, carefully trained raters would use standardized criteria to record security screenings, including traveler gender, ostensible race/ethnicity/religion, approximate age, size, dress, and manner. Screening procedures employed for each traveler would also be recorded. Raters would be blind to the purpose of the study, and two raters would be used, working independently of each other, according to identical rating criteria and standard social scientific procedures. Airport and personnel information would be kept strictly confidential. This sort of data coding method is the most appropriate approach for codifying and analyzing large samples of naturalistic human behavior (as opposed to structured, questionnaire measures or experiments)[1].

The purpose of the study would be to identify if, where, when, and under what circumstances disparate screening treatments have been imposed on different groups. The study does not aim to make value judgments or second-guess screening procedures. It will simply quantify the screening behaviors, and their varying rates, with regard to identifiable physical attributes of travelers. In this manner, we can identify if there is empirical support for the complaints of the Sikh community, specifically, and other groups as well.

The participants:

Jack Glaser is an Associate Professor at the Goldman School of Public Policy at the University of California, Berkeley. Professor Glaser has a PhD in Psychology from Yale University. He teaches graduate level courses on statistical analysis, policy analysis, and the social psychology of prejudice and discrimination. His research focuses primarily on the application of social psychological approaches to criminal justice, including work on racial profiling, hate crime, capital punishment, and unintended forms of racial bias in policing. He is preparing a book on racial profiling for Oxford University Press.

Steven Raphael is a Professor at the Goldman School of Public Policy at the University of California, Berkeley. Professor Raphael received his Ph.D. in economics from UC Berkeley in 1996. His primary fields of concentration are labor and urban economics. He has authored several research projects investigating the relationship between racial segregation in housing markets and the relative employment prospects of African-Americans. Raphael has also written theoretical and empirical papers on the economics of discrimination, the role of access to transportation in determining employment outcomes, the relationship between unemployment

[1] Bakeman, R. (2000). Behavioral observation and coding. In H.T. Reis & C.M. Judd (Eds.), *Handbook of Research Methods in Social and Personality Psychology* (pp. 138-159). New York: Cambridge University Press.

18

and crime, the role of peer influences on youth behavior, the effect of trade unions on wage structures, and homelessness.

The Sikh Coalition is a national, community based civil rights organization that actively promotes civil and human rights for all people. The Sikh Coalition was formed in the aftermath of the terrorist attacks of September 11, 2001, to help address bias and discrimination against the Sikh American community. **Neha Singh**, the Western Region Director of the Sikh Coalition, is serving as liaison to the research project.

Inquiries about the project should be addressed to:

Jack Glaser
Associate Professor
Goldman School of Public Policy
University of California, Berkeley
2607 Hearst Avenue
Berkeley, CA 94720-7320
510-642-3047
jackglaser@berkeley.edu

A

Washington DC Office
1330 Connecticut Ave NW, Suite B
Washington, DC 20036

Tel: (202) 347-6776
Fax: (202) 347-6047
www.vera.org

VERA INSTITUTE OF JUSTICE

To: [redacted] Transportation Security Administration

From: [redacted] The Vera Institute of Justice

Date: June 3, 2009

Re: Preliminary TSA Research Proposal

The Vera Institute of Justice is pleased to outline a preliminary research proposal to examine the application of secondary screening policies at Transportation Security Administration (TSA) airport checkpoints. We understand that TSA has been working internally – as well as externally with concerned citizens and organizations – to ensure that secondary screening policies do not result in discrimination. Based on our conversations, it is our understanding that the TSA has been tasked with making a recommendation on how to determine (1) if screeners in the field uniformly adhere to TSA's national secondary screening policies and practices, and (2) if the application of those policies has a disparate impact on who is selected for secondary screening, particularly with regard to census characteristics such as perceived race, ethnicity, national origin, and religion. This memo outlines Vera's proposed research methodology to examine the issues you have identified. We view this proposal as a work in progress. The methodology description is preliminary and is intended to offer a sample of what is possible. Details of this methodology would be developed and adapted based on a more in-depth understanding of TSA procedures, restrictions, and the outcomes that TSA wants to realize from the research. The memo also offers examples of relevant work from Vera's nearly fifty-year history delivering robust research and program development and services as a trusted partner to leaders in government and civil society.

Research Methodology

Investigating whether disparate impact exists in the screening of several million passengers per day across widely diverse settings is a very complex and multi-dimensional task. It is not simply a question of 'who' is selected for secondary screening but rather, 'who is selected among those eligible to be screened secondarily' and 'whether policies, procedures, or practices are affecting the likelihood of secondary screening in any particular subset of those eligible to be screened.' Vera first must conduct a number of preliminary assessments before determining optimal sampling strategies, measurements, and analytic strategies. During the initial stage of the project, Vera staff will work with expert TSA staff to gather information critical to the development of an appropriate and effective research design – including problem definition, sampling strategy, site selection, data collection procedures, and measurement.

Problem Definition and Overall Approach.

20

Vera's primary research goals for this project are to examine: (1) whether TSA officers are adhering to Agency secondary screening policies; (2) whether disparities exist within TSA's secondary screening process; and (3) if disparities exist, potential underlying causes and subsets of travelers -- if any -- most affected by these disparities. These goals will be refined and adjusted based on further discussion of TSA's concerns and needs.

Vera staff also will team with TSA to determine what degree and level of detail is of interest. Discussions will include whether TSA is interested in answers to the above questions on a national, regional, or local level (or by size of airport), if there are particular regions or arrays of primary concern due to the number of complaints received, and if specific populations are of concern. Vera then will work with TSA to customize the research plan and incorporate these issues. Once the extent of TSA's needs and interests has been identified, Vera will develop an appropriate sampling strategy and method of data collection and analysis.

Sampling Strategy and Site Selection.

Vera researchers will work with TSA staff to develop a categorized list of potential sites, based on criteria determined during problem definition (*e.g.*, numbers of TSA checkpoints & personnel, volume of passengers, geographic region, types of outgoing flights served (commuter, domestic, international), composition of general population, *etc.*). Parallel to this procedure, Vera staff, in consultation with a survey sampling statistician, will determine the appropriate sample size needed to answer the research questions at the desired level of confidence.

Measurement and Data Collection.

To assess whether there is disparate impact, Vera will collect data on those eligible for secondary screening as well as those selected for screening. To accomplish this, Vera must answer the questions "What categories of persons qualify for secondary screening?" and "Under what conditions are people pulled for a secondary screen?" As a first step in this process, Vera staff will conduct interviews and focus groups with staff members as well as review relevant documents to develop a comprehensive understanding of TSA's policies and procedures for secondary screening, including gathering information about whether discretion is permitted, under what circumstances, and what review procedures or other internal controls are currently in place. (At the option of TSA, Vera might also develop a separate, internal project to assess how closely TSA officers are adhering to TSA's national policies; this option will be discussed with TSA at a later date.)

Once the overall information is collected, Vera can proceed to ascertain what decisions are made; whether disparate impact occurs, to whom, and under what conditions; and the degree to which discretion versus policy accounts for that disparity. To assess this, Vera researchers will first measure secondary screening outcomes based on strict adherence to policy in the aggregate to determine if disparate outcomes result. This measure will provide our baseline, which may or may not uncover disparate outcomes. If applicable under TSA procedures, we could then measure what happens if discretion is permitted, specifically seeking to answer the question: "Does discretion result in disparate outcomes, and if so, are they greater in magnitude than the baselines?"

Vera anticipates using a combination of quantitative and qualitative methods to measure whether groups are being affected disparately. For example, one possible method of assessment would be to use independent raters – either trained researchers with necessary security clearances and/or TSA personnel – to identify who is eligible for secondary screening during a particular time period via onsite observations – our preferred methodology, or through recorded footage from the checkpoint, combined with any other information available to the TSA screener prior to the secondary screening. The "eligible" group may then be compared to the actual group selected for screening to assess whether there is a higher risk of screening for any subgroup. Another potential method for examining disparities is to engage confederates (*e.g.*, "confederate" or "tester" passengers hired by Vera with particular characteristics of interest) to subject themselves to screening and track who is selected for a secondary screen and for what reason. Specific characteristics of these confederates or testers can be deliberately manipulated to see whether, individually or in combination, they are related to screener decisions and to decisions resulting in disparate impacts.

The research project would also provide TSA with an additional tool to use in quality control and management. Vera's work would result in TSA staff being trained to do on-going assessments of TSA screenings and the knowledge of how to effectively use results of the screening assessments to improve the quality of services.

Vera's Background

The Vera Institute of Justice is an independent nonprofit organization that combines expertise in research, evidence-informed programmatic design, demonstration projects, and technical assistance to help leaders in government and civil society improve the systems people rely on for justice and safety. Vera has an extensive history of conducting research, including federally funded research projects. Vera's research department conducts three types of research: exploratory research on issues of interest to Vera or to a government partner, evaluations of innovative programs including Vera's own demonstration projects, and special projects providing research advice and assistance to other nonprofit organizations or government agencies. The driving force behind these research models is that the findings be of use to our government partners and that they be in a form that can be utilized to develop more effective services. Launched in 1961, Vera has developed substantial staff capital and infrastructural capability over its nearly fifty-year history to deliver robust research and programmatic services in a wide range of government and civic settings.

In addition to our established research capacity, Vera has built a solid reputation for providing technical assistance to a variety of governmental entities. Vera offers a range of services to help government partners improve their systems. We provide decision makers at the local, state, and national level with expertise and nonpartisan advice to help them craft practical solutions that are viable, effective, sustainable, and tailored to support their specific goals. In these efforts we combine subject matter expertise, research and analytical capacity, and knowledge of government systems with skilled facilitation and process consultation to help our partners achieve optimal outcomes tailored to meet their information and programmatic goals.

Highlights of Vera's work include:

- ***Appearance Assistance Program***. In 1996, the Immigration and Naturalization Service asked Vera to establish a supervised release project for people in removal proceedings in New York City. The INS goal was to assess supervision and evaluate its effect on rates of appearance in court and compliance with court ruling compared to other alternatives to detention already in use by the agency, such as bond, parole, and release on recognizance. The Appearance Assistance Program (AAP) – a three-year test of community supervision for people in immigration removal proceedings – began operating in February 1997 and concluded in March 2000. All Vera employees working on AAP obtained the appropriate security clearances needed to perform the work. The AAP demonstrated that it is not necessary for the INS to detain all noncitizens in removal proceedings to ensure extremely high rates of appearance at immigration court hearings. Ninety-one percent of participants in the intensive program attended all required hearings, in comparison to 71% of noncitizens released on bond or parole. Among Vera's other findings: supervision is more cost effective than detention, and AAP supervision almost doubled the rate of compliance with final orders.
- ***Prosecution and Racial Justice***. Since 2006, Vera's Prosecution and Racial Justice Program (PRJ) has partnered with district attorneys in Milwaukee County, Wisconsin; Mecklenburg County, North Carolina; and San Diego County, California, to pilot an internal assessment and management procedure that is helping supervisors to (a) identify evidence of possible racial or ethnic bias in their staff's aggregate decision-making and (b) respond appropriately when such biases are found. In the course of this work, PRJ has analyzed administrative data from district attorney's offices and conducted focus groups and surveys with prosecutors. Vera also worked effectively to design and help implement constructive solutions when problems were identified. For example, in 2006, Vera found that junior prosecutors in Milwaukee, WI, were filing drug paraphernalia charges against 59 percent of whites compared to 73 percent of non-whites. Vera facilitated discussions about this finding among the staff, which resulted in district attorney requiring prosecutors to consult their supervisor prior to issuing drug paraphernalia charges. Within a matter of months, the disparity disappeared. More recently, Vera developed a monitoring tool to provide district attorneys with an early warning system that flags potential areas of racial disparity in initial case screening. Vera continues to work closely with these district attorneys in identifying and eliminating racial bias, thereby enhancing the integrity of judicial outcomes and building public confidence in the criminal justice process.
- ***Law Enforcement & Arab American Community Relations after 9/11***. After the bombings on September 11, 2001, Vera conducted a research study funded by the National Institute of Justice examining the effects nationally of the events of September 11th on law enforcement agencies and communities with high concentrations of Arab-American residents. To explore these issues, Vera researchers conducted telephone surveys with community leaders, local law enforcement

officials, and field office agents from the Federal Bureau of Investigation (FBI) in 16 representative sites around the country. Four sites were then selected for in-depth study involving additional interviews, facilitated focus groups, and researcher' observation of police-community relations. Vera produced a report from study findings that provided in-depth insight into relations between Arab Americans and local and federal law enforcement as well as challenges each of these stakeholders faces in responding to pressures that are increasingly global in nature. The Vera report also identified examples of best practice partnerships and innovations that have successfully bridged gaps identified in the study. Recommendations and opportunities for restoring trust and creating alliances to reduce crime and address terrorism and other public safety concerns also are included.

- ***Translating Justice***. For the past six years, Vera also has partnered with the U.S. Department of Justice's Office of Community Oriented Policing Services (COPS Office) to assist law enforcement agencies nationally in improving their relationships with immigrant communities through developing multi-jurisdictional recommendations and action plans. In 2005 with funding from the COPS Office, Vera partnered with the Anaheim Police Department, Clark County (OH) Sheriff's Office, and the Las Vegas Metropolitan Police Department to develop language access action plans and policies specifically tailored for each jurisdiction. Each language access action plan was based on in-depth findings from interviews, focus groups, and police-community strategic planning meetings. In addition, Vera created a document offering practical steps that law enforcement agencies nationwide can take to overcome language barriers for immigrants, including gathering data to identify immigrant community needs, developing a language access policy, and cultivating existing bilingual personnel. Currently, Vera and the COPS Office are concluding a project highlighting promising practices nationally for overcoming language barriers in policing; this project involved Vera collecting and analyzing assessments of nearly 200 agencies' practices. The COPS office has also partnered with Vera to assemble a group of police and community leaders for a focus group discussing how law enforcement and new immigrants can cultivate, maintain, and restore partnerships aimed at keeping communities safe.

- ***Legal Orientation Program***. The Legal Orientation Program (LOP) was created to inform immigrant detainees about their rights, immigration court, and the detention process. The LOP is a partnership between Vera, the Annie E. Casey Foundation, the U.S. Department of Health and Human Services, the U.S. Department of Justice's Executive Office for Immigration Review (EOIR) and their Office of Community Oriented Policing Services (COPS). On behalf of the EOIR, program staff work with nonprofit legal service agencies to provide the program at 25 detention facilities across the country. Research indicates that program participants move through immigration court more quickly and are therefore likely spend less time in detention than people who do not have access to legal help.

- ***Accessing Safety Initiative (ASI)***. The Accessing Safety Initiative helps its partner jurisdictions – states and cities – enhance the capacity of their social services and criminal justice systems to assist women with disabilities and deaf women who have experienced domestic violence, sexual assault, and stalking. ASI partnered with the U.S. Department of Justice's Office on Violence

Against Women in 2006 to provide intensive consulting and training to federally funded initiatives that are working to improve services for these survivors. Its goal is to increase victim agencies' knowledge, skills, and resources for offering accessible and welcoming services to people with disabilities and, at the same time, help disability organizations offer safe and responsive services to survivors of domestic or sexual violence.

- ***Work with the National Prison Rape Elimination Commission.*** Vera's Washington DC Office worked over a three-year period with the congressionally mandated National Prison Rape Elimination Commission (NPREC) to develop standards to detect, prevent, and respond to sexual abuse and rape in jails, prisons, lock-ups, juvenile residential detention facilities, immigration detention facilities, and community-corrections settings and to produce a final report for the Commission. The standards, submitted for public comment in 2008, incorporate public as well as intensive key stakeholder feedback. They will be released June 24th 2009 along with the final report and recommendations and presented to the U.S. Attorney General, President, and Congress for further action

Attachment 3

24

Attachment 3

35

Transportation Security Administration

Practical Skills Observation/Demonstration Checklist
Non-Form Fitting Headwear Screening

Performance Accountability and Standards Audit for Check Point Screening

PRINCIPAL PURPOSE(S): This information will be used as part of the Contractors performance review

Non-Form Fitting Headwear		
Employee's Name	**Last 4**	**Date/Time**
Supervisor's Name	**Auditor's Name**	**Location**

(b)(3) 49 USC 114(r)

[redacted]

Transportation Security Administration

Practical Skills Observation/Demonstration Checklist
Non-Form Fitting Headwear Screening

Performance Accountability and Standards Audit for Check Point Screening:

PRINCIPAL PURPOSE(S): This information will be used as part of the Contractors performance review

Comments:

TSA Strategic Options to Consider
Secondary Screening – Bulky Clothing & Headwear
Community Perceptions of Racial or Religious Profiling

June 11, 2009

JA 000586

(b) (6)

Senior Leadership Development Program - 3

Office of the Special Counselor (OSC)

Transportation Security Administration (TSA)

Transportation Security Administration

38

Project Overview

Since August 2007 the TSA has collaboratively worked with the Sikh organizations to ensure screening options appropriately balance security needs with the passenger's civil rights and civil liberties, including freedom of religion. This effort has resulted in screening alternatives for passengers who cannot remove their headwear for secular of religious reasons. 2 years later, concerns still remain among this group. These concerns pertain to:

- *Inconsistent screening procedures - verbal announcements of the screening options delivered by Transportation Security Officers*
- *Inconsistent screening advisements – inadequate or poor communication to the passenger about the screening alternatives*
- *Some airports perform 100% secondary screening of all religious headwear*
- *Decommissioning of Trace Portals (Puffers) and proposed Congressional limitations of Whole Body Imaging (WBI) technology – Primary Position*
- *Recent changes to the Primary Position WBI SOP (Not Shared Publicly)*
- *TSA's lack of data collection efforts as it relates to secondary screening and passenger demographics*
- *U.S. is the only country that requires additional headwear screening requirements*

JA 000587

WIF (b)(3), (b)(5)

Proposed Strategic Options for TSA

- Data collection efforts on secondary screening
- Civil Liberties Impact Assessment
- [redacted] (b)(3) 49 USC 114(r)
- Operational Screening Audits
- Practical Skills Observations/Demonstration Checklist
- Expansion of CCTV coverage at passenger checkpoints
- Rapid deployment of "hush" radio equipment
- Hybrid option suggested as interim Agency response
- Advance screening technology is the ultimate solution

JA 000588

HUMAN
RIGHTS
CAMPAIGN®

U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, DC 20590-0001

June 24, 2013

Re: Docket No. TSA-2013-0004, Passenger Screening Using Advanced Imaging Technology

To Whom it May Concern:

On behalf of the Human Rights Campaign's more than one million members and supporters nationwide, I write in response to the above notice of proposed rulemaking regarding passenger screening and the use of advanced imaging technology published March 26, 2013. Although HRC recognizes the necessity for passenger screening, we are deeply concerned about the need to preserve the privacy and dignity of travelers, especially those who are at an increased risk of harm as a result of unnecessarily intrusive searches.

We appreciate the steps TSA has made to address concerns from the LGBT community; however, these concerns cannot fully be resolved within the agency's current approach to screening. This NPRM is especially problematic for vulnerable traveler populations including transgender people. The cost-benefit analysis in the NPRM fails to adequately address passenger privacy interests that will likely be impacted by the proposed regulatory approach. The NPRM also fails to propose any additions to passenger protection policy and does not codify even the minimal passenger protections in current agency practice. We urge the agency to conduct a new cost-benefit analysis that fully considers the ways in which passenger privacy is impacted by the current screening approach. We further urge TSA to adopt proposed regulatory alternative #3 (walk-through metal detectors supplemented with explosive trace detection) or, alternatively, to consider additional regulatory alternatives to reduce reliance on body scanners and pat-downs. Finally, to the extent that any final rule incorporates *any* use of body scanners and/or pat-downs, we strongly urge the formal adoption of protections for passengers that are already part of TSA practice as provided by guidance.

Transgender Travelers Are Disparately Affected by TSA's Invasive Screening Approach

An estimated nearly 700,000 adults in the United States, or 0.3% of the adult U.S. population, are transgender.[1] While estimates of the population of transgender children and adolescents are lacking, this population is also significant. In a national survey conducted in 2008-09, more than one in five transgender adults reported having been harassed or disrespected at the airport.[2] Since the implementation of the current regime of routine scanning and pat-downs, LGBT organizations have continued to be contacted with stories of harassment, rudeness, being singled out for additional screening, and other potentially discriminatory treatment of transgender children and adults and their loved ones. In addition, LGBT organizations continues to hear from many travelers that they are afraid of going to the airport, uncertain of how they will be impacted by current screening techniques or treated by Transportation Security Officers (TSOs), and in some cases are unwilling to fly as a result.

While we recognize and appreciate the steps that TSA has taken to improve screening procedures, including staff training and traveler education, transgender people will always be disparately impacted by any system based on routine scrutiny of the contours of passengers' bodies under their clothes, whether by body scanners, pat-downs, or the current combination of both. Transgender people's common use of sensitive prosthetics, high rates of past physical and sexual trauma, and pervasive experiences of harassment and discrimination, make the routine use of even modified scanners, when paired with intensive pat-downs as the only alternative option or form of resolution, a very serious imposition on individual privacy, comfort, and well-being.

Cost-Benefit Analysis Fails to Adequately Address Passenger Privacy Interests

The ruling of the Court of Appeals directing the agency to undertake this rulemaking was premised on a simple conclusion: "Despite the precautions taken by TSA, it is clear that by producing an image of the unclothed passenger, an AIT [advanced imaging technology] scanner

---

[1] G. Gates, *How Many People Are Lesbian, Gay, Bisexual and Transgender?,* WILLIAMS INST. ON SEXUAL ORIENTATION LAW, UCLA (Apr. 2011), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Gates-How-Many-People-LGBT-Apr-2011.pdf.

[2] J.M. GRANT, L.A. MOTTET, J. TANIS, J. HARRISON, J.L HERMAN, M. KEISLING, INJUSTICE AT EVERY TURN: A REPORT OF THE NATIONAL TRANSGENDER DISCRIMINATION SURVEY, 130 (2011).

intrudes upon his or her personal privacy in a way a magnetometer does not."[3] Yet the NPRM and accompanying Initial Regulatory Impact Analysis fail to acknowledge any impact on the privacy of the traveling public. Rather, the IRIA provides that the privacy protections noted by the Court of Appeals, together with the Congressional mandate for automated target recognition (ATR) software, have "adequately addressed privacy concerns."[4]

HRC recognizes that these steps are important; however they are not reflected in the NPRM as published. Nor do these measures eliminate all privacy impacts on the public. Even with most of these measures in place, the ruling of the Court of Appeals was premised on a real privacy impact from body scanners. While the ATR mandate is a positive step, it also does not eliminate all privacy impacts. The agency admits this impact on privacy stating in its IRIA that it "anticipates future advancements to AIT in … privacy protection" and by stating that its proposed regulatory approach has the "Potential for negative public perception on… privacy concerns"[5] Indeed, as the Congressional Research Service has noted, respondents to a 2010 survey identified privacy more than twice as often as delay as a primary concern with AIT.[6]

The use of body scanners as a primary screening method is inseparable from the use of highly intrusive physical pat-downs. These screening techniques are inextricable because (1) TSA relies on the alternative option of pat-downs to mitigate the privacy impact of the scanners themselves, and (2) TSA relies on the use of pat-downs to resolve many, if not most, anomalies identified by ATR. While TSA regularly cites the high rate at which passengers opt for scanning over pat-downs, this rate demonstrates not that passengers view scanners as non-intrusive, but rather that most view the alternative of a pat-down as *even more intrusive*.[7] Accordingly, pat-downs are an essential part of the operation of body scanners, and the privacy impacts of the use of pat-downs in conjunction with body scanners must be assessed in this rulemaking. Additionally, ATR does not eliminate the privacy impact of body scanners themselves. Even with this software, scanners generate and analyze data representing the contours of passengers' bodies underneath their clothing, and use this data to highlight areas of passengers' bodies that may then be subject to a pat-down.

For these reasons, an adequate regulatory impact analysis would not only identify measures the agency has taken to mitigate privacy concerns, but would also identify remaining privacy impacts on passengers, estimate the total privacy impact, and weigh this impact alongside the other costs and benefits of the proposed regulatory action. Other agencies routinely include

[3] EPIC v. DHS, 653 F.3d 1, 6 (D.C. Cir. 2011).
[4] IRIA at 101.
[5] IRIA at 110, 119.
[6] U.S. Congressional Research Service. Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening (7-5700; September 12, 2012), by Bart Elias.
[7] See DHS v. EPIC, 653 F.3d 1, 10 (D.C. Cir. 2011) (pat-down alternative "allows [the traveler] to decide which of the two options … is *least* invasive" (emphasis added)).

privacy impacts on the public in their analysis of regulatory costs. It is unacceptable for TSA not to do so in this case, which will impact millions of members of the traveling public.

Regulatory Alternative #3 and Reduced Reliance on Pat-Downs and Scanners will Best Ensure the Safety and Dignity of Vulnerable Travelers

We strongly urge the Department to adopt proposed regulatory alternative #3 as described in the NPRM (walk-through metal detectors supplemented with explosive trace detection), or alternatively, to consider additional regulatory alternatives that reduce reliance on body scanners as a primary method of checkpoint screening. We note that while the NPRM describes the proposed regulatory alternatives in hardline terms, TSA's historical practice has been to use a mix of screening methods providing a layered approach and a certain amount of variability. Accordingly, we expect that TSA's regulatory alternatives include the use of both body scanners and pat-downs on a more limited basis to supplement the use of metal detectors and explosive trace detection. However, the NPRM fails to address the possibility of redeploying already-purchased scanner devices on a more limited basis, such as for random or secondary screening.

The Final Rule Must Codify Existing Passenger Protections

Despite the significant privacy implications noted by the Court of Appeals, the proposed rule does not incorporate *any* limitation on the use of body scanners or pat-downs. It fails to incorporate even the minimal requirements already incorporated in TSA policy and practice or mandated by Congress. If TSA maintains use of body scanners, the final rule must incorporate these existing protections. Because public trust is fundamental to the viability of airport screening, these protections must be codified in regulation as opposed to less formal operating procedures. These include the following:

1. No human viewing of individual passenger images
2. No retention of individual passenger image data
3. Providing passengers with clear notice of choices
4. All physical searches to be conducted by officers of the same self-identified gender
5. All secondary screening to be conducted in private at passenger's election, and with a witness of passenger's choice
6. No passenger required to expose sensitive areas under clothing to reveal prostheses, medical devices, or other items
7. Physical searches to resolve an anomaly detected by scanning to be no more intrusive then necessary to resolve the anomaly
8. Training for TSOs to include working with diverse traveler populations

9. Nondiscrimination on the basis of race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, parental status, or gender identity

1. Automated Target Recognition Mandate

Congress has mandated that all body scanners employ ATR software, and it would be inconsistent for the final rule to authorize the use of scanners without this fundamental requirement. If they are to be used, the final rule must define scanners not only as technology that allows screening without physical contact, but also as technology that allows screening without human viewing of individual passenger images.

2. No Retention of Individual Passenger Image Data

TSA has stated that, with the use of ATR, individual passenger image data is neither viewed nor retained. The assurance that such data are not retained was central to the reasoning of the Court of Appeals in *EPIC v. DHS.*[8] Nevertheless, many passengers reasonably fear that their individual body image could be retained and viewed at a later time. If ATR is to be used, the final rule should define scanners as technology that allows screening without subsequent retention of individual passenger image data.

3. Clear Notice of Passengers' Choices

As previously stated, the use of pat-downs as an alternative to body scanners is grossly inadequate. Most travelers experience these pat-downs as *even more invasive* than scanners.

Passengers must be provided clear notice of the choices they are given by TSA. TSA's current practice of providing this information in small print on an 11" x 14" poster, in a crowded checkpoint area where passengers are rushed to load their belongings into bins, fails to gain the informed consent needed to make this choice meaningful. The "high level of acceptance" of the scanners cited in the NPRM is evidence of the inadequate notice of alternatives currently provided. As the Court of Appeals noted, "Many passengers . . . remain unaware of this right [to opt out].[9] The final rule must require that information about passengers' screening choices be prominently posted, in plain language and in large type, at all checkpoints.

[8] 653 F.3d 1, 4, 10.
[9] *Id.* at 3.

4. Physical Searches Conducted by Officers of Same Self-Identified Gender

The current use of body scanners is inseparable from the use of thorough physical pat-downs as an alternative as well as secondary screening measure. TSA's deployment of scanners cannot work without the use of pat-downs as a secondary method, and TSA's justification for use of scanners hinges on the use of pat-downs as an alternative. The inextricable link between these two, tandem checkpoint screening methods is underscored by the panel opinion of the Court of Appeals, which emphasized the importance of the pat-down alternative in mitigating the personal intrusion caused by the scanners.[10]

Accordingly, if TSA is to codify use of scanners it must also codify basic protections for the use of pat-downs. Among the most basic, minimal protections is TSA's long-standing requirement that, absent exigent circumstances, all pat-down searches be conducted by officers of the same self-identified gender as the traveler (rather than the gender listed on identification or the gender an officer assumes the traveler was assigned at birth).

5. Physical Searches Conducted in Private and with Chosen Witness at Passenger's Election

Also among the minimal protections long provided by TSA is that physical searches and other secondary screening be, at the passenger's election, conducted in a private location and with a witness of the passenger's choosing. This is also a basic expectation of passengers that must be reflected in the final rule.

6. Limitation on Requirement to Lift or Remove Clothing

Another key protection currently established in agency policy, which must appear in any final rule authorizing body scanners, is a minimal zone of privacy protection for travelers with personal medical devices or prostheses or other items under clothing that must be identified during screening. This includes not requiring passengers to lift or remove clothing in sensitive areas to reveal a prosthetic or medical device or any other item, and instead allowing travelers, when necessary, to conduct a self pat-down of the item, followed by an explosive trace detection sampling of the hands. If TSA is to authorize the use of intrusive routine pat-downs and body scanners, this fundamental protection must be included in any final rule.

7. Additional Limits on "Resolution" Pat-Downs

In addition, current TSA policy provides for "resolution" pat-downs to be limited in appropriate cases to only those areas of the body where an anomaly was detected by a body scan. If a body

[10] *Id.* at 3, 10.

scan has identified an anomaly only in the area of a passenger's head or arm, for example, it is simple common sense that further screening limited only to that area will be sufficient in most cases to resolve the anomaly. If no threat object is identified in the area highlighted by the scanner, any further physical screening is an unnecessary invasion of privacy and a waste of time. Any final rule that authorizes body scanners must codify a requirement that "resolution" pat-downs be limited to the area of an anomaly wherever possible.

8. *Comprehensive Training for TSOs including Working with Diverse Passenger Populations*

TSA has publicly committed to substantially expanding training for TSOs, including training on working with diverse passenger populations, many of which are disparately or uniquely impacted by aspects of TSA's current screening techniques – such as transgender and gender non-conforming people, people with disabilities, religious minorities, older travelers, and families with children. Robust training on these topics is essential to public trust in the screening process, and should be explicitly required by any final rule.

9. *Traveler Civil Rights Policy*

TSA's Traveler Civil Rights Policy should also be codified in the final rule, and should be expanded to include nondiscrimination on the basis of gender identity.

The Final Rule Must Use Clearly Defined Terms

In addition to the lack of passenger protections, the proposed rule uses vague, confusing terms that fail to adequately define the agency's authority for the use of body scanning technology, or to give sufficient notice to the public of the technologies' purpose or impact on travelers.

Most notably, the proposed rule authorizes the use of "screening technology used to detect concealed anomalies" without providing a definition or context for the term "anomalies." As commonly defined, an anomaly is "something different, abnormal, peculiar, or not easily classified."[11] This extremely broad and amorphous term could potentially incorporate not only foreign objects that could be put to a potentially dangerous use an aviation environment, but any item, garment, or even features of the traveler's own body that are deemed to be unusual. The use of this vague, undefined term fails to establish appropriate objectives and limits for security screening and invites abuse. Checkpoint screening should be expressly limited to the detection of prohibited foreign items that pose special risks of creating physical danger in the aviation environment. Codifying the limits of screening objectives in this way is essential to public trust.

[11] *Merriam-Webster's Dictionary,* http://www.merriam-webster.com/dictionary/anomaly.

In conclusion, HRC recognizes the difficult job that TSA faces in protecting the nation's transportation systems and, most importantly, its travelers. We strongly believe that TSA can fulfill its security mission while respecting the rights and dignity of all passengers. We look forward to continued dialogue and collaboration with your agency. If you have any questions regarding our comments, please do not hesitate to contact us.

Sincerely,

Brian Moulton

Legal Director

Comments in response to TSA Notice of Proposed Rule-Making regarding Passenger Screening Using Advanced Imaging Technology, Docket No. TSA-2013-0004

Summary of my comments:

TSA's body scanners are easily circumvented

TSA's body scanners are less effective at finding weapons than walk-through metal detectors

TSA's body scanners have well-publicized exploits and vulnerabilities

TSA's body scanners detect anomalies that TSA has no method for resolving

TSA's body scanners are humiliating and offensive, and create nude images of minor children

TSA's body scanners reveal innocent but embarrassing information

TSA's body scanners discriminate against the disabled, people with medical conditions, and others

TSA's body scanners interfere dangerously with medical devices

TSA's body scanners are not cost-effective

TSA's body scanner rule is not sufficiently detailed to inform the public how scanners will be used

TSA's body scanners create security vulnerabilities because they are slower than alternatives

TSA's body scanners and patdowns create adversarial tension between screeners and passengers

TSA's body scanners exposed passengers to carcinogenic ionizing radiation: there is no safe dose

TSA's body scanners increase the rate of patdowns, many of which constitute sexual assaults

TSA's body scanners cause more deaths than they prevent

TSA's body scanners are easily circumvented

There are many airports and checkpoints that do not have body scanners. For example, Reagan Airport's Terminal A and Fort Lauderdale's Southwest terminal have no body scanners. A full list of terminals without body scanners is available online at tsastatus.net. From the Congressional Research Service's recent report, we know this wide-open door for anyone to fly sans body-scanning will remain open: "Even at full operating capacity, not all airports and not all screening lanes will be equipped with AIT under TSA's plan." Only innocent travelers will ever be screened with body scanners – terrorists can evade it easily.

If a purported evildoer feared that a body scanner would reveal his plot, he could simply choose flights from airports and terminals that don't have body scanners installed, which is what I do when I fly. Only innocent travelers have to go through body scanners, because travelers might not be able to find a scanner-free airport to get them where they need to go. But it's a piece of cake to gain access to the passenger compartment of a commercial plane while guaranteeing you won't go through a body scanner. So we can be absolutely, totally certain that the TSA's body scanners will never and could never foil a plot.

Of course, our imaginary evildoer needn't even trouble himself to choose a scanner-free airport. Instead, he can simply travel with a child under 12 or a pet. Travelers meeting these criteria are diverted to the walk-through metal detectors. If any passenger can assure himself that he will be sent to a walk-through metal detectors, then WTMDs must suffice to search all passengers. A defensive chain is only as strong as its weakest link.

TSA's body scanners are less effective at finding weapons than walk-through metal detectors

The TSA's body scanners do not detect weapons, incendiaries, explosives, blades, or anything of the kind. Instead, body scanners detect what each passenger looks like without his clothes on. By contrast, walk-through metal detectors (WTMD) are capable of finding metal weapons, so they are in fact the superior technology compared with body scanners. It was widely reported that testers successfully brought guns through the body scanners in Dallas five times out of five tries. Those guns would have been detected by the WTMD. Some of the many concealment methods the Dallas testers could have used to bring guns through the scanners are detailed in the next section.

TSA's body scanners have well-publicized exploits and vulnerabilities

Some of the flaws and failings of body scanners are simply self-evident: that a scanner which sees the outer surface of our bodies can not find items between folds of skin, in one's mouth, or in other body cavities.

Kaufman and Carlson have published a peer-reviewed paper in the Journal of Homeland Security outlining another vulnerability of the scanners: that plastic explosives look like flesh to the scanner because both materials are low Z. This means that one can hide moldable explosives by fashioning them into a beer belly or other anatomically plausible shape with tapered edges.

If the item one wishes to bring through a body scanner is high Z (a metal gun, for instance), then it can be hidden from view by wearing it to the side of the body. Without one's flesh to provide contrast, metal objects will simply disappear into the background of the image.

Jonathan Corbett defeated the body scanners in this latter fashion with a sewing kit, and videotaped himself doing it. Millions of viewers have watched a how-to on sneaking metal objects past the body scanners on YouTube: http://tsaoutofourpants.wordpress.com/2012/03/06/1b-of-nude-body-scanners-made-worthless-by-blog-how-anyone-can-get-anything-past-the-tsas-nude-body-scanners/ There is another video available on YouTube in which a man sets off a rather large explosion on a German television show using only the items he sneaks through a body scanner, including a detonator which he hides in his mouth. (http://www.youtube.com/watch?feature=player_embedded&v=nrKvweNugnQ)

TSA's body scanners detect anomalies that TSA has no method for resolving

From the testimony of Fred H. Cate to U.S. House of Representatives, March 16, 2011:

But even if there were only a few "anomalies" detected by AITs, it turns out that the TSA has little ability to actually "clear" many of them. I was reminded of this just last week at Reagan Washington National Airport when the AIT discovered a loose aspirin in my shirt pocket. This anomaly called for a pat down. The agent felt the pill and said "what is this?" I said "aspirin" and he politely waved me through. It could just as easily have been potassium cyanide: neither the AIT nor the TSA agent has any process or equipment for determining the difference.

We have spent more than $2 billion installing a technology to identify "anomalies" that we cannot practically evaluate for the risk they pose. It was this inability to clear many of the false positives identified by AITs that led to the TSA's disastrous policy begun last October of intimate, intrusive searches. The problem is that despite their intimacy, the searches did nothing to help the agent determine whether the "anomaly" was a real risk or just another false positive.

This is especially clear in the case of people with medical devices or prosthetics. As a diabetic on an insulin pump—a device the size of a pager strapped to my waist that provides life-sustaining insulin—under the TSA's October policy, an agent would search me head to toe, including a careful pat-down of my genitals—as if somehow my genitals have become suspicious because I use an insulin pump. At the end of the search, however, the agent has no better idea than he did at the beginning whether the pump is loaded with insulin or high-tech explosives.

After two months of this policy, the TSA shifted ground and determined that insulin pumps would not require a full body search, but instead would be swabbed and the swab tested for explosive residue. A colleague of mine who works for the federal government and is also a diabetic described the indignity of recently having a TSA agent at Dulles International Airport reach inside her underwear with the swab. To what end? Are insulin pump users more likely than other travelers to secret explosives on their bodies? And what happened to the much-vaunted AIT machines that were supposed to detect the presence of such explosives? Why are we now swabbing inside travelers' underwear as well as using AITs to peer inside, especially when there is no sign of any "anomaly" from either technique?

I have found it easier and far less intrusive to simply remove my insulin pump before being required to undergo AIT screening. (I don't remove it before passing through a metal detector because it doesn't trigger any alarm.) I am fortunate to have this option; most travelers with medical devices or prosthetics aren't so lucky. But I am still left with the tiny plastic cannula in my abdomen to which the pump connects. The AIT sometimes—interestingly, not consistently—identifies this as an "anomaly." When it does, a TSA agent pats me down, feels the sensor, and says "what is this?" I say "an insulin cannula" and the agent invariably politely waves me through. The agent has no idea, no verification, and no certainty what is actually taped to my stomach. I am "cleared" not because the agent has determined that the plastic tube poses no danger, but because there is no way a TSA agent can make any further determination.

Many travelers suffer far greater indignities due to physical searches, triggered by AIT "anomaly" detection, that reveal nothing about whether the "anomaly" poses a threat. For example, after agents finish inspecting the breasts of a woman with an implant, they have no better idea whether the implant is filled with liquid explosives or silicone. The same is true with prosthetic limbs, urostomy bags, and most other medical appliances.

This type of response to having the AIT identify something as an "anomaly" is the very definition of "security theater"—it looks like the agency is doing something, but it accomplishes nothing. The same is true with many, perhaps most, of the searches that are triggered by AIT "anomalies." A rational person might question whether it is worth the money we are spending to identify "anomalies" if the vast majority of them (indeed, perhaps all of them) are false positives, and we lack the practical ability to follow up on many of them in any event. This is the height of ineffectiveness.

TSA's body scanners are humiliating and offensive, and create nude images of minor children

In order to use a body scanner, innocent travelers must hold their hands up in a surrender position, as if these are people being mugged, or booked into a jail. All body scanners create nude images of our bodies, even the scanners that supposedly have privacy filters. After the TSA's first batch of lies about the body scanners – in which the TSA claimed that scanners could not save or transfer images, until a FOIA lawsuit revealed documents showing that the TSA required manufacturers to build those capabilities into the scanners – the public can have no faith in the TSA's solemn vows not to look at these naked images.

The TSA is even forcing minor children to display their naked bodies in the scanners, despite laws against creating and viewing such images. The Rutherford Institute filed suit on behalf of the parents of a 12-year-old girl who was scanned and had her nude body viewed by strangers without the parents' knowledge or consent. No parent should ever allow strangers to create nude images of a child, but this is precisely the demand of the TSA's body scanner program.

TSA's body scanners reveal innocent but embarrassing information

The TSA's charge is to find weapons, not to investigate each passenger's anatomy to determine whether our bodies are acceptable or not. TSA body scanners have revealed intimate piercings and flagged anomalous genitalia. TSA body scanners have exposed transgender and transitional passengers, leading to further humiliation when screeners loudly and publicly demand that passengers declare themselves on the gender binary of male or female. TSA body scanners have even flagged menstruating women for extra scrutiny of their sanitary products and other people for their incontinence products. That some passengers have non-normative bodies or use sanitary products is not the slightest bit relevant to finding weapons. Investigating the private details of passengers' bodies is deeply offensive and has zero security value.

TSA's body scanners discriminate against the disabled, people with medical conditions, and others

In 2010, Alaska State Representative Sharon Cissna was forced to take a four-day ferry ride home after she traveled to Seattle to seek medical treatment. Cissna is a breast cancer survivor with a mastectomy, and Seattle's body scanners singled her out for a sexually invasive patdown of her breasts. Cissna is also a survivor of childhood sexual trauma, and she bravely refused to allow strangers to touch her breasts after a previous TSA patdown re-awakened her trauma.

Consider two elements of Cissna's experience that apply broadly: first, women with mastectomies and other people who have non-normative bodies as a result of their medical conditions will be selected for patdowns because of the body scanners. Frequent flyers with non-normative bodies will find themselves subject to weekly or daily humiliation. Another frequent flyer I know experiences twice-weekly patdowns in the Phoenix airport that she calls assaults, all because she is physically unable to hold her arms above her head as the body scanner requires.

Second, these patdowns are more frequently traumatic to female passengers, because a higher proportion of women than men have experienced sexual trauma. A huge part of recovering from sexual trauma is to regain one's autonomy and authority over one's body. To have that control over one's intimate body parts wrested away, in public or in a shameful back room, by a stranger in a threatening uniform, must be a perfect storm to re-activate traumatic memories in those with sexual trauma and PTSD.

Travelers who are transgender or who can't be visually sorted into a gender binary are also discriminated against by the body scanners. Why must body scanners require that complete strangers guess whether each traveler is "Male/Female"? Sex and gender encompass far more varieties than these, and body scanners create predictable distress about this issue that would never happen with walk-through-metal-detectors. Requiring that all passenger bodies fit neatly into two categories has nothing to do with security.

It is true that for a select group of passengers, namely those with medical metal, the body scanners may be less intrusive than walk-through metal detectors. Body scanners allow passengers with metal hips or joints to avoid the truly horrifying experience of a TSA patdown. For this reason, I encourage the TSA to maintain body scanners but allow passengers to choose for themselves between scanners and walk-through metal detectors. Again, since any traveler can guarantee by changing his routing that he will board a plane after using only a walk-through metal detector, there is no defensible reason not allow all passengers to choose.

TSA's body scanners interfere dangerously with medical devices

Sixteen-year-old Savannah Barry was forced to replace her $10,000 insulin pump after TSA screeners in Denver, Colorado ignored her request to opt-out and instead directed her repeatedly into a body scanner. The TSA claims that passengers have the right to opt out of body scanners, but in practice many passengers are cajoled, tricked, or intimidated into the machines anyway.

TSA's body scanners are not cost-effective

The TSA's Notice of Proposed Rule-Making (NPRM) details only the costs of the body scanner program to the TSA; it entirely neglects the costs imposed on every one else. Passengers bear the brunt of the cost in increased waiting time: if body scanners cause an average of three minutes' delay to 700 million or so passengers, then they cost the American public roughly one billion dollars in wasted productivity per year. Passengers also incur increased risk of death if body scanners divert them to less-safe travel modes like driving.

Importantly, the TSA's NPRM fails to quantify the decrease in risk of terrorist attack that it expects body scanners will achieve. What is the risk of a successful terrorist attack on an airliner with and without body scanners? Quantifying risk is an essential ingredient of cost-benefit analysis, which the TSA and DHS have repeatedly failed to apply. Consider the comments of the Committee to review the Department of Homeland Security's approach to risk analysis; National Research Council, National Academies Press, 2010. (http://www.nap.edu/catalog.php?record_id=12972):

"With the exception of risk analysis for natural disaster preparedness, the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making.

Moreover, it is not yet clear that DHS is ona trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses other than for natural disasters. (2_3, 80)

Little effective attention was paid to the features of the risk problem that are fundamental. (11)

Assessment of individual components of risk and their integration into a measure of risk is seriously deficient and is in need of major revision. (11)

Until these deficiencies are improved, only low confidence should be placed in most of the risk analyses conducted by DHS. (11, 98)"

In their excellent book Terror, Security, and Money, John Mueller and Mark G. Stewart examine unacceptable, tolerable, and acceptable risk quantification. Across a wide swath of agencies and governments, risks lower than about 1 in 700,000 down to maybe 1 in 1,000,000 are generally considered to require no further action or regulation. The risk of death by terrorism in the U.S. is lower than 1 in 3.5 million. In fact, death by furniture is more likely than death by terrorism.

Even under the most generous assumptions about the effectiveness of body scanners, Mueller and Stewart have shown in a peer-reviewed publication that body scanners are far too expensive to justify spending public safety dollars on them. Many more lives could be saved with those dollars by improving levees, building tornado shelters, installing carbon monoxide and smoke detectors, upgrading fire-fighting equipment, et cetera.

TSA's body scanner rule is not sufficiently detailed to inform the public how scanners will be used

Airline passengers are required to consent to a TSA search. However, both before and after the proposed rule-making, passengers have been given almost no information about what search will be conducted. Surely the most basic element of consent is to know what one is consenting to! The proposed rule implies that passengers who submit to a body scanner will not be touched, but this is belied by the huge number of people who endure a manual search after passing through a body scanner. Under what conditions will passengers who use body scanners be touched? Will screeners lay their hands on our genitalia through our clothing if the body scanner shows an alarm? What is the alternative search procedure if passengers opt out of the body scanners? Will screeners lay their hands on our genitalia through our clothing if we opt out?

TSA's body scanners create security vulnerabilities because they are slower than alternatives

The TSA's body scanners slow passenger throughput at the checkpoint, so using them will certainly make passengers less safe. A recent RAND study of airport vulnerabilities at LAX concluded that, "small, portable explosives have been the most likely and most lethal means of attacks at airports" and that "The greatest risks for casualties for most types of attacks are in the high-density areas passengers encounter before reaching the security checkpoint, particularly lines for ticketing and for passing the security checkpoint." Thus, body scanners are not only ineffective, they are actually dangerous because they leave travelers vulnerable as they wait in long lines.

TSA's body scanners and patdowns create adversarial tension between screeners and passengers

Predictably, forcing people who are not suspects in any crime to expose their nude bodies to strangers and / or submit to sexually degrading physical examinations makes victims angry. The TSA's body scanners have created anger and fear that poisons the relationship between the public and TSA. TSA screeners report being regularly excoriated and verbally abused by passengers since the body scanners and patdowns hit the news in November 2010. The TSA has made itself the enemy with its offensive actions, which means that it can only blame itself for a lack of cooperation from travelers.

This adversarial atmosphere damages our security. The TSA is forever claiming that passengers are its partners, but I want to make one thing perfectly clear: I will never, ever, be the partner of an agency that sexually humiliates people like this. John Pistole wants to put his hands down our pants. I want to stop him. John Pistole wants to take naked pictures of kids. I want to stop him. I am not now and I never will be "partners" with the TSA. Body scanners have made me and millions of others into the opponents of the TSA.

TSA's body scanners exposed passengers to carcinogenic ionizing radiation: there is no safe dose

The backscatter X-ray scanners produced by Rapiscan dosed millions of airline passengers with carcinogenic radiation. There is no safe dose of X-ray radiation; it is a standard medical dictum that ionizing radiation dose should be kept "as low as reasonably achievable". Exposing passengers to a known carcinogen for no medical benefit was unconscionable. The Committee to Assess Health Risks from Exposure to Low Levels of Ionizing Radiation, National Research Council, National Academies (http://www.nap.edu/catalog/11340.html), said after a comprehensive review of the available data that: "the risk of cancer proceeds in a linear fashion at lower doses without a threshold and the smallest dose has the potential to cause a small increase in risk to humans." Further, "The committee has concluded that there is no compelling evidence to indicate a dose threshold below which the risk of tumor induction is zero."

While it is true that Rapiscan backscatter X-ray machines have been removed from airports at present, there is nothing in the TSA's proposed rule that prevents ionizing radiation being used in the future as it had been used up until May of 2013.

TSA's body scanners increase the rate of patdowns, many of which constitute sexual assaults

The TSA's body scanners generate excuses for the TSA to conduct many more patdowns than would happen at a checkpoint without body scanners. In a German airport that tested body scanners with generic body outline privacy filters, the false positive rate was reported to be 54%. False positives might be caused by sweat, sequins, fasteners, seams, zippers, pockets, metallic threads, underwire, embroidery; in short, by anything and everything.

The TSA refuses to reveal its body scanner false positive rate, but casual observation suggests that screeners send a large proportion of passengers to a secondary patdown because of body scanner false alarms that would not have occurred with a walk-through metal detector. Further, many passengers are subjected to enhanced patdowns because these passengers *must* opt out of the body scanners to protect their medical devices or because they can not stand unassisted with their arms above their heads.

The TSA's proposed rule is deliberately misleading about the patdown procedures that are part and parcel of the body scanner program. The TSA states that "Advanced Imaging Technology currently provides the best opportunity to detect metallic and non-metallic threats concealed on the body under clothing without physical contact." However, it is clear from passenger reports that at least some people are subjected to a full enhanced patdown even after they submit to the body scanner, perhaps because they triggered more than five yellow-box alarms. Thus, any objections to the TSA's patdowns must be viewed as objections to the TSA's body scanner program.

The TSA has repeatedly refused to clarify whether screeners intend to make contact with passengers' genitalia in an enhanced patdown, but thousands of passengers have reported that screeners touched, rubbed, or hit their testicles, penis, vulva, or anus during these patdowns. Forcing sexual contact on an unwilling participant through coercion constitutes sexual assault. I fear I can not singlehandedly impress upon you the gravity of this concern, so I will let the voices of some of the victims speak.

"… he was so rough he injured my testicles and I was nauseated for hours. Please instruct your employees to be gentle with the old vet."

"The security agent aggressively ran the side of his hand upward into my testicles 4 times during the patdown. This action caused me physical pain each time. This was the first time I had been assaulted in this manner. The result of this action also caused mental anguish. When I complained to the policeman at the screening facility I was briskly informed that this was a federal government matter and that I 'have no rights here.'"

"I am required to turn down the waistband so the agent can pat my penis. Pretty degrading, you might agree, but nothing compared to my wife's experience."

"She felt all the way up and down inside my legs through an ankle-length dress. I felt violated and moved away, to which she responded, 'I'm not done yet!' This so shook me, an 82-year old virgin, that I sat in the area ½ hour to calm down. "

“We were made to stand spread-eagled … and the officers did not slide their hands. Rather they squeezed in a way that felt assaultive and demeaning.”

“She used the word ‘brutal’ to describe her patdown.”

”during a new patdown I received I had to ask the screener to remove his finger from my anus. I am humiliated for the fact that I had to make this request of the screener and for the fact that this happened in public.”

“Rather than perform a traditional patdown, my breasts, buttocks, and genitals were stroked and the agent placed her hands inside my pants and stroked my stomach and torso. I felt that this was sexually violating.”

“I can honestly say that day was one of the worst days of my life. I was chosen for the new patdown procedure, which is now referred to in my house as ‘assault and battery’.”

“This is a protest against the trauma I suffered from a sexually perverted woman employed by our federal government in the Spokane, Washington, airport.”

“His touch was firm enough that he felt the shape of my legs. This includes feeling around my crotch enough that he could clearly feel my testicles through my jeans. I couldn’t believe it. But the worst was yet to come. He then walked behind me, pulled my shirt tail out of my pants and then stuck his hands down my pants. He walked all the way around my body with his hands in my underwear. I’ve never been so humiliated in my whole life.”

“During the patdown the TSA employee gave such a severe chop to my groin that it not only hurt, but knocked me off balance.”

“He poked my penis and my testicles very hard, I was very much in pain from this type of inspection which has never been performed on me at any airport that I have ever been to. After he poked my private parts very hard, he proceeded to use the metal detector wand on my buttocks, he poked and stuck his wand into my rectum very hard and again I was very much in pain. I worked in a federal prison for 20 years and not even inmates were treated like I was treated by this security officer at the Phoenix, Arizona airport.“

“To say the least, the experience was both intimidating and humiliating. The TSA agent only said – you are not going to avoid the body scan or a patdown. I began to freak out and started to cry. Immediately I was surrounded by three TSA agents, all who began yelling at me. They continued to harass me and say, ‘you are going through the scanner.’ Suddenly another TSA agent was on her knees giving me a full patdown (including legs, private areas, etc.) That should have been the end, however, I was pushed into the scanner.”

“The experience is beyond demeaning. Picture the nastiest, surliest, grossest, most belligerent DMV employee you’ve ever encountered and now picture that this person has the right to put their nasty, vile, gross hands all over you. And be verbally abusive as well. The thug who groped me whispered something in her compatriot's ear and they both apparently had a good laugh at my distress."

"I said that I had a torn right shoulder rotator cuff. He then asked me to hold my arms up. I said I couldn't. He said that I had to anyway. The patdown took 3 to 5 minutes and I finally lowered my shoulder as the perspiration rolled off my forehead from the pain. Now I am overweight, say 250 pounds. I had no belt on and the officer after first doing my front, sides top and back, went back to the front of my waist and grabbed my fat. He said, 'what do you have in here?' I said, it's me, it's my skin. Then the three of them chuckled, laughed, and let me go to my gate. I am still shaking when I think about how I was treated! I am barely sleeping… everytime I fall asleep I wake up sweating and shaking. I don't know if I will ever fly again."

"I then had a patdown so abusively rough that it left bruising on my left arm. This treatment had nothing to do with safety – it had to do with power and unquestionable authority of these TSA individuals."

"Is a TSA agent allowed to spread my labia in her inspection? Why is a TSA agent allowed to put so much pressure on my breasts that she leaves bruises? Is this standard procedure? When I ask the TSA agent to touch her own body where she intends to touch mine, so I can get a true and honest understanding of her techniques – why is she allowed to refuse providing such explicit information?"

"The way I was treated made me never want to fly again. In the future I will just make the 8 hours to Denver by car. It will certainly be easier and less demeaning. I was treated like a criminal, separated from my 13yo son, taken to a separate room so that I could have the demeaning patdown that for some reason takes three men to perform. I don't care all that much about a patdown for me, because I'm used to taking abuse from uneducated people in my line of work. I will say, however, that if they tried to treat my son that way I would have punched the guy.

I expect you not to repond to, or even to see, this letter. Please know that I would much rather have no response than a patronizing response about how everybody is doing their best. If this is your best, woe is us."

"It was one of the worst experiences of my life. I never want to be subjected to this kind of physical, mental, and emotional abuse again, especially anywhere in the United States of America."

"Then the search became much worse. The TSA agent felt my breasts and buttocks in a very thorough manner, much more invasive than in the past. She then lifted my blouse and took two fingers from each hand and stretched the elastic of my slacks and underpants by going completely around my waist inside my clothes, looking down into my underwear. Next she felt my legs and thighs over my slacks and ended this intrusive search by grabbing my groin. I dread the thought of having to go through TSA again, and I do not think that as an American I should feel this way."

"My husband is so undone by the thought of me or my daughter being groped in this manner that he is strongly encouraging me not to fly. I do not believe that scanning or groping me and other passengers in this invasive, humiliating, and degrading fashion will result in a higher level of safety."

"I am still fuming over my experience yesterday afternoon at the Fort Lauderdale-Hollywood airport. "

"As a result of these intrusive and offensive body searches, [my wife] is reluctant to travel anywhere."

"As I was leaving the pat down (sexual assault) area I conversed with two older women. Both had knee replacements. The eldest (in her late 70's I would guess) was in tears. She could hardly walk and was also horrified. She had a dress on and couldn't believe where the TSA person had stuck her hands. This has got to STOP‼ I find this procedure mortifying, discriminatory, and a total violation of basic human rights. All any of us were doing was flying to see grandchildren or other relatives. We should NEVER be subjected to this kind of treatment. This just makes the terrorists the winners in this ugly battle. Please do everything possible to stop this physical assault of anyone who has to fly. Please!"

"As an armed posseman of the Maricopa County Sheriff's Office I am trained and certified in searching prisoners, including patdowns. Before this training I was required to pass a strict police background check on many levels. I fly a lot and I have personally watched people being felt up, not patted in any way, but full open hand rubbing of crotch and legs, in public, by people that from my considered perspective would never make it to the police force."

"On November 2nd, flying out of Riverton I was subjected to the new, more invasive patdown by a TSA agent. This now includes shoving a hand between my legs, pushing it up into my crotch, and grabbing and squeezing my inside thigh. This was repeated four times – on each leg – from front and back. That is 4 shoves, 4 pushes, 4 squeezes. I am not overly modest – but I was greatly offended and felt violated. This is unacceptable treatment."

"I strenuously object to the complete body groping so-called patdowns to which I am now being subjected. They are intrusive, degrading, and humiliating. "

"I was appalled, embarrassed, and admittedly, afraid. I did not want her or anyone else to touch me like that, but what choice did I have? The TSA agent who searched [my friend] was very intrusive. The TSA agent ran her hands all over her body and used enough force in touching her vaginal area to separate the folds of her skin. I was mortified and deeply hurt with her. Had this happened on a bus we would be calling the police for protection and assistance."

"She said that the screening would be more invasive. I was unclear what that meant. I was not aware the TSA had changed the nature of secondary security screenings. The agent touched me twice in my groin area and frankly, I was shocked! I was not expecting her to touch me inappropriately. Having a private screening is not the point of my letter. I don't want anyone touching me between my legs. I consider this screening a sexual violation. I consider the space between my legs PRIVATE!"

"This past week I have been made to feel like a common criminal by our nation. My crime: having a medical implant (artificial metal knee) and then traveling by air within our nation. Until today the procedure was to hold a hand-held scanning device and then pat-down the areas where there was a signal. I knew the change was coming, but until I experienced it, I did not realize how violated I would feel."

“I felt violated. If any other person had done this to me it would constitute sexual assault. We tell our children to tell people to stop if they are touched inappropriately, but there was nothing I could do about this. If I did not do the patdown they would not let me on the plane. I felt like a criminal.”

“On November 23rd, 2010, I endured the most humiliating event of my life at the hands of TSA agents at a security checkpoint at the Raleigh-Durham airport. My patdown ended with a uniformed TSA agent sticking his hand inside the waistband of my underwear. I can’t believe that such invasive, dehumanizing treatment is sanctioned by the TSA or that it is even legal.”

“This kind of mandated inspection where a federal agent manipulates my breasts and feels my crotch is not acceptable in a free society. I must go through a screening and patdown procedure every time I fly, and my job requires me to fly 2 to 4 times per week.”

“This new strategy is creepy, disgusting, and from my perspective, pointless. Therefore I am interested in knowing about your new method of keeping our country safe by touching my groin area four times.”

“The fact that we are doing this to our children (over 12 is still a child) is absolutely horrendous to me. After years of teaching our children your body is yours, no one can touch your private areas without your permission, we are now going to stand by while a perfect stranger in an airport touches our children inappropriately?! It brings me to tears when I think of all the children that have already been the victims of abuse being put through this. How do people sleep at night knowing this? I feel less safe with these measures in place.”

“It was disgusting and abusive. If I had been violated in this manner on a Chicago street I could have called the police and asked them to arrest the person. The assault of the traveling public needs to stop.”

“My 17 year old daughter was told that she needed to submit to a full patdown after being told ‘it did not scan’. Being 17, she had no idea what that meant or how intense a detailed full body patdown can be. Even when she began to cry, the TSA agent continued the patdown. My daughter felt molested and violated and as a parent I was helpless to stop this violation. As a parent, I have serious concerns that such a search could be conducted on a minor. This search crossed the line.”

“I just thank God my six year old daughter was not with me because I believe she would have been truly frightened to see her mother being treated in such a manner. Seriously, it was enough to make me not want to fly anymore.”

“What followed was nothing short of sexual assault in public. I retired from the Air Force Reserve as an officer in 1994. My broken body is all that I have left. Simply because I was severely disabled by osteoarthritis, TSA now expects me to willingly submit to sexual assault by a complete stranger each and every day I go to work for the rest of my life.”

“First the coerced physical contact in public and then the deliberate lies contribute to a sense of abuse. In another context this would be fourth degree sexual assault. TSA’s behavior makes us feel less safe, not more safe.”

"I was not aware of the new patdown regulation and was quite startled when the TSA female was prodding my breast. I was sickened by the way the person was touching me. I was extremely devastated when she told me to spread my legs and put my right foot forward as she had to run her hands up my leg. I informed her not to touch my private area and she informed me that she had to run her hands over my genital area. I was furious."

"I was already hysterical and crying when she began her examination. Once again my breasts, my inner thigh, brushing against my virginal area and the inside of my waistline were physically examined. A pad was wiped across my hands to screen for explosives! This TSA agent also implored me not to cry and tried to explain why it was necessary and that she didn't like doing it either. What possible difference would it make to her if I cry? Who is she to tell me how to feel or react as long as she got her job done? Simply because TSA agents are of the same sex when they perform the whole body patdown does not make this experience any different than if they weren't of the same sex.

In my opinion I was sexually assaulted and abused at LAX and MCO airports by TSA agents. I want you to know that I was touched chest to ankle by someone other than my husband. I was examined for explosives. I was humiliated and insulted and assaulted without due cause and in my opinion against my will. Not being able to control my feelings and still crying as we boarded I thought that if I were a child this would legally be considered molestation in the first degree. As an adult with a disability it should be considered sexual abuse and a crime against persons with disabilities. I am a 63 year-old woman. I have never been arrested or been to court. I have no record of ever being a person of interest to anybody. I am white, I am American, I am a United States citizen and I am angry!"

"After telling the TSA agent that my breast were extremely tender and PLEASE don't hurt me, she turned sadistic and was so rough with me that I involuntarily screamed out in pain and my tears were immediate. I felt like I had been sexually assaulted. I hope your daughters or wife would never have to go through what I went through. I have to fly on the first of December and I am terrified, so yes, the terrorist have won. I would rather die than be molested again and yes, I am a victim of sexual assault."

"While reading this story, I became appalled at the very notion that adults who act as an aviation security and screening force (TSA officials) would consider the option to convince a child and their parents/guardians that having a stranger in a uniform (TSA officers) touching the child in otherwise forbidden places, was a 'game'.

This is the most repulsive thing I have ever read! I am shocked that this is what we've come to. Furthermore, the article claims that sex abuse victims may receive an alternate screening process. I would like to know just how TSA administrator John Pistole will go about making changes to TSA screening rules for victims of sex abuse. That is, will victims of sex abuse be made to preregister for screening or will they have an exclusive TSA Sex Abuse Victim Elective Screening (a.k.a. 'SAVES') I.D. Card?

Additionally, I was able to find an on-camera interview with TSA Regional Director, James Marchand- where Mr. Marchand suggests "You try to make it as best you can for that child to come through. You ask the child to put their arms up in some way, and if you can come up with some kind of game that you're trying to play with the child, then it makes it a lot easier." Prior to this statement, the news reporter's own three year old daughter was recorded on camera screaming and crying at the TSA officer "Stop touching me!" all the while the mother restraining the child into the TSA officer's submission. Children of all people know when behavior is inappropriate, even if they do not understand what the behavior is.

Is this really who we are? Is this the present and future that my family and my child have to look forward to?"

"In early October, I became a victim of an 'enhanced patdown'. It was one of the most degrading, humiliating, repulsive experiences of my nearly 70 years. The prior pat down process was degrading enough, but now, to have one's testicles weighed by the hand of male stranger while standing in public goes beyond reasonable into the realm ofKafka-esque absurdity. I choose not to put myself in this position, and thus not to fly."

"I walked through the scanner without buzzers or incident. I then apparently was randomly chosen for humiliation.

I objected verbally to the invasion of my privacy and excessive search of my body without any stated cause or reason. Toward the finish of the patdown, when the rep stated that she was going to feel my breasts, I raised my shirt revealing a sports top, making it visually clear that there was nothing concealed in my breasts. [The screener] began to holler at me, and called in his reinforcements. Immediately two police officers and three or four more TSA employees appeared. I was told I would be arrested for disorderly conduct. The TSA supervisor threatened to escort me out of the airport causing me to miss my flight home.

Another TSA employee was brought over to give me a second patdown. [The screener] ***searched my crotch, not once, not twice, but three times.*** The patdown was repetitive of the first patdown and then repetitive of itself as [the screener] invaded my body already searched with special repetitive attention to groping my crotch and fondling my breasts. [The screener] then demanded that I lift my shirt, despite the fact that the police had just told me that lifting my shirt was disorderly conduct, after which she put her hands down my jeans.

Hostility overflowed and made it clear that I was being punished for the audacity to object to government employees feeling and groping my body. The screening manager exuded self-importance, clearly an under-trained man with little grasp of his real responsibilities and the purpose of the TSA. He was determined to see me grovel."

"To say the least, I felt that I was sexually assaulted by the procedure. The procedure included a complete wipedown of all parts of my body including shoulders, arm, chest, back, torso, buttocks, crotch, thighs, and calves. While the 'patdown' historically involved agents using the backs of their hands, the enhanced procedure allows the agent to use the palms of their hands and fingers to wipe down almost all areas of my body. This wipedown included having the agent, while standing behind me, sliding the palms of her hands down and around my buttocks and between my thighs and sliding her fingers over my crotch. The agent then came around the front of my body and slid the palms of her hands up my legs and her fingers over my crotch. As if offering some sense of decency, the agent slid the back of her hands all around my breasts. The new procedure also included the agent pulling the waistline of my garment away from my body and waching down into my garment while sliding their hands around my complete waist. Completely mortified by the experience, I was finally allowed to gather my belongings that had sat in an open, unsecure area during the exam, and the agent sent me on my way.

When I returned through Chicago on November 11, 2010, I was again pulled out of line. By this time I vocally objected to having my genitals touched in full view of passengers. Only after repeatedly asking that the agent not touch my genitals was the manager called over to deal with the situation. As she lectured me about the fact that the new enhanced procedures were standard policy and while the agent tried to continue the exam, a crowd gathered to watch. The reactions from the crowd ranged from outright laughter to shocked faces as the agent reached up my leg and slid her hands and fingers across my crotch. The exam continued in full view of passengers without consideration of my objections. Only after the crowd became large enough to impede the flow of traffic did the manager's boss have the manager remove me to a private screening area. Only then did the agent or manager give any consideration to my personal belongings, which sat unattended on the end of the table. Thankfully, a passenger had seen what was going on and was kind enough to gather them into a pile before moving on.

What ensued was even more appalling that I imagined. I was made to walk through the security area in my bare feet until I objected and asked for my shoes, which the agent and manager initially denied. Once in the private area, the agent in consultation with the manager conducted the enhanced pat down procedure as if I did not exist.

At no point would the agent speak to me or acknowledge my objection; In addition, the manager continually dismissed any concerns I raised about the new procedures, explaining that their staff is 'professionally trained' to conduct such procedures. She even stated that they did not touch passengers' genitals, but rather their 'groin', and explained that the procedure requires them to slide their hands up a passenger's thigh until they feel resistance and then examine the area. She also stated that if I was uncomfortable having my clothes touched, I could disrobe. With that she offered me a sheet of paper - the type offered in a doctor's exam room - to wear, if I preferred. In addition, the manager told me that I would not be allowed to board my plane, if I did not comply with the exam procedures. When I responded that I did not like being threatened, she replied that it was not a threat but merely information as to what I could expect if I did not comply.

When my children were young I repeatedly told them that no one has a right to touch the private parts of their bodies. As a woman I am well aware of when someone's touch crosses acceptable boundaries. I am at a loss to understand why the TSA believes they have a right to violate my body in the name of security or what leads them to believe that by subjecting me to a demoralizing examination the skies are suddenly safer."

"I was subjected to the hand screen, euphemistically called a patdown when in practice there is no 'patting' going on at all. It is not possible for a hand screener to find an explosive on my body by putting her hands on my vagina, but that is exactly what she did. The buttocks, back, and breast explorations were bad enough but the invasion of my vaginal area caused me to have a traumatic reaction that lasted for days. It was no consolation that the screener was the same gender that I am. You cannot possibly believe that this is going to solve whatever the cause for this invasive handling of the inside of a traveler's thighs to 'where the legs meet the trunk.' This must be stopped."

"But their pat down on me was up and down my pant legs, torso, arms, shoulders, and testicles felt, I am 78 yrs old. My wife, 76 yrs old, was patted down inside her bra upper and lower, they used the back of their hands, then they went under her panties and reached all the way down in front and back. On the outside she was patted all around arms and legs, back and front, but two thumbs pressed up toward and into her labia- uncalled for. I feel we were wrongly checked over and too much-personally, for me and especially my wife having hands inside her bra and panties and thumbs up her private area.
We have joined the Tea Party and trust me, we are telling all the people we meet how we were treated. We will NEVER fly again."

In reading the letters from victims of TSA patdowns, strong patterns emerge. Nearly every letter uses one of these turns of phrase: demeaning, degrading, dehumanizing, humiliating, violated, traumatized, sexually assaulted. How did being coerced into letting TSA employees handle their genitals impact the victims? Many people cried and dissolved into shaking or nausea.

"I stood there holding my baby in shock. I did not move for almost a minute. I stood there, an American citizen, a mom traveling with a baby with special needs formula, sexually assaulted by a government official. I began shaking and felt completely violated, abused and assaulted by the TSA agent. I shook for several hours, and woke up the next day shaking."

"It wasn't so much the 3 vertical strokes and three horizontal strokes he gave my penis (over my pants)… humiliating as that was … it was when he put his hand INSIDE my boxers, cupped my testicles then had my turn around and slid a finger down and inside my butt crack. That killed me. I'm a grown man and I was in tears."

"It is now over a week since I endured the following incident at Denver airport and I am still in total shock and intensely sickened that a situation like this can occur at any U.S. airport. I have NEVER been treated with such lack of respect in all the many miles I have traveled here and internationally. Additionally, in my clinical practice I cannot imagine treating a patient in this manner! It was dehumanizing.

I cannot emphasize enough that I was totally, but totally, shell-shocked. Nothing like this had ever happened in my life before and I felt like I was in a totalitarian dictatorship. No rights, belongings, no personal worth, nothing. I was nauseated to the extreme and could barely think. Of course by this time my flight had departed."

"This thorough patdown was horrifying. (Please forgive this most graphic and embarrassing description.) She ran her hand and patted (more like groped) every part of my body, all around and over my breasts, up my legs, and literally patted every inch of my groin – front and then back. I felt like crying, hitting her, curling up in a ball, and screaming all at once. I have never felt like I had been sexually assaulted before this incident. I was shaking and infuriated for hours."

"They touched my genitals four times and then my breasts. I was sobbing by the end of it. I am sentenced to this violation again tomorrow and every time I fly. I am an abuse survivor and this is traumatic to require this violation. I must fly home tomorrow and I don't know how I'll get through it."

"I have a history of physical as well as sexual abuse, and I experienced the rough touching as violating. My PTSD kicked in and I began to cry. I was asked again if I would like a private screening but to a person who has been violated, there is less security in a private area than being in a public area. By now there were 4-5 TSA workers gathered around me and focusing the attention of other travelers on me. I again began to cry and shake.

I am a strong person. I know all the coping techniques for handling a trauma-inducing situation and my techniques failed me. I want to be free to travel by air and enjoy my professional as well as personal rights to life, liberty, and the pursuit of happiness."

Others assaulted by the TSA reported sleep disturbances, nightmares, and flashbacks to the experience.

"I spent many a sleepless night since this experience wondering what I did wrong to deserve this type of treatment by my government."

"On November 2, 2010 I arrived at SeaTac airport where, unbeknownst to me, the intrusive patdown protocol had been instituted. I really could not have imagined that some stranger would put her hand up my legs to my groin, down my buttocks, and across my breasts that were not even encased in a bra – and all this was done with hundreds of people milling around to watch the 'show'. My initial reaction was to scream or to use my hands to protect myself. At the gate and on the plane, out of total frustration and anger I fought back tears. For the next four days while I was attending a major international scientific meeting I had difficulty falling asleep as I relived the awful experience. I had nightmares about it and wondered if I would have to travel across the country by train to get home. The difficulty falling asleep has persisted and the process of writing this letter has only worsened the insomnia.

I was powerless. Some strange woman was going to put her hands on my breasts and groin and I had absolutely no recourse. When I returned to Seattle I resigned from [a group] which meets in Washington DC, because I refuse to travel by air until this process is corrected."

"She was subjected to the most intimidating and humiliating sexual molestation I have ever witnessed. As a former rape victim in college, she was forced to relive this horrific event as she was reduced to tears and trembling. Numerous women who fly daily experience similar trauma, many quietly, as our government uses these highly sexual and intrusive measures to protect us. My wife's horrific experience has caused this million mile flyer subsequent nightmares, sleeplessness, and a genuine fear of flying."

Still others described ongoing emotional symptoms: powerlessness, rage, fear, and depression.

"The further humiliation and violation of the patdown is more than I can tolerate. I wish to make a formal complaint of sexual abuse and harassment. No one should have to endure having their body felt up three times in a 30-day period. I feel violated and depressed and disconsolate about what has happened to me and I am very fearful about what I will endure when I travel again. What can I do to be <u>completely</u> assured that no TSA person will put their hands on my body? I can not stress enough to you how <u>outraged</u> and <u>upset</u> I am. I think that if another TSA person touches me again, I may strike them."

"The patdown was very deliberate and invasive causing soreness in my groin area for several hours. I believe the patdown was an invasion of privacy as well as an assault, in addition to being embarrassing, physically painful, and causing me long term emotional distress. I can not physically or mentally withstand the same experience again. [Must] I discontinue flying until some sanity has returned to your organization?"

"Your agent manipulated my breasts – pushing her hand under and in between them. Then she proceeded to tell me she was going to check my inner thighs, starting at the juncture of my upper leg. However, your agent was either so ignorant of human anatomy or simply a sexual pervert hiding behind a badge because she rammed – and I emphasize the word rammed – her hand up in between my labia until it hit my pelvic bone. Then she spread my labia and felt all the way down my leg for whatever she felt I must have been hiding. I thought at first that this was a clumsy and insensitive move on her part but she repeated the same procedure when 'investigating' the left-hand side of my labia and inner leg. I burst into tears at this demeaning and dehumanizing invasion of my privacy and could not think or see clearly.

I have no choice but to fly every week, so I must subject myself to the physical, invasive torture every single time I trip the metal detector, which will be every time because of my metal implants in my hips. I love my job and desperately need the work but I may have to quit because I am becoming depressed and moody. To be honest, I feel that I am suffering from stress that is typical of victims of sexual assault. I feel hopeless and helpless. I can't sleep, I can't eat, and I am finding it difficult to do my job. I know full well that [TSA agents] have the power and authority to deny me access to the plane that I need to board to go to work or to return to what little sanctity I have left in my home."

As the latter letter-writer notes, the symptoms that all these victims describe are the same as those associated with sexual assault trauma – crying, shaking, and nausea in the moment; nightmares, insomnia, and lasting fear and depression as the trauma is processed. It matters little whether TSA's search procedures are legally classified as sexual assault or not – for a certain population of people, the impact of a patdown and sexual trauma will be similar, and profound.

The excerpts above are drawn from just one sample of TSA complaint letters from the months of November and December 2010. (http://www.scribd.com/doc/105000289/104904507-TSA-Complaints-2010)

What's heartbreaking is how worthless and pointless all of this pain has been. How many weapons has the TSA ever found in between the folds of a woman's labia? What exactly is "safe" about strangers spreading open the skin at the entrance to a teenage girl's vagina against her will?

TSA Administrator John Pistole has said of patdowns and body scanners, "Yeah, it's inconvenient."

Compare that to what the Supreme Court had to say about bodily integrity in UNION PAC. RY. CO. v. BOTSFORD, 141 U.S. 250 (1891), "The inviolability of the person is as much invaded by a compulsory stripping and exposure as by a blow. To compel any one, and especially a woman, to lay bare the body, or to submit it to the touch of a stranger, without lawful authority, is an indignity, an assault, and a trespass; and no order of process, commanding such an exposure or submission, was ever known to the common law in the administration of justice between individuals."

TSA's body scanners cause more deaths than they prevent

Because of the TSA's body scanner program, I have shifted a large proportion of my travel to driving trips. Driving is a far, far more dangerous proposition than flying, but I would rather take the risk of dying than let a complete stranger create nude images of me or touch my genitals. The TSA offends people and causes diversion from the airplanes to the roads, which means that the TSA causes 15 excess road deaths for every million passengers diverted. If just one percent of the 700 million annual would-be air passengers decide to drive instead of flying because of the body scanners, then the TSA's body scanner program will kill more than 100 people.

At least one angry passenger diagnosed the problem perfectly in his complaint letter, released recently pursuant to a FOIA request: "Do we as law-abiding citizens have no rights? … It seems to us that we are in more danger from Homeland Security than from terrorists."

Kathy Huff

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4761

Tracking Number: 1jx-8618-ckn4

Comment

"Dear TSA:

As member of the LGBT and allied community, I am deeply concerned that the TSA's proposed rule does nothing to protect passenger privacy and merely expands the agency's power. Transgender travelers especially are put in fear of being outed, humiliated, and facing additional screening because of their appearance, physical characteristics, or necessary personal items.

TSA should conduct a new cost-benefit analysis that fully considers the impact of both body scanners and pat-downs on traveler privacy.

I urge TSA to adopt Regulatory Alternative #3, using walk-through metal detectors and explosive trace detection instead of body scanners and pat-downs. Alternatively, TSA should consider additional regulatory solutions that reduce reliance on body scanners and prison-style pat-downs as primary screening methods.

To the extent TSA continues the use of body scanners and pat-downs, the final rule should codify minimum protections, including guaranteeing individual passenger image data is not retained; that all physical searches are conducted by officers of the same self-identified gender; that secondary screening will be conducted in private at passenger's election; that no passenger is required to expose sensitive areas under clothing to display any item; that searches to resolve an anomaly are no more intrusive then necessary to resolve the anomaly; that screeners receive training on working with diverse populations; and that no traveler will be subject to discrimination on the basis of gender identity.

Sincerely,
Kathy Huff

Document Information

Date Posted:
Jun 28, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Kathy Huff

ZIP/Postal Code:
78412

FAMILY EQUALITY COUNCIL

June 24, 2013

Docket Management Facility
U.S. Department of Transportation
1200 New Jersey Avenue SE
West Building Ground Floor, Room W12-140
Washington, DC 20590-000

Re: Docket No. TSA-2013-0004, Passenger Screening Using Advanced Imaging Technology

Family Equality Council is pleased to provide the following comments on the above notice of proposed rulemaking (NPRM). Family Equality Council is the national organization that supports, connects, and represents the three million parents who are lesbian, gay, bisexual, and transgender (LGBT) and their six million children. Almost 40% of transgender people are parents, and almost 20% of transgender people are caring for at least one dependent child.[1] Discrimination and lack of culturally competent care have negative impacts on transgender people and their families. We are therefore grateful to have the opportunity to comment on traveler privacy, an issue important to the transgender community.

While we appreciate the steps the Transportation Safety Administration (TSA) has made to address concerns from the LGBT community, these concerns cannot fully be resolved within the agency's current approach to screening. The NPRM is fatally flawed, nonresponsive to the concerns identified by the Court of Appeals, and especially problematic for vulnerable traveler populations such as transgender people. Instead, the NPRM is merely a rubber stamp of unlimited authority to use privacy-invasive screening techniques. We are deeply troubled that TSA's cost-benefit analysis completely ignores real passenger privacy interests that are impacted by the proposed regulatory approach, and that the NPRM proposes neither any change in current policy nor even to codify the minimal passenger protections in current agency practice. We urge the agency to conduct a new cost-benefit analysis that fully considers the ways in which, notwithstanding existing mitigation measures, passenger privacy is in fact impacted by the current screening approach. We further urge you to adopt proposed regulatory alternative #3 (walk-through metal detectors supplemented with explosive trace detection) or, alternatively, to consider additional regulatory alternatives to reduce reliance on body scanners and prison-style pat-downs. Finally, to the extent that any final rule incorporates *any* use of body scanners and/or prison-style pat-downs, it must at a bare minimum codify protections for passengers that are already part of TSA practice.

There can be no doubt that TSA has a public trust problem, that the existing airport screening approach does impact traveler privacy, and that it disparately impacts transgender travelers among other traveler groups. We urge you in the strongest possible terms to issue a fair and well-considered final rule that provides more than a rubber stamp.

---

[1] Grant, Jaime M., Lisa A. Mottet, Justin Tanis, Jack Harrison, Jody L. Herman, and Mara Keisling. *Injustice at Every Turn: A Report of the National Transgender Discrimination Survey*. Washington: National Center for Transgender Equality and National Gay and Lesbian Task Force, 2011, 90-91.

Transgender Travelers Are Disparately Affected by TSA's Invasive Screening Approach

An estimated nearly 700,000 adults in the United States, or 0.3% of the adult U.S. population, are transgender.[2] While estimates of the population of transgender children and adolescents are lacking, this population is also significant. In a national survey conducted in 2008-09, more than one in five transgender adults reported having been harassed or disrespected at the airport.[3] Since the implementation of the current regime of routine scanning and pat-downs, LGBT organizations have continued to be contacted with stories of harassment, rudeness, being singled out for additional screening, and other potentially discriminatory treatment of transgender children and adults and their loved ones and families. In addition, LGBT organizations continue to hear from many travelers that they are afraid of going to the airport, uncertain of how they will be impacted by current screening techniques or treated by Transportation Security Officers (TSOs), and in some cases are unwilling to fly as a result.

While we recognize and appreciate the modest steps TSA has taken to improve screening procedures, staff training, and traveler education with regard to this population, transgender people will always be disparately impacted by any system based on routine scrutiny of the contours of passengers' bodies under their clothes, whether by body scanners, prison-style pat-downs, or the current combination of both. Transgender people's unique bodily sensitivities, common use of sensitive prosthetics, high rates of past physical and sexual trauma, and pervasive experiences of harassment and other discrimination in all area of social life, make the routine use of even modified scanners, when paired with intensive pat-downs as the only alternative option or form of resolution, a very serious imposition on individual privacy, comfort, and well-being.

TSA's Cost-Benefit Analysis Completely Ignores Passenger Privacy Interests

The ruling of the Court of Appeals directing the agency to undertake this rulemaking was premised on a simple conclusion: "Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT [advanced imaging technology] scanner intrudes upon his or her personal privacy in a way a magnetometer does not."[4] Yet the NPRM and accompanying Initial Regulatory Impact Analysis fail to acknowledge any impact whatsoever on the privacy of the traveling public. Instead, the IRIA simply claims that the privacy protections noted by the Court of Appeals, together with the Congressional mandate for automated target recognition (ATR) software, have "adequately addressed privacy concerns."[5]

While these steps are laudable, they are not reflected in the actual rule TSA has proposed. Nor do these measures eliminate all privacy impacts on the public. Even with most of these measures in place, the ruling of the Court of Appeals was premised on a real privacy impact from body scanners. While the ATR mandate is a positive step, it also does not eliminate all privacy impacts. The agency tacitly admits as much by stating in its Initial Regulatory Impact Statement that it "anticipates future advancements to AIT in. . .privacy protection" and by stating that its proposed regulatory approach has the "Potential for

[2] G. Gates, *How Many People Are Lesbian, Gay, Bisexual and Transgender?,* WILLIAMS INST. ON SEXUAL ORIENTATION LAW, UCLA (Apr. 2011), http://williamsinstitute.law.ucla.edu/wp-content/uploads/Gates-How-Many-People-LGBT-Apr-2011.pdf.
[3] *Supra* note 1.
[4] EPIC v. DHS, 653 F.3d 1, 6 (D.C. Cir. 2011).
[5] IRIA at 101.

negative public perception on… privacy concerns"[6] Indeed, as the Congressional Research Service has noted, respondents in a 2010 survey identified privacy more than twice as often as delay as a primary concern with AIT.[7]

First and most importantly, the use of body scanners as a primary screening method is inseparable from the use of highly intrusive physical pat-downs. These screening techniques are inextricable because (1) TSA relies on the alternative option of pat-downs to mitigate the privacy impact of the scanners themselves, and (2) TSA relies on the use of pat-downs to resolve many, if not most, anomalies identified by ATR. While TSA regularly cites the high rate at which passengers opt for scanning over pat-downs, this rate demonstrates not that passengers view scanners as non-intrusive, but rather that most view the alternative of a prison-style pat-down as *even more intrusive*.[8] Accordingly, pat-downs are an essential part of the operation of body scanners, and the privacy impacts of the use of pat-downs in conjunction with body scanners must be assessed in this rulemaking. Additionally, ATR does not eliminate the privacy impact of body scanners themselves. Even with this software, scanners generate and analyze data representing the contours of passengers' bodies underneath their clothing, and use this data to highlight areas of passengers' bodies that may then be subject to a pat-down.

For these reasons, an adequate regulatory impact analysis would not only identify measures the agency has taken to mitigate privacy concerns, but would also identify remaining privacy impacts on passengers, estimate the total privacy impact, and weigh this impact alongside the other costs and benefits of the proposed regulatory action. Other agencies routinely include privacy impacts on the public in their analysis of regulatory costs, and it is unacceptable for the agency not to do so in the case of a program impacting millions of members of the traveling public.

TSA Should Adopt Regulatory Alternative #3 or Consider Additional Regulatory Alternatives that Reduce Reliance on Body Scanners and Prison-Style Pat-Downs

We strongly urge the Department to adopt proposed regulatory alternative #3 as described in the NPRM (walk-through metal detectors supplemented with explosive trace detection), or alternatively, to consider additional regulatory alternatives that reduce reliance on body scanners as a primary method of checkpoint screening. Because of the intrusive, time-consuming, costly and controversial nature of body scanners, as well as persistent questions about their ability to detect the most significant threats and to avoid false positives, body scanners are not appropriate for use as a primary method of checkpoint screening.

We note that while the NPRM oddly describes the proposed regulatory alternatives in all-or-nothing terms, TSA's historical practice has been to use a mix of screening methods providing a layered approach and a certain amount of variability. Accordingly, we expect that TSA's actual regulatory alternatives actually include using both body scanners and pat-downs on a more limited basis to supplement the use of metal detectors and explosive trace detection. Curiously, the NPRM completely ignores the possibility of redeploying already-purchased scanner devices on a more limited basis, such as for random or secondary screening. Given the intrusive, time-consuming, and controversial nature of

---

[6] IRIA at 110, 119.

[7] U.S. Congressional Research Service. Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening (7-5700; September 12, 2012), by Bart Elias.

[8] See DHS v. EPIC, 653 F.3d 1, 10 (D.C. Cir. 2011) (pat-down alternative "allows [the traveler] to decide which of the two options … is *least* invasive" (emphasis added)).

body scanners, they would be more appropriate for these more limited uses than as a primary screening method.

The Final Rule Must, at a Bare Minimum, Codify Existing Passenger Protections

Despite the significant privacy implications noted by the Court of Appeals, the proposed rule does not incorporate *any* limitation on the use of body scanners or pat-downs – not even the minimal requirements already incorporated in TSA policy and practice or mandated by Congress. If TSA ultimately chooses to maintain use of the body scanners, the final rule must, at a bare minimum, incorporate these existing protections. Because public trust is fundamental to the viability of airport screening, these protections must be codified in regulation as opposed to less formal operating procedures that are less transparent and more readily modified. These include at least the following:

1. Automated target recognition mandate; No human viewing of individual passenger images
2. No retention of individual passenger image data
3. Clear notice of passengers' choices
4. Physical searches to be conducted by officers of the same self-identified gender
5. Secondary screening to be conducted in private and with chosen witness at passenger's election
6. No passenger required to expose sensitive areas under clothing to reveal prostheses, medical devices, or other items
7. Physical searches to resolve an anomaly detected by scanning to be no more intrusive then necessary to resolve the anomaly
8. Training for TSOs to include working with diverse traveler populations
9. Nondiscrimination on the basis of race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, parental status, or gender identity

1. Automated Target Recognition Mandate

Congress has mandated that all body scanners employ ATR software, and it would be irrational for the final rule to authorize the use of scanners without this fundamental requirement. If they are to be used, the final rule must define scanners not only as technology that allows screening without physical contact, but also as technology that allows screening without human viewing of individuals passenger images.

2. No Retention of Individual Passenger Image Data

TSA has stated that, with the use of ATR, individual passenger image data is neither viewed nor retained. The assurance that such data are not retained was central to the reasoning of the Court of Appeals in *EPIC v. DHS.*[9] Nevertheless, many passengers reasonably fear that their individual body image could be retained and viewed at a later time. If ATR is to be used, the final rule should define scanners as technology that allows screening without subsequent retention of individual passenger image data.

3. Clear Notice of Passengers' Choices

As previously stated, provision of prison-style pat-downs as an alternative to body scanners is grossly inadequate because most travelers experience these pat-downs as *even more invasive* than scanners. The proposed rule omits even this inadequate requirement.

[9] 653 F.3d 1, 4, 10.

Passengers must be provided clear notice of the choices they are given by TSA. TSA's current practice of providing this information in small print on an 11" x 14" poster, in a crowded checkpoint area where passengers are rushed to load their belongings into bins, is far from adequate to gain the informed consent needed to make this choice meaningful. The "high level of acceptance" of the scanners cited in the NPRM is rather evidence of the inadequate notice of alternatives currently provided. As the Court of Appeals noted, "Many passengers . . . remain unaware of this right [to opt out].[10] The final rule must require that information about passengers' screening choices be prominently posted, in plain language and in large type, at all checkpoints.

4. Physical Searches Conducted by Officers of Same Self-Identified Gender

The current use of body scanners is inseparable from the use of thorough physical pat-downs as an alternative as well as secondary screening measure. TSA's deployment of scanners cannot work without the use of pat-downs as a secondary method, and TSA's justification for use of scanners hinges on the use of pat-downs as an alternative. The inextricable link between these two, tandem checkpoint screening methods is underscored by the panel opinion of the Court of Appeals, which emphasized the importance of the pat-down alternative in mitigating the personal intrusion caused by the scanners.[11]

Accordingly, if TSA is to codify use of scanners it must also codify basic protections for the use of pat-downs. Among the most basic, minimal protections is TSA's long-standing requirement that, absent exigent circumstances, all pat-down searches be conducted by officers of the same self-identified gender as the traveler (rather than the gender listed on identification or the gender an officer assumes the traveler was assigned at birth).

5. Physical Searches Conducted in Private and with Chosen Witness at Passenger's Election

Also among the minimal protections long provided by TSA is that physical searches and other secondary screening be, at the passenger's election, conducted in a private location and with a witness of the passenger's choosing. This is also a basic expectation of passengers that must be reflected in the final rule.

6. No passenger required to expose sensitive areas under clothing to reveal prostheses, medical devices, or other items

Another key protection currently established in agency policy, which must appear in any final rule authorizing body scanners, is a minimal zone of privacy protection or travelers with personal medical devices or prostheses or other items under clothing that must be identified during screening. This includes not requiring passengers to lift or remove clothing in sensitive areas to reveal a prosthetic or medical device or any other item, and instead allowing travelers, when necessary, to conduct a self pat-down of the item, followed by an explosive trace detection sampling of the hands. In the context of the routine, invasive pat-downs on which the current screening approach depends, not to codify this minimal limitation would be shocking. If TSA is to authorize the use of intrusive routine pat-downs and body scanners, this fundamental protection must be included in any final rule.

---

[10] *Id.* at 3.
[11] *Id.* at 3, 10.

7. *Physical searches to resolve an anomaly detected by scanning to be no more intrusive then necessary to resolve the anomaly*

In addition, current TSA policy provides for "resolution" pat-downs to be limited in appropriate cases to only those areas of the body where an anomaly was detected by a body scan. If a body scan has identified an anomaly only in the area of a passenger's head or arm, for example, it is simple common sense that further screening limited only to that area will be sufficient in most cases to resolve the anomaly. If no threat object is identified in area highlighted by the scanner, any further physical screening is an unnecessary invasion of privacy and a waste of time. Any final rule that authorizes body scanners must codify a requirement that "resolution" pat-downs be limited to the area of an anomaly wherever possible.

8. *Comprehensive Training for TSOs including Working with Diverse Passenger Populations*

TSA has publicly committed to substantially expanding training for TSOs, including training on working with diverse passenger populations, many of which are disparately or uniquely impacted by aspects of TSA's current screening techniques – such as transgender and gender non-conforming people, people with disabilities, religious minorities, older travelers, and families with children. Robust training on these topics is essential to public trust in the screening process, and should be explicitly required by any final rule.

9. *Traveler Civil Rights Policy: Nondiscrimination on the basis of race, color, national origin, sex, religion, age, disability, genetic information, sexual orientation, parental status, or gender identity*

TSA's Traveler Civil Rights Policy should also be codified in any final rule, and should be expanded to include nondiscrimination on the basis of gender identity. This will increase public trust.

The Final Rule Must Use Clearly Defined Terms

In addition to completely lacking passenger protections, the proposed rule uses vague, confusing terms that fail to adequately define the agency's authority for the use of body scanning technology, or to give sufficient notice to the public of the technologies' purpose or impact on travelers.

Most notably, the proposed rule authorizes the use of "screening technology used to detect concealed anomalies" without providing any definition or context for the vague term "anomalies." As commonly defined, an anomaly is "something different, abnormal, peculiar, or not easily classified."[12] This extremely broad and amorphous term could potentially incorporate not only foreign objects that could be put to a potentially dangerous use an aviation environment, but absolutely any item, garment, or even features of the traveler's own body that are deemed to be unusual in any way. The use of this vague, undefined term fails to establish appropriate objectives and limits for security screening and invites abuse. Checkpoint screening should be expressly limited to the detection of prohibited foreign items that pose special risks of creating physical danger in the aviation environment. TSA has been unable or unwilling to publicly confirm whether current ATR software may or may not misidentify atypical bodily characteristics as anomalies. Codifying the limits of screening objectives in this way is essential to public trust.

---

[12] *Merriam-Webster's Dictionary,* http://www.merriam-webster.com/dictionary/anomaly.

Conclusion

We recognize the difficult job that TSA faces in protecting the nation's transportation systems and, most importantly, its travelers. We strongly believe that TSA can fulfill its security mission while respecting the rights and dignity of all passengers, and we look forward to continued dialogue and collaboration with your agency.

If you have any questions about our recommendations, please email me at ehecht@familyequality.org or contact me by phone at 202-496-1285.

Thank you,

Emily Hecht-McGowan

Emily Hecht-McGowan
Director of Public Policy
Family Equality Council

NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication) (Document ID TSA-2013-0004-0001)

The TSA should not be allowed to amend their regulations to allow body scanners as to be used as primary screening. Nor should they be allowed to use "pat downs" as currently defined, as a screening alternative for those who prefer not to go through the body scanners.

1. Both screening methods violate our privacy. Right now the choice is to be electronically strip-searched or go through a "pat down" that is so thorough that it borders on sexual assault. Often times pat downs are performed in a retaliatory manner because the passenger has chosen to 'opt out' of being screened by a body scanner. It's one thing for the TSA to prefer that passengers go through a body scanner, and quite another for them to heap abuse upon passengers who opt out of that screening method.

2. Body scanners waste an incredible amount of time, and don't guarantee that a person won't be patted down. An article came out on June 14th noting that over 150 people have missed flights at SeaTac airport due to "summer travel", but also notes that TSA was informed of increased loads and did nothing about it. http://seattletimes.com/html/travel/2021188818_seatacdelaysxml.html As someone who uses that airport, what I've seen is that it is the body scanners that increase wait times. As soon as metal detectors open up, the backlog all but disappears. The need to resolve the high number of false-positive anomalies can also increase wait times, and pat downs.

Additionally, and not specifically called out in the rulemaking, is the cost of people who have decided to quit flying altogether because of the screening procedures currently in place. For myself, I used to fly almost once per week, now I only fly when I absolutely must. I drive the rest of the time, even if the drive is more than 14 hours long.

3. Passengers are at increased risk of theft of their belongings because of the scanning procedures. Theft is a huge problem. Countless news articles have appeared detailing the loss of items, particularly iPads at security checkpoints. The thefts often occur as people are in the scanners and unable to see their belongings. And unfortunately, TSA agents stealing from passengers account for too many of the theft incidents. TSA Newsblog has a master list of incidents that have occurred at checkpoints. The link to the master list is here: http://tsanewsblog.com/master-list-of-tsa-abuses-and-crimes/ .

4. Dignity of passengers is compromised. Many, many news articles have appeared where passengers have been forced to remove prosthetics, been forced to try to stand when they are unable, have had a delicate medical apparatus destroyed, and have ended up covered in their own urine due to body scanners and/or a pat down. This should never, never happen at a checkpoint.

For the above reasons body scanners and pat downs should not be allowed as primary screening. We should go back to screening via metal detectors only. Swabbing a passenger's hands for explosives in conjunction with the metal detectors should also be explored as a possible screening method.

Confession #1: All the Airport's a Security Stage.

Posted on October 25, 2012 by takingsenseaway

I would have been terminated once they'd found out about this site.
As soon as they'd tracked down my identity, the wheels of the TSA bureaucracy would have groaned into motion in order to eject the outspoken employee in their midst. I would have been walked out by a TSA suit with a smug look on his face as he solemnly demanded I turn over my badge
So it's a good thing I recently resigned.
I don't intend to remain anonymous for too long, anyway, so I'm sure I'll be blackballed from DHS employment for life, which is fine with me. TSA's annually-required reading of the Employee Rules of Conduct makes it clear that it is forbidden for TSA employees to bring shame or embarrassment upon the Transportation Security Administration. But, honestly? What embarrassment could anyone bring upon them that they haven't already brought upon themselves. I assure you, the most controversial things on this blog will invariably be matters of public concern.
This month marks the beginning of federal fiscal year 2013, which will include another 8 billion dollar allocation of tax payer money to the Transportation Security Administration in their mission to keep America safe from the "existential threat of terrorism." Having been employed by the Transportation Security Administration for seven years, working passenger screening at a fairly large airport on the East Coast, I feel I am in a good position to comment upon matters concerning the TSA's use of taxpayers' money. I have absolutely no personal grudge against the TSA. I resigned on good terms with the agency in order to pursue a new career. It's just that, as any officer on the checkpoint will tell you, and as several officers at our Logan International recently expressed to the tune of the front page of the New York Times , there are a lot of absurd and, occasionally, egregious things going on at the TSA at any given time.
The full body scanners, the racial profiling by TSA officers at Logan International, and stories of criminal behavior among bad apple TSA employees have been all the talk lately. I will come to the behavior detection program soon, and the bad apple employees in another post, but for now, having operated the full body scanners for 3 years, I can vouch for the ineffectiveness of the full body scanners— the backscatter iterations, especially.
Recently, a blogger named Jonathan Corbett released a video proving that anyone can easily bypass the billion dollar full body scanner technology, filming himself repeatedly passing through the scanners with a medium-sized metal object; the equivalent, for all intents and purposes, of a gun. He provided proof to the public that the machines can easily be rendered useless by exploiting a laughable weakness in the technology. The video went viral, and the TSA downplayed the video's significance.
But I believe it is of public concern , especially to those party to the federal lawsuits pending against the full body imagers (Ralph Nader, the Electronic Privacy Information Center, Bruce Schneier et al, all of whom– along with the American Civil Liberties Union– have been informed of this blog's existence as well as of my true identity), and to the taxpayers who both fund the purchase of these machines while simultaneously being compelled to submit to their use, that both Corbett and EPIC's claims are absolutely correct, despite the TSA's assertion otherwise.
The backscatter radiation machines are not only ineffective and of questionable security value, they are absolutely useless, and represent an unnecessary impingement upon people's privacy.
Furthermore, the TSA clumsily attempted to cover up the critical flaw in its scanners with a panicked internal directive to frontline TSA officers within a week of the release of the Corbett video, instructing all officers to begin randomly patting down the sides of passengers, essentially making the machines no more than million dollar random pat-down generators– ones that emit radiation and capture nude images of passengers– a procedural redundancy, since random pat-downs are already performed on passengers.
This billion dollar comedy of errors would perhaps not be so bad if it weren't for the fact that, again, in addition to the TSA's reckless foisting of this ineffective technology on the public, the technology exposes millions of flyers (which, for the first year of its roll out, included toddlers) to completely unnecessary doses of radiation. Low-level doses? Yes, assuming that the scanners are functioning properly. But as usual with the TSA, the question concerns the big picture in all of this, not myopic technicalities such as Rapiscan's specs concerning the theoretical properly-functioning nude scanner. The real question is whether or not it even made any sense at all to subject travelers to this theoretically small, yet unnecessary dose of radiation, to begin with.

It didn't.

The backscatter units do not work (possibly one reason why Europe recently banned them), and that there are still hundreds of them operating in American airports is absurd. As to the "harmless dose of radiation" that the TSA always speaks so reassuringly of (which is true, assuming that any given machine is functioning according to the manufacturers' specifications) I believe it is important for the public to know that the number of TSA employees who themselves feel extremely uncomfortable working around these machines due to concerns about the radiation is substantial. I am confident that a discreet, nationwide survey given to the frontline TSA officers who operate the backscatter machines would confirm this.

The lesson here is not that the TSA should replace all backscatter machines with millimeter wave units; the TSA is already doing this, rushing to sweep another reckless, costly, embarrassing decision under the rug. The real take away here is that all of this represents business as usual for the Transportation Security Administration, and that it would probably be a good idea for lawmakers and their constituents to take a good hard look at TSA's decision making processes.

In addition to all this, in my years at the agency I witnessed TSA management at local levels routinely becoming lax in their enforcement of the agency's original promise to the public that officers would never come face-to-face with the passenger whose nude image they viewed. They did this in order to decrease the enormous wait times produced by the ineffective machines themselves, often urging– under threat of disciplinary measures– the speeding up of checkpoint floor rotations. In many cases (such as where, for instance, the past 5 images were male, with only 1 female) this makes it easy for officers to match a passenger with the nude image they just viewed, completely validating just one of EPIC's privacy concerns. FOIA requests for the checkpoint footage of the average large, highly trafficked airport where the backscatter machines were or are installed could substantiate this. I have a few ideas as to specific sections of footage, which will soon be passed along to EPIC. All of this information, taken together, serves to confirm EPIC's general concern that the full body scanner program is "unlawful, invasive, and ineffective."

The obvious question is this: since the full body scanners– both backscatter as well as MMW iterations– essentially amount to little more than just random pat down generators, why not cut the costly, much-maligned "middle man" machines out of the picture as primary screening methods altogether, and just continue with the existing random pat downs, which are already performed both officially and *de facto?*

The answer is that it would be an acknowledgement of poor decision making by the TSA, as well as a concession of proposed budgetary needs. It is characteristic of a large bureaucratic organization such as the TSA to attempt to exert and consolidate its power, inflate its necessity and needs insofar as possible (Wilson, James Q. "Bureaucracy") so as to justify large budgets, private contracts, and extraneous, yet well-paying upper level management positions in this "top heavy" organization, as the Government Accountability Office's May 9 report on the TSA deemed it, "an unmanageable agency, evidenced by its 400% increase in workforce since its founding, an agency's flaws that are not the fault of TSA employees working everyday on the front lines, but instead that of a bloated leadership structure in Washington, DC. Our investigations of TSA have been met with obfuscation, excuses and attempts to mislead".

"We have many layers protecting the nation from the ever-evolving terrorist threat."

That is the refrain that TSA launches into in the face of most criticism: an incessant drone concerning layers; 20 layers in all. The TSA's go-to sleight-of-hand rhetoric of critically-important, billion dollar security layers amounts to little more than a distraction from the big picture; the big picture revealing the truth of a world where terrorism is so rare and unpredictable as to make most of the taxpayers' money the TSA spends better spent elsewhere. As security expert Bruce Schneier has often sharply observed, "once a terrorist gets to an airport, it is already too late"

The question is not whether this or that layer of security performs a function. The question is whether the function— be it behavior detection or full body scanners— makes any sense at all in the big picture, and whether or not the money spent on the TSA's lavishly-funded winter wardrobe of layers is really doing anything beyond making for a good fashion show.

It is also a good time to remind you, dear American public, that you have essentially paid more than 1 billion dollars over the past 4 years, and will likely pay somewhere near a quarter of a billion dollars more in 2013, for a group of self-proclaimed truth wizards to patrol your airports, playing the role of airport terror busters. I am not using the term "truth wizards" arbitrarily, or purely derisively. Not enough people realize that the man behind the theory of the BDO program as it is taught (in conjunction with Israel's airport security model) Paul Ekman, deemed his science capable of bringing out the "truth wizard" in all of us. This "science" was bought, wholesale, by your federal government (Ekman's research having itself been widely criticized by the scientific community, see "On Lie Detection Wizards," Bond and Usayl, 2007.)

People call the TSA "Thousands Standing Around." Within TSA culture, I can tell you that the BDOs have a place further derision. After an "intensive" 2 weeks of training in a program that has been roundly questioned to possess any scientific merit by leading publications, often fresh out of high school and 2 weeks of airport security training, a BDO is unleashed upon the world as a federal airport human lie detection machine.

One of the most prestigious scientific publications in the world, *Nature*, found the program's value to be spurious. In 2008 the National Research Council of the National Academy of Sciences deemed the program's underlying theory as "preliminary, at best." The Government Accountability Office, in 2011, suggested that the TSA should have determined the scientific validity of the SPOT program before implementation (the same conclusion which was reached with the full body scanners).

A 2011 congressional report that same year correctly deemed the BDO program "one of TSA's biggest failures." The entire BDO program is, in fact, probably "no more accurate at detecting a terrorist than a flip of a coin."(Hontz, C. R., Hartwig, M., Kleinman, S. M. & Meissner, C. A. Credibility Assessment at Portals, Portals Committee Report, 2009.) Link

And now, just a few months ago, it was found that— surprise—BDOs at Logan International Airport were profiling in order to meet imposed quotas and produce numbers to ostensibly justify their program's existence to tax payers.

Larger airports even devote the BDOs to full time "walking the line," freeing them of any other work, so that they are essentially strolling around for 8 hours every day at 20 dollars an hour, trying to detect microexpressions in terrorists who aren't there, or completely missing the ones who, ever so rarely, do pass through (Hearing Before the Subcommittee of Investigations and Oversight, 2011).

If anything, the SPOT program could possibly make sense with highly trained officers operating in a single, small, high-stakes, politically-unique setting such as Israel's Ben Gurion International. In a crowded American airport, this already-shaky science becomes absolutely useless. One where, for instance, Federal officers are discovered to be using racial profiling in order to get numbers, or where at "least 16 least individuals later accused of involvement in terrorist plots flew 23 different times through U.S. airports since 2004, yet none were stopped by TSA behavior detection officers working at those airports."

One of these terrorists was Faisal Shahzad, the attempted Times Square bomber of 2010, whose attempted destructive handy work was detected and heroically brought to real law enforcement's attention by a street vendor, Aliou Niasse, a Muslim.

Let's all just be glad that Niasse was not being detained and "chatted down" by a racially-profiling BDO at Logan or Newark at the time.

The solution to all these inherently flawed systems of TSA's is not retraining or ad hoc quick fixes. The solution is to cut loose the unnecessary, ineffective, unpopular, wasteful and intrusive measures, and to address the fact that the problem is systemic, lying within the TSA's culture and modus operandi. The fundamental problem with this organization and its mission to become an advanced counter-terrorism organization is precisely *that* it needs to stop trying to be an advanced counter-terrorism organization.

Again: once a determined and lethal terrorist gets to an airport, it is already too late. We need to repeat and accept this, as taxpayers, media entities, and society as a whole: a group of airport cops is not going to be the ones to foil or deter a determined terrorist.

The terrorists on 9/11 could have pulled off what they did with the same security we have today on the checkpoint. This whole subconscious culture of the TSA's— caught in a perpetual, quixotic quest to retroactively prevent 9/11— needs to stop (and D.C., if you are reading, please, enough with the 9/11 propaganda in your officer training videos, please).

All of this, dear readers, seems just as ridiculous to the thinking TSA employee as it seems to the public, I assure you. Work life as a Transportation Security Administration officer is bizarre and surreal, where a federal officer is as likely as not to be heard bragging about her skill as a "wizard"; where officers have historically been compelled, per federal standard operating procedure, to inform the pilot of an airplane, with a straight face, that his Swiss army knife must be confiscated, under the logic that he may use it to hijack his own plane.

As anyone working for TSA will likely attest (in private, at least), working for the TSA has the feel of riding atop the back of a large, dopey dog fanatically chasing its tail clockwise for a while, then counterclockwise, and back again, *ad infinitum*.

Before the
TRANSPORTATION SECURITY ADMINISTRATION
DEPARTMENT OF HOMELAND SECURITY
Washington, DC 20590

Notice of Proposed Rulemaking: Passenger Screening Using Advanced Imaging Technology	)	TSA-2013-0004 (RIN 1652-AA67)
	)	Comments of Jim Harper, John Mueller, and Mark Stewart of the Cato Institute

Table of Contents

I. Introduction and summary

Submitting these comments in response to the Notice of Proposed (NPRM), "Passenger Screening Using Advanced Imaging Technology,"[1] are Jim Harper, John Mueller, and Mark Stewart of the Cato Institute.

The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets and peace. Its scholars and analysts conduct independent, nonpartisan research on a wide range of policy issues. Founded in 1977, Cato owes its name to Cato's Letters, a series of essays published in 18th-century England that presented a vision of society free from excessive government power.

[1] 78 Fed. Reg. 18287-18302 (Mar. 26, 2013), docket number TSA-2013-0004, RIN 1652-AA67.

Jim Harper is director of information policy studies at the Cato Institute, in which role he works to adapt law and policy to the unique problems of the information age. He deals with areas such as privacy, telecommunications, intellectual property, and security. Harper was a founding member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and he recently co-edited the book *Terrorizing Ourselves: How U.S. Counterterrorism Policy Is Failing and How to Fix It*.

John Mueller is a senior fellow at the Cato Institute. He is also a member of the political science department and Senior Research Scientist with the Mershon Center for International Security Studies at Ohio State University. He is a leading expert on terrorism and particularly on the reactions (or over-reactions) it often inspires. His most recent book on the subject, *Terror, Security and Money: Balancing the Risks, Benefits and Costs of Homeland Security* (co-authored with Mark Stewart) was published in September 2011 by Oxford University Press. Other books on the subject include *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (Free Press, 2006) and *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (Oxford, 2010).

Mark G. Stewart, recently a visiting fellow at the Cato Institute, is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He is also currently an Australian Research Council Professorial Fellow. He is the author, with R.E. Melchers, of Probabilistic Risk Assessment of Engineering Systems (Chapman & Hall, 1997), as well as more than 300 technical papers and reports. He has more than 25 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems that are subject to man-made and natural hazards.

The euphemism "Advanced Imaging Technology" fails to describe the technology at issue in the instant rulemaking. It would be more accurate to call them "nude body scanners." The machines look under the clothes of travelers, as a traditional strip-search does, without actually stripping the person. Obscuring language like "AIT" is just one dimension of the indifference to privacy shown in the preamble and the proposed rule, which does not account for the privacy concerns that prompted the court to order this rulemaking.

As to the substance of the rulemaking, the proposed rule fails fully to articulate the TSA's policies, existing or proposed, with respect to the use of body scanners at the nation's airports. It thus fails to fulfill the order of the D.C. Circuit Court of Appeals in *EPIC v. TSA*.

Secret classification of the agency's "risk-reduction analysis" is not warranted by law or policy, and it fatally undercuts the requirements in administrative law and related executive orders that require the agency to perform and publish various analyses. Risk management and cost-benefit analysis can easily be conducted without revealing technical details or threat information that may legitimately be kept confidential. The agency must conduct risk management and cost-benefit analyses of its policies so that its policies can be examined for rationality and sufficiency under the law.

Independent, scholarly, and unchallenged risk management and cost-benefit analyses of the use of body scanners in U.S. airports have been made. They find that the machines fail overwhelmingly to reduce risk enough to justify their costs—even assuming they work effectively. Among the costs produced by TSA policies is this area is disinclination to travel by air, which is quite safe relative to automobile travel. Thus, TSA policies may result in increased mortality among travelers.

Having taken twenty months to issue a deficient proposed rule and utterly lacking analysis, the TSA has abused the rulemaking process to the detriment of the public, some of whom may needlessly be killed due to current TSA policy. The only appropriate remedy is for TSA to suspend its body scanning policy and commence a new rulemaking, adopting whatever policy emerges from that rulemaking. Otherwise, some Americans may die awaiting the resolution of this rulemaking, the appeals that follow it, and the new rulemaking that those appeals will inevitably produce.

II. The NPRM and proposed rule fail to account for privacy

Though the TSA is obliged to produce privacy impact assessments under the E-Government Act of 2002, and though the Department of Homeland Security has had a privacy advisory committee since 2005, the NPRM does not exhibit an understanding of privacy. It uses language that obscures the privacy interests of travelers, and betrays no recognition that privacy is lost to the TSA's policies.

In this comment, we decline, as noted earlier, to adopt the obscuring euphemism "advanced imaging technology" or "AIT" because it inappropriately draws attention away from the interest that sparked the *EPIC v. TSA* lawsuit and this court-ordered rulemaking. Instead, we will use a term we believe to be accurately descriptive: nude body scanner. This terminology acknowledges the privacy interests of travelers, to which we now turn.

a. The NPRM does not exhibit an understanding of privacy

Privacy's legal roots go back as far as 1890 and the publication by Samuel D. Warren and Louis D. Brandeis of "The Right to Privacy" in the Harvard Law Review.[2] Since the late 1960s, scholars, advocates, and government agencies have been grappling articulately with privacy and its protection. The late 1960s and early 1970s were an era of privacy foment not unlike today, with books written on the subject and state constitutions amended to protect privacy explicitly. In 1967, the year that the Supreme Court decided

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

Katz v. United States,[3] scholar Alan Westin characterized privacy in his seminal book as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[4]

This is the strongest sense of the word "privacy": the enjoyment of control over personal information. A tighter, more legalistic definition of privacy is: "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[5] Given control over information about themselves, people will define and protect their privacy as they see fit.

Among other techniques, such as contractual agreements, people control information about themselves by arranging physical things with reference to themselves and by changing their behavior. Retreating into one's home and drawing the blinds, for example, causes what happens inside to be "private." Lowering one's voice to a level others cannot hear make a conversation "private." Draping the body with clothing makes the details of its shapes, textures, and colors "private." These arrangements and behaviors literally prevent others from perceiving things, maintaining the privacy of those things. Body scanners defeat this privacy protection for everyone passing through them.

b. Body scans undercut privacy

So-called "Advanced Imaging Technology" examines what is underneath the clothes of travelers. It does this using machines rather than human vision, but it is no less a scan of the body. The scanners evade rather than remove the coverings of the body.

Millimeter wave technology directs radio waves through the clothes and captures their reflection. Recording the reflected radio waves that have passed through clothing allows software to produce a visual image of the naked body similar to what reflected photons would produce. The court in *EPIC v. TSA* characterized the situation this way: "Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon his or her personal privacy in a way a magnetometer does not."[6] It is the functional equivalent of recording photon patterns that have reflected off a nude body. This defeats the privacy-protecting function of clothing and allows an image of the unclothed person to be created.

It is true that, along some dimensions, the use of millimeter wave scanning to produce an image of the nude body offers greater privacy protection than an actual, physical strip-search. For example, in millimeter wave, the object of the search does not

---

[3] 389 U.S. 347 (1967).
[4] Alan Westin, Privacy and Freedom 7 (1967).
[5] See Jim Harper, Understanding Privacy—and the Real Threats to It, Cato Institute, Policy Analysis No. 520 (2004).
[6] U.S. Ct. App. D.C. Cir. No. 10-1157, slip op. at 8 [hereinafter "EPIC v. TSA"].

experience the physical sensation of having her clothes removed and her body exposed to the cool surrounding air. This reduces the sense of mortification most travelers would experience if undergoing a physical strip-search. If recent modifications to body scanning software are reliable, no human sees an image of the nude body. The knowledge that a human has seen one's body contrary to one's wishes is a common, strongly held privacy concern.

Along other dimensions, though, nude body scans are worse for privacy than a physical strip-search because they produce a *digital* image of the unclothed body. This is an image that computers can store indefinitely, transfer around the globe in seconds, and copy an infinite number of times without the copies degrading. The scanners take the control travelers have exercised over the appearance of their bodies by putting on clothes—their privacy—and makes it contingent on the TSA maintaining body scanners and their software as advertised. If the TSA does not enforce its policies—a prospect that is within the realm of possibility given hundreds of machines around the country and the possibility of official dereliction—travelers may learn that nude digital images of themselves flow across the Internet.

So, where a physical strip-search produces the sensation of bodily exposure and the embarrassment of having one or two other people (typically) view areas of the body that one intended to keep private, body scanners reduce the perception of bodily exposure, but replace it with the risk of massive online exposure of one's nude image worldwide. The trade-off is not subject to cold calculation, but it is roughly a wash. Either treatment is a loss for privacy.

Millimeter wave machines are certainly imaging technology, but the anodyne term "advanced" is not justified. It provides no relevant meaning, obscures what the machines do, and leaves their functionality inappropriately nondescript.

People put on clothes in the morning in order to conceal the appearance of their bodies. This is not only for practical purposes—because revealing their bodies can cause embarrassment, for example—but because one has a right over one's body, including a right to control what parts of it one reveals. Indeed, it is a specifically itemized constitutional right, the right to be secure in one's person against unreasonable searches.

c. The NPRM takes body scanners as a given to deny their privacy effects

To read the NPRM, one might think that the proposed rule improves privacy over the status quo ante. It says, "The use of ATR software enhances passenger privacy by eliminating images of individual passengers…" But the policy of subjecting American travelers to either a nude body scan or an intimate pat-down incontrovertibly reduces the privacy of travelers. The proposed rule, such as it is, codifies TSA's discretion to maintain this policy.

The use of "Automated Targeting Recognition" software, which shows on an outline where suspect articles may be found, undoubtedly mitigates the privacy lost to the use of body scanners in the first place. But the NPRM fails to acknowledge or address that original, significant loss to travelers' bodily privacy in the use of nude body scanners at all. This is a basic insufficiency of the NPRM caused in part by failing to apprehend what privacy is.

III. The proposed rule fails to articulate sufficiently clear standards

The proposed rule is insufficient to apprise members of the public of their rights and responsibilities at the airport. It does not articulate, even in a general way, what people can expect at the airport, what they must do at the airport, what they may not do at the airport, or what they can do to appeal any adverse action. Neither does the proposed rule articulate what TSA agents must do, what they may do, what they may not do, or any other dimension of their rights and responsibilities. The vague policy statement, proposed as if it were a rule, flies in the face of the D.C. Circuit Court of Appeals ruling requiring the instant rulemaking. It should be revised to clearly articulate the rights and responsibilities of both travelers and TSA agents with respect to body scanning.

The Administrative Procedure Act (APA) generally requires that a notice of proposed rulemaking be published in the Federal Register, unless the rule fits into one of a few exceptions.[7] In *EPIC v. TSA*, the court rejected arguments that the TSA's policy on the use of strip-search machines fit into one of these exceptions: It was not a "procedural rule," an "interpretive rule," or a "general statement of policy."[8] In order to resolve the deficiencies in its procedure, the court remanded to the TSA "to conduct a notice-and-comment rulemaking."[9] Throughout its opinion, the court relied on the premise that this rulemaking would pertain to a legislative rule: a rule adding to or amending the body of rules that dictate action or conduct.

The APA requires that such a rulemaking show the terms or substance of the proposed rule, or at least a description of the subjects and issues involved.[10] In its opinion requiring notice and comment proceedings, the court repeatedly emphasized the importance of issues surrounding body scanners. The court ordered a rulemaking that reflects the TSA's policies' "'substantial impact' upon the persons subject to it."[11] The court thought few rules "impose [as] directly and significantly upon so many members of the public" as the use of body scanning machines.[12] The court said that "the TSA's use of

[7] 5 USCS § 553(b)(3)(A).
[8] EPIC v. TSA at 7-11.
[9] EPIC v. TSA at 12.
[10] 5 USCS § 553(b)(3).
[11] EPIC v. TSA at 7.
[12] EPIC v. TSA at 9.

AIT for primary screening has the hallmark of a substantive rule…."[13] Finally, the court held that the TSA's policy "substantially changes the experience of airline passengers."[14]

Despite the repeated emphasis the D.C. Circuit Court's opinion puts on the significance of this rulemaking for exploring the TSA's policies and rationale, the court's opinion is more informative about TSA policies than the proposed rule laid out in the NPRM. The decision in *EPIC v. TSA* says, for example:

> No passenger is ever required to submit to an AIT scan. Signs at the security checkpoint notify passengers they may opt instead for a pat down, which the TSA claims is the only effective alternative method of screening passengers. A passenger who does not want to pass through an AIT scanner may ask that the pat down be performed by an officer of the same sex and in private.[15]

This is more informative than the NPRM or proposed rule.

Describing the regulations in place at the time of the decision, now changed in fact if not by the proposed rule, the court wrote:

> Each image produced by a scanner passes through a filter to obscure facial features and is viewable on a computer screen only by an officer sitting in a remote and secure room. As soon as the passenger has been cleared, moreover, the image is deleted; the officer cannot retain the image on his computer, nor is he permitted to bring a cell phone or camera into the secure room.[16]

This is more informative than the NPRM or proposed rule.

The court was able to describe the rules as they affected both travelers and the TSA at the time of its decision. These were the rules it expected the TSA to articulate in the rulemaking it ordered. When an agency statement is of "'present binding effect,'" the court wrote, "then the APA calls for notice and comment."[17] The court called for notice and comment because the TSA was to produce a legislative rule.

The government, too, took as a premise that it would produce a legislative rule. When EPIC filed a motion seeking enforcement of the court's mandate, the government filed a declaration averring the difficulty of producing a regulation in the challenging area of airline security.

---

[13] EPIC v. TSA at 9.
[14] EPIC v. TSA at 10.
[15] EPIC v. TSA at 3-4.
[16] EPIC v. TSA at 4.
[17] EPIC v. TSA at 10-11.

"The rulemaking of the type contemplated by the Opinion requires extensive preparation" declared James Clarkson, Acting General Manager of the Intermodal Security Support Division at TSA, "including in-depth economic analysis, that is generally measured in months."[18] The court of appeals, expecting a legislative rule, evidently accepted the gist of the declaration, as it declined the motion.

This "extensive preparation" did not amount to much. The proposed rule is a thin scrap of language, especially given the twenty months it took to produce. A regulatory agency like the TSA "has an obligation to make its views known to the public in a concrete and focused form so as to make criticism or formulation of alternatives possible."[19] Instead, it provided the public with two vague sentences containing fewer than fifty words:

> (d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.

This language delineates no obligations, either on the part of travelers or the TSA. It provides no notice to the public of what they can expect at the airport. It fails to signal in any way the rules that might pertain to the machines and their use. The language does nothing to bind the agency to a course of conduct or to cabin its exercise of discretion in any way.

Issuing such a general statement of policy a full twenty months after a court order requiring a legislative rule is totally insufficient. The statement hardly provides the "sufficient factual detail and rationale for the rule to permit interested parties to comment meaningfully" that the D.C. Court of Appeals requires.[20] The TSA's proposed rule does not even address most of the issues that the *EPIC* court found substantive enough to require notice and comment rulemaking in the first place. The NPRM is therefore non-responsive to the order of the court, as it fails to meet the basic notice requirements of administrative law and regulatory policy.

As the *EPIC v. TSA* court said, "the purpose of the APA would be disserved if an agency with a broad statutory command (here, to detect weapons) could avoid notice-and-comment rulemaking simply by promulgating a comparably broad regulation (here, requiring passengers to clear a checkpoint) and then invoking its power to interpret that statute and regulation in binding the public to a strict and specific set of obligations."[21] Yet that is what the TSA has done here. The NPRM has the form of notice-and-comment

---

[18] Declaration of James S. Clarkson in Support of Respondents' Opposition to Petitioners' Motion to Enforce the Court's Mandate, ¶ 4 (filed Nov. 10, 2011).
[19] Home Box Office, Inc. v. FCC, 567 F.2d 9, 36 (D.C. Cir. 1977).
[20] Florida Power & Light Co. v. United States, 846 F.2d 765, 771 (D.C. Cir. 1988).
[21] EPIC v. TSA at 10.

rulemaking, but it is just as broad as the agency's statutory command, preserving for later the specific set of obligations to which the public will be subjected. The APA does not require the TSA to provide precise notice of every aspect of the regulation, but in order for notice to be sufficient it must at the very least offer a rule that is "sufficiently descriptive of the subjects and issues involved so that interested parties may offer informed criticism and comments."[22] The NPRM flies in the face of the court's ruling and the direct language of the court rejecting overly broad regulatory language.

Given the purposes of APA rulemaking, adding requisite detail to the final rule would be insufficient. "[N]otice is inadequate if the interested parties could not reasonably have anticipated the final rulemaking from the draft rule."[23] The NPRM as it exists now gives no means of anticipating any aspect of the body scanning policy, other than an ambivalent statement that body scans might be used. Without a more descriptive rule, criticism of, and comment on, the TSA's body scanning machine is impossible, making the notice-and-comment process purposeless and defeating the court's order.

As we discuss at the end of this comment, the appropriate remedy, given the threat to human life produced by current policy, is to suspend the use of the body scanning machines for primary screening and commence a new rulemaking aimed at discovering the policy that most effectively secures the nation's travelers. The new rulemaking should be on the record and it should not use vagueness to insulate TSA policy from public review.

IV. Unjustified secret classification of the "risk-reduction analysis" undercuts the rulemaking

Classification of the "risk-reduction analysis" noted in the NPRM deprives the public of the benefits that notice-and-comment rulemaking is intended to provide, it deprives the agency of information and data that could improve the rule, and its likely result is more American highway deaths because of a poorly tuned rule. If the TSA cannot declassify the results of the risk-reduction analysis entirely, it should declassify the bulk of the analysis itself, redacting only specific threat and vulnerability information, and, if it issues a new proposed rule as called for below, it should create a new analysis of that rule, leaving it declassified in its entirety.

The NPRM claims the existence of a "risk-reduction analysis" that validates the proposed rule, such as it is. But the NPRM says that "the results of TSA's risk-reduction analysis are classified."

There is no possible way that the *results* of a risk-reduction analysis could possibly justify classification. It is possible that some parts of an entire risk-reduction

[22] Ethyl Corp. v. EPA, 541 F.2d 1, 48 (D.C. Cir. 1976) (quotation marks omitted).
[23] Am. Iron & Steel Inst. v. OSHA, 182 F.3d 1261, 1276 (11th Cir. 1999) (quotation marks omitted).

analysis could be subject to classification, but inappropriate use of classification authority that undercuts notice-and-comment rulemaking.

To arrive at these conclusions, we begin with a précis on risk management.

a. An understanding of risk management is essential

Risk management is the identification, assessment, and prioritization of risks[24] followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events. Everyone manages risk every day, in nearly every decision, substantial or insubstantial. But with the growth of large organizations and complex processes, risk management is a distinct planning and organizing tool. When a lot is on the line, it is worth taking time to manage risks articulately. And a lot is on the line with passenger air travel.

A formal risk management effort will generally begin with an examination of the thing or process being protected. This is often called "asset characterization."[25] Studying whatever infrastructure, business, or process one wants to protect will reveal what particular things are important about it, what weaknesses it might have, what things might threaten it, what would happen if it was damaged or destroyed, and so on. Asset characterization is the survey that begins the risk management process.

The next step in risk management is to identify and assess risks, often called "risk characterization" or "risk assessment." There are a few key concepts that go into it:

- *Vulnerability* is weakness or exposure that could prevent an objective from being reached. Vulnerabilities are common, and having a vulnerability does not damn an enterprise. The importance of vulnerabilities depend on other factors.

- *Threat* is some kind of actor or entity that might prevent an objective from being reached. When the threat is a conscious actor, we say that it "exploits" a vulnerability. When the threat is some environmental or physical force, it is often called a "hazard." As with vulnerability, the existence of a threat is not significant in and of itself. A threat's importance and contribution to risk turns on a number of factors.

With vulnerabilities and threats in hand, risk managers then make rough calculations about likelihood and consequence:

[24] Risk is defined in ISO 31000 as "the effect of uncertainty on objectives," whether positive or negative. *See* Wikipedia, "Risk Management" page, visited July 13, 2010, http://en.wikipedia.org/wiki/Risk_Management

[25] *See* Thomas L. Norman, Risk Analysis and Security Countermeasure Selection (Boca Raton: CRC Press, 2010), pp. 85-99.

- *Likelihood* is the chance that a vulnerability left open to a threat will materialize as an unwanted event or development that frustrates the objective. Knowing the likelihood that a threat will materialize is part of what allows risk managers to apportion their responses.

- *Consequence* is the significance of the loss or the impediment to objectives that would result should the threat materialize. Consequences can range from very low to very high. As with likelihood, gauging consequence allows risk managers to focus on the most significant risks.

Though these factors are often difficult to measure, a simple formula guides risk assessment:

Likelihood x Consequence = Risk

The matrix in Figure 1 illustrates which risks deserve little or no attention (green), which deserve some priority (yellow), which deserve prompt attention (orange), and which deserve immediate attention (red). Obviously, threats that are rare and inconsequential deserve no attention at all. Threats that are common and existential should be addressed first.

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Extreme
Rare	Low	Low	Low	Low	Low
Unlikely	Low	Low	Low	Medium	Medium
Possible	Low	Low	Medium	Medium	Medium
Likely	Low	Medium	Medium	High	High
Almost Certain	Low	Medium	Medium	High	Extreme

Figure 1. Risk Matrix, Combining Likelihood and Consequence

After risk assessment, the next step in risk management is choosing responses.

There are four general ways to respond to risk:

- *Acceptance* – Acceptance of a threat is a rational alternative that is often chosen when the threat has low probability, low consequence, or both.

- *Prevention* – Prevention is the alteration of the target or its circumstances to diminish the likelihood of the bad thing happening.

- *Interdiction* – Interdiction is any confrontation with, or influence exerted on, a threat to eliminate or limit its movement toward causing harm.

- *Mitigation* – Mitigation is preparation so that, in the event of the bad thing happening, its consequences are reduced.

An important consideration when choosing a response is whether or not the response creates new risks to the asset or to others. This is known as "risk transfer." Airport body scans, intended to interdict the smuggling of dangerous articles aboard planes, transfer risk to travelers who, averse to being scanned, choose to drive instead of fly. These travelers suffer injuries and die in greater numbers, as automobile travel is more dangerous than air travel.

The DHS Privacy Committee recommended use of a risk management model like this in 2006. [26] The NPRM exhibits no discernable methodology, and the resulting "rule" is arbitrary as a result.

To reach that conclusion, we had to guess at the agency's thinking. The inappropriate use of classification shields the documents that purportedly justify the rule and existing policy.

b. Classification of the risk management document is unwarranted

Under Executive Order 135256, classification is permitted if "disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism." The order continues: "If there is significant doubt about the need to classify information, it shall not be classified." The need to classify the risk management work underlying the proposed rule is indeed doubtful, and its classification undercuts the purpose of notice-and-comment rulemaking.

Because risk analysis by its nature requires analysts to make assumptions and to work with data that are often far from precise, it is crucial that the full analysis be open and transparent. This allows other analysts to evaluate not only the results, but also the components from which they derive. As a RAND report puts it:

> [B]est practices for analytic products generally, and policy analysis modeling specifically, emphasize the importance of transparency and comprehensibility of the model; clear and candid accounting of its caveats, assumptions, and hypotheses; and a thorough assessment of how uncertainties in the model's logic, underlying theory or input data could affect its

---

[26] *See* Department of Homeland Security, Data Privacy and Integrity Advisory Committee, "Framework for Privacy Analysis of Programs, Technologies, and Applications," Report No. 2006-01 (Mar. 7, 2006) http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf.

findings.[27]

Obviously, risk analyses that have been classified do not conform to this important—indeed vital—characteristic.

There may be justifications for keeping from the public (and, by inference, attackers) details about body scanning—about its mechanical workings, for example, its error rate, or methods by which it might be defeated. However, analysis designed to assess the overall cost-effectiveness of a security measure does not need to delve into such issues. One might simply assume that the measure is technically effective and then seek to determine whether, given that assumption, it is cost-effective. Obviously, if it fails to be so, the measure should not be deployed no matter how technically effective it might be. On the other hand, if analysis conducted under that assumption deems the measure to be cost-effective, further analysis (which might then run into the classification issue) should be done to see if altering the assumption importantly changes the result about the measure's cost-effectiveness.

A second sort of detail that might be kept confidential is threat information that reveals sources and methods by which the information was gathered or that signals to threats that their existence or plans are known. (The latter could deter threats, which would be fine, but if it inspires threats to evade detection or capture, that would be a setback for security.) If a risk analysis reaches a level of detail that could compromise national security in these ways, the solution is simple: Dial back to a level of generality that is not so revealing.

As noted earlier, publishing the *results* of a risk-reduction analysis cannot possibly damage national security. Depending on how it was produced, there may be elements of TSA's "risk-reduction analysis" that merit redaction. But classification of the document as a whole is excessive and it undercuts the rulemaking disproportionately to the negligible risk that its release would create.

Credible and complete risk management analysis of TSA's airport body scanning policy has been done, publicly, by co-authors of this comment Mark G. Stewart of the University of Newcastle, Australia, and John Mueller of Ohio State University. Their analysis was published in 2011 in an important, peer-reviewed journal, *The Journal of*

[27] A. R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System*, pg. 98 RAND Corporation (2012), citing James H. Bigelow and Paul K. Davis, *Implications for Model Validation of Multi-Resolution Multiperspective Modeling (MRMPM) and Exploratory Analysis*, Santa Monica, Calif.: RAND Corporation, MR-1750-AF, 2003; Office of the Director of National Intelligence, Intelligence Community Directive, Number 203, Analytic Standards, Effective June 21, 2007; National Research Council, *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*, Washington, D.C.: National Academies Press, 2008; and National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*, Washington, DC: National Academies Press, 2010 [hereinafter "NRC 2010"].

Homeland Security and Emergency Management, and it was included later in the year in their Oxford University Press book, *Terror, Security, and Money*. No one has ever asked Mueller and Stewart not to discuss their research, and they have been invited to present their findings at national security conferences open to the public.

Their study did not reveal unknown information or break any new analytical ground. Rather, they systematically and transparently applied standard risk-analytic and cost-effective procedures that have been codified and are routinely applied throughout the world when determining the desirability of measures and procedures intended to enhance security and welfare. Neither author of the study has heard objection from any quarter that their analysis exposes information that terrorists or other attackers could exploit.

Stewart and Mueller would, of course, be delighted to bring this experience to bear in evaluating any TSA studies that arrive at different conclusions, but they are prevented from doing so by the fact that such studies have been classified.

Walking through how well policies and technologies produce security can be done without revealing any intelligence about threats, and it can be done without revealing vulnerabilities in the policy and technology. The TSA's use of secrecy is inappropriate, and it should be reversed.

V. Risk management and cost-benefit analysis show that the policy supported by the proposed rule is not cost-effective

Nothing excuses the TSA from performing risk management and cost-benefit analyses that validate the proposed regulation, such as it is, and validate actual TSA practice at airports. Though it says that one exists and is classified, the language of the NPRM suggests either that the risk management and cost-benefit work underlying the proposed rule are invalid, or, as will be discussed more fully below, that the authors of the NPRM do not understand risk management.

Full-fledged, articulate risk management studies show that the policies in place under the proposed rule are not justified. Indeed, by shifting travelers to more dangerous automobiles, the policies currently in place may cause more travelers to die than it saves.

a. Nothing excuses TSA from using risk management and cost-benefit analysis

There is no argument that current policies are dictated by statute. The court said so in *EPIC v. TSA*: "Although the statute, 49 U.S.C. § 44925, does require the TSA to develop and test advanced screening technology, it does not specifically require the TSA to deploy AIT scanners let alone use them for primary screening."[28] The authorities cited

[28] EPIC v. TSA at 10.

in the preamble to the proposed rule do not exempt the TSA from rational cogitation about its policies in the course of the instant rulemaking.

Indeed, listing a variety of possible technologies, 49 U.S.C. § 44925 calls for "*optimal* utilization and deployment of explosive detection equipment…." (emphasis added). None of the hortatory language in appropriations conference reports and other legislative history since then overcomes the statutory requirement of "optimal" use of technology. Optimization requires risk management and balancing of costs and benefits. The agency must flesh out its policies through the rational processes required in administrative law.

Among the things the agency must take into account, which it does not in the preamble, is "the public right of freedom of transit through the navigable airspace" referred to in 49 USC § 40101 and 49 USC § 40103. These two statutory provisions do not establish a statutory right for purposes of administering that title of the U.S. Code. They acknowledge a preexisting right. The TSA must minimize its interference with the right of travel in the course of optimizing its policies and the rule.

The agency must also take into account the Fourth Amendment to the U.S. Constitution, which bars unreasonable searches and seizures. Though the court in *EPIC v. TSA* summarily concluded that the use of body scanners fell within the "administrative search" exception to Fourth Amendment protection,[29] the issue was not ripe for decision, as the court did not have a rulemaking record before it. This rulemaking may invalidate the *EPIC v. TSA* decision as to the Fourth Amendment merits, and other courts will reconsider the issues in light of the record in this rulemaking.

b. Amidst talk of risk management, DHS and TSA have long failed to implement risk-based decision-making, and they fail to do so here

Homeland security is concerned with public safety—or domestic tranquility—the central, foundational reason for government. It is imperative, therefore, that decisions and expenditures be made sensibly and responsibly in this area because human lives are at stake.

To do so requires applying the kind of analytic risk management approaches that are routinely required of other governmental agencies and that have been standard coin for policy decision making for decades throughout the world. These approaches seek to balance the competing demands of safety and cost even in such highly charged and politicized decisions as where to situate nuclear power plants, how to dispose of toxic waste, and how to control pollution—decisions that engage the interests and passions of multiple groups.

[29] EPIC v. TSA at 16-18.

Most policies aimed at security will improve security. The important question is not whether a given policy improves security. It is whether the improvement in security justifies its costs. Nothing in the preamble to the proposed rule overcomes the evidence that the current body scanning policy does not provide cost-effective security. Indeed, it could produce greater death among American travelers than it averts.

Risk reduction measures that produce little or no net benefit to society or produce it at very high cost are not only irresponsible but also, essentially, immoral. When we spend resources to save lives at a high cost, we forgo the opportunity to spend those same resources on regulations and measures that can save more lives at the same cost or even at a lower one. Bad risk management kills.

Upon taking office in 2005, Department of Homeland Security (DHS) Secretary Michael Chertoff strongly advocated that the department "must base its work on priorities driven by risk."[30] Yet, a year later, when DHS expenditures had increased by some $135 billion beyond those already in place in 2001, and when the department had become the government's largest nonmilitary bureaucracy, one of its senior economists wistfully noted, "We really don't know a whole lot about the overall costs and benefits of homeland security."[31] By 2007, RAND President James Thomson was contending that DHS leaders "manage by inbox," that the "dominant mode of DHS behavior" was not risk management, but "crisis management."[32] In the same year, the Congressional Research Service after an exhaustive assessment, concluded that DHS simply could not answer the "central question" about the "rate of return, as defined by quantifiable and empirical risk reductions" on its expenditure.[33]

The emphasis on risk-informed decision making continued with the change of administrations after the 2008 elections, as Secretary Janet Napolitano insisted, "Development and implementation of a process and methodology to assess national risk is a fundamental and critical element of an overall risk management process, with the ultimate goal of improving the ability of decision makers to make rational judgments about tradeoff s between courses of action to manage homeland security risk."[34]

Yet a 2010 report of the National Research Council of the National Academies of Sciences, Engineering, and Medicine ("NRC") suggests that little progress had been

[30] Mayer, Matt A. 2009. *Homeland Security and Federalism: Protecting America from Outside the Beltway*, p. 62 (Santa Barbara, CA: ABC-CLIO).
[31] Troy Anderson, "Terror May Be at Bay at Port; Shipping Hubs Too Vulnerable," *Daily News of Los Angeles* , May 18, 2006.
[32] James A. Thomson, "DHS AWOL? Tough Questions about Homeland Security Have Gone Missing," *RAND Review* , Spring 2007.
[33] Todd Masse, Siobhan O'Neil, and John Rollins. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress,* pg. 14, Washington, DC: Congressional Research Service, February 2, 2007.
[34] NRC 2010, pg. 108.

made by that time. Requested by Congress to assess the activities of the Department of Homeland Security, a committee worked for nearly two years and came up with some striking conclusions. Except for the analysis of natural disasters, the committee "did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making," and therefore "only low confidence should be placed in most of the risk analyses conducted by DHS." Indeed, "little effective attention was paid to the features of the risk problem that are fundamental."[35]

The committee also found an "absence of documentation of methods and processes," with the result that the committee sometimes had to *infer* details about DHS risk modeling. In fact, "in a number of cases examined by the committee, it is not clear what problem is being addressed." It also found "a pattern" of "trusting numbers that are highly uncertain." Concluded the committee: "It is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses": although it found that "there are people at DHS who are aware of these current limitations," it "did not hear of efforts to remedy them."[36]

This situation is particularly strange because, as the committee also noted, the risk models used in the department for *natural* hazards are "near state of the art" and "are based on extensive data, have been validated empirically, and appear well suited to near-term decision needs."[37]

At times DHS has ignored specific calls by other government agencies to conduct risk assessments. For example, GAO requested that DHS conduct a full cost-benefit analysis of the extremely costly process of scanning 100 percent of U.S.-bound containers. To do so would require the dedicated work of a few skilled analysts for a few months or possibly a year. Yet, DHS replied that, although it agreed that such a study would help to "frame the discussion and better inform Congress," to actually carry it out "would place significant burdens on agency resources."[38]

The DHS appears to focus all or almost all of its analyses on the contemplation of the consequences of a terrorist attack while substantially ignoring the equally important "likelihood" component of risk assessment—whether the attack will happen or not—as well as the key issue of risk reduction. DHS risk assessment seems to simply identify a potential source of harm and then try to do something about it without evaluating whether the new measures reduce risk sufficiently to justify their costs. Kip Hawley, head of the TSA when the NRC report came out, responded, unconvincingly and contrary to the

---

[35] NRC 2010, pg. 11.
[36] NRC 2010, pg. 65.
[37] NRC 2010, pg. 57
[38] United States Government Accountability Office, "Report to Congressional Requesters: 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, October 2009.

conclusions of the report, that risk analytic work is done by TSA. "It's just not done the way they are defining it."[39]

In 2007, TSA, under Hawley, commissioned Boeing to develop and operate a Risk Management Analysis Tool ("RMAT"). In 2010 the agency asked RAND to evaluate the tool—"before relying on RMAT results for high-stakes resource management and policy decisions," according to the RAND report which came out late last year. RMAT is a "suite of tools and processes for conducting risk assessments" designed "to model and explain the complex interactions between security providers and systems and adversaries."

It is not clear how it is put together because the tool remains proprietary, but the RAND report is quite critical. The tool has "thousands of input variables," many of which cannot be estimated with much precision, and it could generate results that are "completely wrong." Moreover, it takes so long to run that "neither RAND nor Boeing have been able to conduct even a superficial sensitivity analysis" of its "many thousands of assumptions and parameter estimates." Moreover, it only deals with relative risk, not absolute risk (a key criticism as well in the 2010 NRC study), and its estimates of these "are subject to strong, probably untenable, assumptions." RMAT is also insensitive to changes in the magnitude of risk and "assumes no attack can be deterred."[40]

Little appears to have changed, as the NPRM devotes only one sentence to the cost-effectiveness of this security measure, and that sentence is problematic: "Risk reduction analysis shows that the chance of a successful terrorist attack on aviation targets generally decreases as TSA deploys AIT." This is a statement of the obvious. Virtually any new security measure—adding one bomb-sniffing dog at one airport, for example—will in some sense decrease the risk of a successful terrorist attack, however microscopically. The question risk analysis seeks to answer is not simply, "Will the added security measure reduce risk?" (or "generally decrease[]" it), but rather, "Will it reduce the risk enough to justify its cost?"

In 2010, the Government Accountability Office considered body scanning technology then being deployed by TSA. It noted pointedly that "cost-benefit analyses are important because they help decision makers determine which…investments in technologies or in other security programs, will provide the greatest mitigation of risk for the resources that are available," and it specifically declared that conducting a cost-benefit analysis of the new, expensive technology was "important."[41]

---

[39] Steven Cherry, Airport Security: Everything You Know Is Wrong, Techwise Conversations (podcast), May 2, 2012.
[40] A.R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System*, p. 98 RAND Corporation, 2012.
[41] Lord, Steve. *Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Areas of Aviation Security Remain*. United States Government Accountability Office, GAO-10–484T, March 17, 2010.

By simply stating that body scanners reduce risk—not that they reduce risk enough to justify their cost—the one sentence in the NPRM devoted to this key issue hints that risk analysis sufficient to validate the rule may not have been conducted.

c. TSA's body scanners fail to be cost-effective

Co-authors of this comment John Mueller and Mark Stewart have conducted exactly the sort of analysis that is required by this rulemaking. At several points, their study biased the analysis in favor of finding body scanning technology to be cost-effective security, and they assumed that it is technically effective at detecting body-borne explosives. Even under these generous assumptions, they found body scanners to be cost-ineffective.

The Mueller/Stewart analysis was published in 2011 in the peer-reviewed *Journal of Homeland Security and Emergency Management*, and it was included later in the year in their Oxford University Press book, *Terror, Security, and Money*. The version published in the *Journal of Homeland Security and Emergency Management* is attached to this comment as Appendix I.

The discussion below is a development of material presented in the 2011 article. It takes a complementary approach, but, while the input data and conclusions are the same, numerical results differ slightly from those in the 2011 analysis because of a change in the definition of what constitutes a successful attack.

The standard definition of risk adopted by the DHS is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequences})$$

where:

- *Threat* = annual probability a successful terrorist attack will take place if the security measure were not in place.
- *Vulnerability* = probability of loss (*i.e.*, that an explosive will be successfully detonated leading to damage and loss of life) given the attempt.
- *Consequences* = loss or consequence (economic costs, number of people harmed) if the attack is successful in causing damage.

Assuming 100% vulnerability, the above equation simplifies to:

$$Risk = (\text{Probability of a Successful Attack}) \times (\text{Losses Sustained in an Attack})$$

Reduction in risk is the degree to which a security measure foils, deters, disrupts, or protects against a terrorist attack.

The *benefit* of a security measure is the sum of the losses averted due to the security measure and any expected co-benefit from the security measure not directly related to mitigating vulnerability or hazard (such as reduction in crime, improved passenger experience, etc.). This benefit is then compared to the cost of the security measure, which should include opportunity costs, to determine cost-effectiveness. A security measure is cost-effective if the benefit exceeds the cost. The benefit of a security measure, then, is calculated:

Benefit = (Probability of a Successful Attack) x (Losses Sustained in an Attack) x (Reduction in Risk Generated by the Security Measure)

One can apply a common, government-approved approach called break-even analysis to these problems. In break-even analysis, one calculates what the likelihood of an otherwise successful attack would have to be to justify a security measure's cost. There are three key considerations in applying this approach.

Reduction in risk generated by the security measure

The threat that body scanners are primarily dedicated to is preventing the downing of a commercial airliner by an improvised explosive device (IED) smuggled on board by a passenger. The present analysis assumes that the terrorist successfully arrives at an airport undetected and proceeds to airline passenger screening bearing a concealed IED.

The analysis then assumes that the terrorist's luck substantially continues to hold through the next barriers:

- the likelihood of successfully avoiding detection by the metal detector and checkpoint transportation security officers is 90%,
- the likelihood of avoiding successful crew and passenger resistance on board the airliner when attempting to set off the bomb is 50%,
- the likelihood of successfully detonating the explosive is 75%, and
- the likelihood the explosion will actually down the airliner is 75%.

Under these conditions, there is a 75% chance the attack will fail due to one or another of these measures: existing checkpoint security measures, crew and passenger resitance, terrorist incompetence and amateurishness, and the technical difficulties in setting off a bomb sufficiently destructive to down an airliner.

The analysis now adds the body scanner/pat-down to this mix of security measures and assumes that the measure reduces the likelihood of a successful attack almost completely—by 85-90%.

The chance the terrorist will fail due to one of another of the existing measures or due to the body scanner now approaches an impressive 97%.

The cost of the security measure

Using TSA figures, it can be determined that the cost of purchasing, installing, maintaining, and staffing 1,800 body scanners will be $1.2 billion per year after it is fully deployed. A 2012 Congressional Research Service (CRS) comes to the same conclusion.[42] It also finds: "Even at full operating capacity, not all airports and not all screening lanes will be equipped with AIT under TSA's plan." Body scanners would clearly need to be fully deployed to be truly effective because, if some airport security lines do not use the technology, it would obviously be a matter of only minor inconvenience for terrorists to determine where the gaps are simply by visiting airports and taking a look—assuming they couldn't get the information on the web.

The NPRM arrives at a significantly lower cost estimate of roughly $400 million per year. However, the NPRM does not say how many scanners it assumes will be deployed, and personnel and operating costs decrease by 20% in 2014 and 2015 while scanner equipment costs increase by over 20% in the same period. This is a clear inconsistency, as more scanners should mean higher staff and operating costs. The NPRM also gives 'net costs' as these deduct the cost of not using metal detectors, yet a walk-through metal detector costs less than $2,000 compared to over $150,000 for a full-body scanner, and staffing will be significantly higher to operate and maintain the new scanners. TSA cost summaries are anything but transparent.

The consequences of a successful terrorist attack

The consequences of a successful terrorist attack where an IED detonates and downs in an airliner would be quite high: somewhere between $2-50 billion, which can be averaged to $25 billion including property loss, loss of lives, and the impact on the economy and on air travel. There have been many studies of such costs inflicted by the 9/11 disaster, and these generally run from around $100 billion to $200 billion. The cost consequences of the successful terrorist downing of a single commercial airliner that does not crash into a significant building on the ground would clearly be less—though they would still be quite substantial.

[42] Bart Elias, *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening*, Congressional Research Service, September 20, 2012.

Results

Applying these assumptions and estimates, body scanners only become cost-effective when the likelihood that there will be a successful attack if the body scanners were not included in the array of security measures is 22%—or one every five years.

TSA body scanning policy seems, then, rather impressively to fail a cost-effectiveness test, even one that very considerably biases the discussion in favor of coming to the opposite conclusion.

In the nine years after 9/11—before body scanners began to be deployed—there were only four instances in which a terrorist boarded (or, it seems, even attempted to board) an aircraft with body-borne explosives. Two of these failed (the 2001 shoe and 2009 underwear bombers), and two were carried out by Chechen women in Russia. None of these boarded their aircraft in the United States where the TSA's body scanners are deployed.

There is a very high likelihood that terrorists would be foiled, deterred or disrupted by police and security services, tip-offs from the public, and other pre-screening security measures at the airport, including no-fly lists, travel document checkers, behavioral detection officers, bomb appraisal officers, and other TSA and policing layers of security. But the analysis essentially assumed these had no effect.

It should also be noted that, since 9/11, only one attack consisting of two explosions has occurred in the United States, and this was on terra firma in Boston in 2013, using devices that could not pass through the magnetometers or x-ray machines that preceded body scanning in American airports. Similarly, there has been one case in which terrorists have been able to detonate bombs in the UK, producing four explosions, also on the ground, on the London transit system in 2005. This experience suggests that, for the most part, the terrorist adversary is not a terribly capable one.[43] Accordingly, the study was very generous in assuming that, if a terrorist were able to get his bomb on board and if he remained un-harassed by crew and passengers, he would still be 75% likely to successfully to detonate his bomb.

PETN seems to be the preferred explosive, and it has a long history of use in terrorist attacks. However, like most stable explosives, it is not easy to ignite. The best detonators are metallic but these are detectable by the airline security measures that were already in place before 9/11. Thus, the underwear bomber of 2009 used a syringe filled with a liquid explosive like nitroglycerin to detonate the PETN. However, this is by no

---

[43] Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft among Islamist Militants in Britain and Spain," *Studies in Con°ict & Terrorism,* Vol. 33, No. 10 (October 2010), pg. 911–932; John Mueller and Stewart, "The Terrorism Delusion: America's Overwrought Response to September 11, *International Security*, 37(1) Summer 2012, pg. 81-110; John Mueller, ed., *Terrorism since 9/11: The American Cases* (Columbus: Mershon Center, Ohio State University, 2012) 2013).

means an easy approach. Notes Jimmie Oxley, director of the Center of Excellence Explosives Detection, Mitigation, Response and Characterization at the University of Rhode Island, "that takes a lot of pre-experimentation to find out what would work."[44]

Richard Reid, the shoe bomber of 2001, spent two years in training camps in Afghanistan and Pakistan, and he had received bomb training by Midhat Mursi who has often been billed as al-Qaeda's "master bomb-maker." However, this obviously was not enough. The bomber needs not only to be highly skilled at the tricky task of detonation, but fully capable as well of improvising wisely to unforeseen technical problems like, in this case, damp shoelaces.

The analysis also assumed that if the on-board terrorist bomb were actually detonated there was a 75% chance it would down the airliner. This is generous because it is not easy to blow up an airliner. Airplanes are designed to be resilient to shock. The 1988 explosion of a bomb in the luggage compartment in a plane over Lockerbie, Scotland, was successful only because the bomb just happened to have been placed at the one spot in the luggage compartment where it could do fatal damage. According to Christopher Ronay, former head of the FBI bomb unit, if the bomb had been placed where it was surrounded by other luggage to absorb the blast, the passengers and the plane would have survived.[45]

Thus, even if the shoe and underwear bombs had exploded, the airliners attacked might not have been downed. The underwear bomber was reported at the time to be carrying 80 grams (Reid's shoe bomb contained only 50 grams) of PETN,[46] and when his effort was duplicated on a decommissioned plane in a test set up by the BBC, the blast did not breach the fuselage. This experiment led air accident investigator Captain J. Joseph to conclude, "I am very confident that the flight crew could have taken this aeroplane without any incident at all and get it to the ground safely."[47] In 2009, a similar bomb with 100 grams of the explosive, hidden on, or in, the body of a suicide bomber was detonated in the presence of his intended victim, a Saudi prince. It killed the bomber but only slightly wounded his target a few feet away.[48]

Moreover, an aircraft may not be doomed even if the fuselage is ruptured. A three-foot hole in the fuselage opened up on a Southwest Airlines plane in 2011, and the plane still landed safely.[49] In 2008, an oxygen cylinder exploded on a Qantas flight from

---

[44] Bryan Walsh, "Why It's Not Easy to Detonate a Bomb on Board," *Time*, December 28, 2009.
[45] Fred Bayles, "'Planes Don't Blow Up' Aviation Experts Assert," *International Herald Tribune*, July 24, 1996.
[46] "'Murderous' PETN links terror plots," CNN.com, December 29, 2009.
[47] BBC News, "Boeing 747 Survives Simulated 'Flight 253' Bomb Blast," March 5, 2010. The explosive test was conducted while the aircraft was on the ground.
[48] Peter Bergen and Bruce Hoffman, *Assessing the Terrorist Threat*, p. 9, Bipartisan Policy Center, Washington, DC, September 10, 2010.
[49] "Southwest to Ground 81 Planes after Hole Prompts Emergency Landing," cnn.com , April 2, 2011.

Hong Kong, blasting a six-foot hole in the fuselage. The plane suddenly depressurized, but the aircraft returned safely to Hong Kong.[50] In 1989, a cargo door opened on a United Airlines flight heading across the Pacific, extensively damaging the fuselage and cabin structure adjacent to the door. Nine passengers and their seats were sucked out and lost at sea, but the plane was able to make an emergency landing in Honolulu.[51]

Given this record, and the many layers of existing security, it seems an enormous stretch to expect that terrorists bearing explosives on their bodies at a U.S. airport would have been able to go from a zero success rate per decade to a success rate of once every five years if body scanners were not deployed. But that, according to the analysis, is what the expensive body scanner deployment essentially assumes—or would need to assume to be considered cost-effective.

d. Non-monetary costs, the mortal danger produced by increased automobile travel, and opportunity costs further undercut the policy

There appears to be an unspoken assumption among those in charge of airline security that, while their measures may sometimes be wasteful or inconvenient, they cause no harm. The assumption is wrong, and it has produced a set of policies underlying the proposed rule that are arbitrary and capricious.

In assessing the costs of body scanning machines, the Mueller/Stewart study, like the TSA's NPRM, included only those attendant on purchasing, installing, maintaining, and operating the machinery itself, along with those imposed by the related pat-down opt-out. Although the benefit of body scanning is vastly eclipsed by these costs alone, it is important to consider as well various other costs inflicted by the technology that are less easily measured. If even decidedly conservative estimates of these were added into the cost estimate, the security measure would fail a cost-benefit test to an even greater degree.

Highly significant to many people—and central to the concerns that led to the demand that TSA produce an NPRM on the body-scanner measure—are the costs in infringement on civil liberties and on privacy. Articulated in the privacy section above, these are not easily quantifiable, but they are clearly considerable and should be part of the cost-benefit analysis.

It is also important to note that security measures that travelers perceive as harassing can cause them to avoid air travel entirely, taking alternative methods of transportation that are more dangerous instead. One study has concluded, for example,

[50] "Depressurisation—475 km north-west of Manila, Philippines—July 25, 2008," ATSB Transport Safety Report, Aviation Occurrence Investigation AO-2008-053 Interim Factual No. 2, Australian Transport Safety Bureau, Australian Government, November 2009.
[51] Aviation Safety Network, Flight Safety Foundation, www.flightsafety.org.

that such harassment has helped lead to a pronounced decline in short-haul flying since 2001, with the result that approximately 500 more Americans die each year than otherwise would because they travel by automobile, a far more dangerous mode of transportation.[52] This is more death than has been visited worldwide by Islamist extremist terrorism since 9/11 outside of war zones.[53] The body scan/pat-down regime seems to be special in the degree to which it inspires irritation and a sense of harassment.

Long queues at TSA screening checkpoints and travelers' perceptions about the chance of delay due to body scanning may produce additional, relevant costs that deserve further study. A 2008 report found that TSA security increased delays by 19.5 minutes in 2004, and that passengers value their time at about $40 per hour (in 2012 dollars).[54] Progress has been made in reducing passenger delays since then, but delays are still frequent.

The body scanners do little to improve the situation, as trials in Australia found that "passenger screening time through the trial lane took slightly longer than the passenger screening time through a standard screening lane," most likely caused by the higher alarm rate, "with the data suggesting that the average passenger is six times more likely to alarm in the body scanner." The delays seem modest (a matter of several seconds), but the CRS 2012 review says, "[R]oughly 20% of those concerned about AIT expressed specific concern over increased passenger delays. "

The longer a passenger waits to be screened the more likely they are to be unsatisfied,[55] and waiting in security lines is an important indicator of passenger experience. A 2012 study found that reducing waiting times from 10 to 5 minutes increased airline market share by 1% for a large airport in the U.S. (or $1.5 billion in additional U.S. airline revenues based on total annual U.S. airline revenues of $150 billion).[56] Hence, an improved passenger experience will also increase revenues to airlines. The opposite must also be true. Longer delays mean less airline revenue.

If concern about delays causes travellers to add an average of one minute to their travel schedules per flight, this equates to $484 million per year in value of passenger time based on $40 per hour and 726 million enplanements in the U.S. in 2011. Avoidance may cause U.S. airline market share to fall by a very modest 0.1% or $150 million. These

---

[52] Blalock, Garrick, Vrinda Kadiyali, and Daniel H. Simon, *The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel*. Journal of Law and Economics 50(4) November, 2007: 731–755.
[53] John Mueller and Mark G. Stewart, Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security, New York: Oxford University Press, 2011, pg. 43.
[54] Treverton, G.F., Adams, J.L., Dertouzous, J., Dutt, A., Everingham, S.F. and Larson, E.V. (2008), The Costs of Responding to the Terrorist Threats. In *Terrorism, Economic Development, and Political Openness* , ed. P. Keefer and N. Loayza. New York, Cambridge University Press.
[55] Gkritza, K., Niemeier, D. and Mannering, F. (2006), Airport Security Screening and Changing Passenger Satisfaction: An Exploratory Assessment, *Journal of Air Transport Management*, 12(5): 213-219.
[56] Holguin-Veras J., Xu, N. and Bhat, C. (2012), An Assessment of the Impacts of Inspection Times on the Airline Industry's Market Share after September 11th, *Journal of Air Transport Management*, 23(1): 17-24.

opportunity costs associated with the scanners sum to over $600 million per year and will dramatically reduce the cost-effectiveness of the scanners.

To the degree that successive layers of security generate a sense of harassment and privacy-infringement that causes passengers to adopt other modes of transport or to forgo travel entirely, substantial costs are imposed on the aviation and travel industries, as well. The fact that aviation security passenger fees have recently doubled in an attempt to fund further "layers" of security at airports is also relevant in this—and flying appears to be very sensitive to price.

e. The risk of being killed by terrorists during an airline flight is already acceptably low by standards TSA uses for other dangers

A key concept in risk analysis is acceptable risk. Overall, it is clear that governments and their regulators have been able to set, and essentially to agree upon, risk acceptance criteria for use in decision making for a wide variety of hazards including ones that are highly controversial and emotive such as pollution, nuclear and chemical power plant accidents, and public exposure to nuclear radiation and environmental carcinogens.

For example, a review of 132 U.S. federal government regulatory decisions associated with public exposure to environmental carcinogens found that regulatory action never occurred if the individual annual fatality risk (the yearly likelihood an American would die from them) was lower than 1 in 700,000.[57] Overall, experience with established regulatory practices in several developed countries suggests that risks are deemed unacceptable if the annual fatality risk is higher than 1 in 10,000 or perhaps higher than 1 in 100,000. If the annual fatality risk is only 1 in 100,000, risks begin to become acceptable, and there is an increasing consensus that this is so when the annual fatality risk is lower than 1 in 700,000 or perhaps 1 in 1 million or 1 in 2 million. The rough annual fatality risk an American will be perish at the hands of terrorists (with the 9/11 tragedy very much included in the count) is 1 in 3.5 million.[58]

These considerations, substantially accepted for years—even decades—by public regulatory agencies after extensive evaluation and considerable debate and public discussion, provide a viable, if somewhat rough, guideline for public policy. Clearly, hazards that fall in the unacceptable range (traffic accidents, for example, which generate an annual fatality rate in the United States of 1 in 8,200) should generally command the most attention and the most resources. By the same token, those that fall, or begin to fall, into the acceptable range (drowning in bathtubs, for example, with an annual fatality risk

[57] Travis, C. C., S. A. Richter, E. A. C. Crouch, R. Wilson, and E. D. Klema. 1987. Cancer Risk Management: A Review of 132 Federal Regulatory Decisions. *Environmental Science and Technology* 21(5): 415–420.
[58] For a discussion see, John Mueller and Mark G. Stewart, *Terror, Security, and Money: Balancing the Risks, Benefits, and Costs of Homeland Security*, New York: Oxford University Press, 2011, ch. 2.

of 1 in 950,000) would generally be deemed of little or even negligible concern—they are risks we can live with—and further precautions would scarcely be worth pursuing unless they are quite remarkably inexpensive.

In one area—and, it seems, in only one—the TSA has actually, if accidentally, engaged in a public assessment of acceptable risk. It involves the risk that the original body scanners, which applied X-ray technology, will cause cancer.

Asked about this on the PBS NewsHour, TSA head John Pistole essentially said that, although the cancer risk was not zero, it was acceptable. A set of studies, he pointed out, "have all come back to say that the exposure is very, very minimal," and "well, well within all the safety standards that have been set."[59] The NPRM, too, says this risk is acceptably low: "the potential cancer risk cannot be estimated, but is likely to remain so low that it cannot be distinguished from the effects of other exposures including both ionizing radiation from other natural sources, and background risk due to other factors."

Contrary to the NPRM's contention, however, if the radiation exposure delivered to each passenger is known (and, of course, it is), one can calculate what the risk of getting cancer is for a single exposure using a standard approach that, although controversial, is officially accepted by nuclear regulators in the United States and elsewhere.

Based on the 2012 review of scanner safety conducted by the European Commission Scientific Committee on Emerging and Newly Identified Health Risks,[60] that fatal cancer risk per scan is about one in 60 million.[61]

The chance an individual airline passenger will be killed by terrorists is much lower: one in 90 million.

Therefore, unless the TSA believes that terrorists will in the near future become far more capable of downing airliners than they have been in the past, the risk of being killed by a terrorist in an airliner is already fully acceptable by the standards TSA applied to the cancer risk from body scanners that used X-ray technology.

This is a key issue. The question that should begin the analysis is not "Are we safer?" Rather, it is "How safe are we?" Or, as the issue was put in 2002 by risk analyst

---

[59] PBS NewsHour, November 16, 2010.
[60] Scientific Committee on Emerging and Newly Identified Health Risks, SCENIHR, Health effects of security scanners for passenger screening, European Commission, Brussels, 26 April 2012.
[61] Passenger exposure to backscatter scanners is 0.4 mSv per scan. A 1 mSv dose, according to standard models, increases the risk of fatal cancers by 0.004 percent. The increase in fatal cancer risk per scan is thus $0.4 \times 0.001 \times 0.004\%$ = one in 60 million.

Howard Kunreuther, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?"[62]

f. It is not clear that the machines actually secure against attacks

Under highly favorable assumptions that only consider dollar expenditures, body scanners are not cost-effective security. When the privacy consequences of rendering nude images of American travelers are added in along with other costs, the evidence that body scanners fail cost-benefit analysis rises to overwhelming.

This analysis assumes that the machines work perfectly to discover explosives and similar threats. Whether this is a valid assumption, however, appears questionable. Certainly TSA officials' public pronouncements on this issue are less than fully reassuring.

When TSA Administrator John Pistole appeared on the PBS NewsHour on November 16, 2010, he was specifically asked: "A lot of passengers are wondering whether these procedures are proportionate to the threat. And I'm just wondering, would, for instance, these more extensive pat-downs and the full-body scans, would they have caught the Christmas Day bomber with the explosives in his underwear?"

Interestingly Pistole did not answer or comment on that question directly. To the key issue about whether the procedures are proportionate to the threat, he simply said, "I know the threats are real." This observation is relevant, but scarcely responsive. His response to the question about whether the measures would have caught the underwear bomber was equally evasive: "I believe that the techniques and the technology we're using today are the best possible that we have. And it gives us the best opportunity for detecting a Christmas Day-type bomber."

To her credit, the interviewer, Margaret Warner, persisted for one more round: "Are there any other examples of people who have gotten through with explosive material that weren't caught that would have been caught with these new methods?"

This generated a response that can charitably be characterized as irrelevant: "We know that the General Accounting Office and the Homeland Security inspector general and even our own TSA Office of Inspection does what we refer to as covert testing. Now, I can't go into the details of those, but some of the results of those are that we could and should improve the techniques that we use to do the security screening."

The TSA's NPRM is distinctly less than clear on this issue, offering ambiguous assertions like:

[62] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis* , 22(4) 2002, pg. 662–663.

> "AIT currently provides the best available opportunity to detect non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security layers."
>
> "The best defense against these and other terrorist threats remains a risk-based, layered security approach that uses a range of screening measures, both seen and unseen. This includes the use of AIT, which is proven technology for identifying non-metallic explosives during passenger screening, such as the device Umar Farouk Abdulmutallab attempted to detonate on Christmas Day 2009."
>
> "Advanced Imaging Technology is proven technology which provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using metal detectors."

Language arguing that body scans are the "best available opportunity" or provide the "best defense" or have detected items missed by other technologies does not make the case that it really works to detect body-borne bombs or bomb material. And it is certainly not the same as saying that the measure is cost-effective.

VI. The body scanning policy should be reversed pending a new, sufficient rulemaking

Due to TSA policies that the proposed rule would ratify, many Americans avoid air travel altogether, preferring to drive long distances instead. This may result in as many as 500 deaths per year, deaths that are attributable to these policies.

The benefits of notice-and-comment rulemaking accrue when the public is allowed to comment on a rule that has contours. In the ideal rulemaking—not even ideal: in the usual rulemaking—a proposed rule delineates much of what may appear in the final rule. This allows affected parties to comment intelligently on manifold nuances of the proposed rule. The agency can then consider the wisdom offered by interested parties with perspective and experience that the agency lacks. The result is often a rule that is improved.

By proposing a rule without contours, and by hiding the analysis that might support even the general policy statement proposed, the TSA has denied the public the ability to meaningfully comment. TSA has also denied itself the ability to learn how its practices (and analyses) could be improved. In an important sense, the rulemaking has already failed.

By proposing a policy statement as if it were a legislative rule, the agency may have irreparably biased the process against the public participation required by notice-and-comment rulemaking. It is unacceptable that the agency's failure in the present notice-and-comment rulemaking should aid the agency in maintaining its disputed policy.

None of the remedies for this are attractive, but given our conclusion that the TSA's current policies cause more death than they avert, the TSA should voluntarily adopt the presumption that its current practices are not justified. TSA should suspend the use of body scanners for primary screening, initiate a rulemaking around a true legislative rule, and await the results of that rulemaking and subsequent litigation before it proceeds with the policy of using body scanners for primary screening.

Reversing the present policy would likely save American lives, reduce taxpayer expenditures, and relieve an impediment to economic growth in the travel industry.

Journal of Homeland Security and Emergency Management

Volume 8, *Issue* 1 2011 *Article* 30

Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening

Mark G. Stewart, *The University of Newcastle, Australia*
John Mueller, *Ohio State University*

Recommended Citation:
Stewart, Mark G. and Mueller, John (2011) "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 30.
DOI: 10.2202/1547-7355.1837
Available at: http://www.bepress.com/jhsem/vol8/iss1/30

Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening

Mark G. Stewart and John Mueller

Abstract

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AITs) that are full-body scanners to inspect a passenger's body for concealed weapons, explosives, and other prohibited items. The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. The cost of this technology will reach $1.2 billion per year by 2014. The paper develops a preliminary cost-benefit analysis of AITs for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and costs of security measures in the estimation of costs and benefits. Since there is uncertainty and variability of these parameters, three alternate probability (uncertainty) models were used to characterise risk reduction and losses. Economic losses were assumed to vary from $2-$50 billion, and risk reduction from 5-10 percent. Monte-Carlo simulation methods were used to propagate these uncertainties in the calculation of benefits, and the minimum attack probability necessary for full body scanners to be cost-effective were calculated. It was found that, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. However, the attack probability needs to exceed 160-330 percent per year to be 90 percent certain that full body scanners are cost-effective.

KEYWORDS: terrorism, security, cost-benefit analysis, aviation security, passenger screening

Author Notes: Mark G. Stewart, Australian Research Council Professorial Fellow; Professor and Director, Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia; phone: +61 2 49216027; email: mark.stewart@newcastle.edu.au. John Mueller, Professor of Political Science and Woody Hayes Chair of National Security Studies, Mershon Center for International Security Studies and Department of Political Science, Ohio State University, Columbus, Ohio 43201, United States; phone: +1 614 2476007; email: bbbb@osu.edu.
Part of this work was undertaken while the first author was a Visiting Professor in the Department of Civil, Structural and Environmental Engineering at Trinity College Dublin. He greatly appreciates the assistance provided by Trinity College. The first author also appreciates the financial support of the Australian Research Council.

INTRODUCTION

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AIT) that are full-body scanners to inspect a passenger's body for concealed weapons and explosives. The cost of this technology will reach $1.2 billion per year by 2014. The U.S. Government Accountability Office (GAO) remarked in 2010 that "conducting a cost-benefit analysis of TSA's AIT deployment is important.", and "would help inform TSA's judgment about the optimal deployment strategy for the AITs" (Lord 2010). Yet, before deciding to install AITs at considerable cost the TSA has not conducted a cost-benefit analysis. This absence of a cost-benefit analysis for AITs is the motivation for the present study.

Since the events of 9/11 there has been much focus on preventing or mitigating damage and casualties caused by terrorist activity. A key issue is whether counter-terrorism expenditure has been invested in a manner that optimizes public safety in a cost-effective manner. This is why the 9/11 Commission report, amongst others, called on the U.S. government to implement security measures that reflect assessment of risks and cost-effectiveness. However, while the U.S. requires a cost-benefit analysis for government regulations (OMB 1992), this does not appear to have happened for most homeland security expenditure.

The need for risk and cost-benefit assessment for homeland security programs, and those supported by the Department of Homeland Security (DHS) in particular, is forcefully made by many in government, industry and academe (e.g., Friedman 2010, Poole 2008). The U.S. National Research Council (NRC 2010), after a 15 month study period, made critical recommendations about the DHS, and their primary conclusion was: "the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested" and "only low confidence should be placed in most of the risk analyses conducted by DHS".

To compare costs and benefits requires the quantification of threat probability, risk reduction, losses, and security costs. This is a challenging task, but necessary for any risk assessment, and the quantification of security risks is recently being addressed (e.g., Stewart et al. 2006, Stewart and Netherton 2008, Dillon et al. 2009, Cox 2009), as well as recent life-cycle and cost-benefit analyses for infrastructure protective measures (Willis and LaTourette 2008, von Winterfeldt and O'Sullivan 2006, Stewart 2008, 2010, 2011). Much of this work can be categorized as 'probabilistic terrorism risk assessment'.

Stewart (2010) has shown that, based on expected values, the threat probability has to be very high for typical counter-terrorism measures for buildings and bridges to be cost-effective. Similar cost-benefit analyses have shown that the U.S. Federal Air Marshal Service which costs over $1 billion per year fails to be cost-effective, but that hardening cockpit doors is very cost-effective (Stewart and Mueller 2008). It therefore appears that many homeland security measures would fail a cost-benefit analysis using standard expected value methods of analysis as recommended by the U.S. Office of Management and Budget (OMB); a detailed assessment of threats and vulnerabilities leads to similar conclusions (Mueller 2010, Mueller and Stewart 2011). This suggests that policy makers within the U.S. government and DHS are risk-averse.

Terrorism is a frightening threat that influences our willingness to accept risk, a willingness that is influenced by psychological, social, cultural, and institutional processes. Moreover, events involving high consequences can cause losses to an individual that they cannot bear, such as bankruptcy or the loss of life. On the other hand, governments, large corporations, and other self-insured institutions can absorb such losses more readily and so governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making (e.g., Sunstein 2002, Ellingwood 2006). This is confirmed by the OMB which requires cost-benefit analyses to use expected values (an unbiased estimate), and where possible, to use probability distributions of benefits, costs, and net benefits (OMB 1992).

For many engineering systems the threat rate is known, but for terrorism the threat is from an intelligent adversary who will adapt to changing circumstances. For this reason, a practical approach is a 'break even' cost-benefit analysis that finds the minimum probability of a successful attack required for the benefit of security measures to equal their cost. While this approach is not without challenges (Farrow and Shapiro 2009), 'break-even' cost-benefit analyses are increasingly being used for homeland security applications (e.g., Ellig 2006, Willis and LaTourette 2008, Winterfeldt and O'Sullivan 2006). Hence, we will undertake a 'break even' cost-benefit analysis in this paper.

The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. Since AITs operated by the TSA are effective only for passengers leaving the U.S., the present paper considers the threat probability, risk reduction and losses for a suicide bomber who attempts to board an aircraft at a U.S. airport. This preliminary study will also include uncertainty analysis in the cost-benefit calculations to reflect the uncertainty in underlying data and modeling assumptions, and will allow the probability of cost-effectiveness to be calculated. AITs are being trialed or deployed in the U.K., France, Netherlands, Italy, Canada, Australia and elsewhere which will cost billions of dollars if they are also used for primary screening in those countries. Hence, the present paper will provide useful guidance to U.S. and international aviation security regulators.

RISK AND COST-BENEFIT METHODOLOGY

A security measure is cost-effective when the benefit of the measure outweighs the costs of the security measure. The *net benefit of a security measure* is:

$$\text{Net Benefit} = \underbrace{p_{attack} \times C_{loss} \times \Delta R}_{\text{benefit}} - \underbrace{C_{security}}_{\text{cost}} \tag{1}$$

- p_{attack}: The *probability of a successful attack* is the likelihood a successful terrorist attack will take place if the security measure were not in place.
- C_{loss}: The *losses sustained in the successful attack* include the fatalities and other damage - both direct and indirect - that will accrue as a result of a successful terrorist attack, taking into account the value and vulnerability of people and infrastructure as well as any psychological and political effects.
- ΔR: The *reduction in risk* is the degree to which the security measure foils, deters, disrupts, or protects against a terrorist attack.

In the process:

- we present our analysis in a fully transparent manner: readers who wish to challenge or vary our analysis and assumptions are provided with the information and data to do so.
- in coming up with numerical estimates and calculations, we generally pick ones that bias the consideration in favor of finding the homeland security measure under discussion to be cost-effective.
- we decidedly do *not* argue that there will be no further terrorist attacks; rather, we focus on the net benefit of security measures and apply "break even" cost-benefit analyses to assess how high the likelihood of a terrorist attack must be for security measures to be cost-effective.
- we are aware that not every consideration can be adequately quantified.
- although we understand that people are often risk-averse when considering issues like terrorism, governments should be risk-neutral when assessing risks, something that entails focusing primarily on mean estimates in risk and cost-benefit calculations, not primarily on worst-case or pessimistic ones.

COST-BENEFIT ASSESSMENT OF FULL BODY SCANNERS

Costs ($C_{security}$)

The TSA will use AITs as a primary screening measure, and plans to procure and deploy 1,800 AITs by 2014 to reach full operating capacity (Lord 2010). The costs are considerable. The DHS FY2011 budget request for 500 new AITs includes \$214.7 million for their purchase and installation, \$218.9 million for 5,355 new Transportation Security Officers (TSOs) and screen managers to operate the AITs at the checkpoints, and \$95.7 million for 255 positions for support and airport management. The TSA estimates that the annualized cost of purchasing, installing, staffing, operating, supporting, upgrading, and maintaining the first 1,000 units is about \$650 million per year (Rossides 2010). We can then infer that 1,800 units will cost approximately \$1.2 billion per year and we assume 100% coverage at all airports in the U.S., although this may be too generous as the planned roll out of 1,800 scanners may still leave 500 airport checkpoints without AITs (Halsey 2010). If correct, the purchase, operation and maintenance of additional scanners will add considerably to the \$1.2 billion cost used herein.

Since AITs provide scans that reveal genitals and other personal information, passengers who opt-out of an AIT are subject to 'intrusive' pat-downs. This perceived invasion of privacy, or extra delays during screening, may deter some from travelling by air, and for short-haul passengers, to drive to their destination instead. Since driving is far riskier than air travel, the extra automobile traffic generated by existing aviation security measures has been estimated to result in 500 or more extra road fatalities per year (Blalock et al. 2007). On the other hand, it may be argued that AITs may provide a type of 'security theatre' that will make travelers feel safer which in itself is beneficial. Whether AITs will result in opportunity costs or not is beyond the scope of the present paper. In the present paper, we will assume that AITs will cost $C_{security}$=\$1.2 billion per year and will ignore opportunity costs - although these have the potential to be very substantial. We also ignore any possible security theatre benefits - likely, however, to be small as there is little evidence that AITs by themselves will make travelers feel much safer, and could well have the opposite effect.

Economic Loss (C_{loss})

The loss of an aircraft and follow-on economic costs and social disruption might be considerable. A 2007 RAND study reported that the loss of an airliner with 300 passengers by a shoulder fired missile, a shutdown of U.S. airspace for a week, and 15% drop in air travel in the 6 months following the attack would cause an economic loss of more than \$15 billion (Chow et al. 2005). Another study, again assuming an attack using shoulder fired missiles also assumed a seven day shutdown, but a two-year period of recovery (Gordon et al. 2007). Losses were summed across airline, ground transportation, accommodation, food, gifts/shopping and amusement sectors to derive loss estimates of \$214-\$420 billion. This seems overly conservative as adding up individual sectoral losses can lead to double counting and "that large scale terrorist attacks cause reallocations of people and resources across sectors" and "it is relatively easy to measure the heavy losses experienced by some areas but very difficult to measure the small indirect gains experienced by thousands of areas." (Enders and Olsen 2011).

The downing of an airliner due to an passenger-borne IED is likely not to trigger the same response as a downing caused by a shoulder fired missile as no counter-measures exist for a missile attack that could be implemented quickly. On the other hand, a series of screening measures were implemented quickly following the 9/11 and subsequent attacks that provides assurance to the public that it is safe to fly. This all suggests that the losses forecast above for a shoulder-fired missile attack will over-estimate losses for our threat scenario.

A report for the DHS concludes that the best estimate for value of a statistical life (VSL) for homeland security analysis is $6.5 million in 2010 dollars (Robinson et al. 2010). If we take 300 lives at VSL of $6.5 million then the economic loss caused by 300 fatalities is approximately $2 billion. If we add the cost of a large commercial airliner of $200-$250 million then direct economic loss is approximately $2.5 billion if we also include forensic and air transport crash investigations. Passenger numbers less than 300 will reduce direct losses considerably, for example, 150 passenger will reduce direct losses to $1.5 billion. However, we will select C_{loss}=$2 billion as a reasonable lower bound.

To establish something of an upper bound for the losses inflicted by conventional terrorist attacks, it may be best to begin with the losses inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. A study by the National Center for Risk and Economic Analysis of Terrorist Events found that the impact on the U.S. economy of the 9/11 attacks range from 0.3 to 1.0 percent of GDP (Blomberg and Rose 2009). While the $15 billion proposed by the RAND study would be a plausible upper value of economic loss, it may fail to consider full losses to the economy. The economic consequences of a suicide bomber would likely be less than the shocking events of 9/11, so we will assume that a reasonable upper bound of losses is 0.3% of GDP ($42 billion based on 2010 GDP figures) which we will round up to C_{loss}=$50 billion.

Results from uncertainty and probabilistic modeling may be sensitive to the shape of the probability distribution. In this case, we will assume three alternate probability distributions of loss (see Figure 1):

1. Normal Distribution - loss is normally distributed with 95% confidence interval between $2 billion and $50 billion, then mean loss is $26 billion and standard deviation is $12.2 billion. Loss is truncated at $500 million to represent loss of a single aircraft with few passengers and no indirect losses.
2. Uniform Distribution - equal likelihood of any loss between $2 billion and $50 billion, with mean loss of $26 billion.

3. Triangular Distribution - higher likelihood of smaller losses bounded by \$2 billion and \$50 billion, with mean loss of \$18 billion.

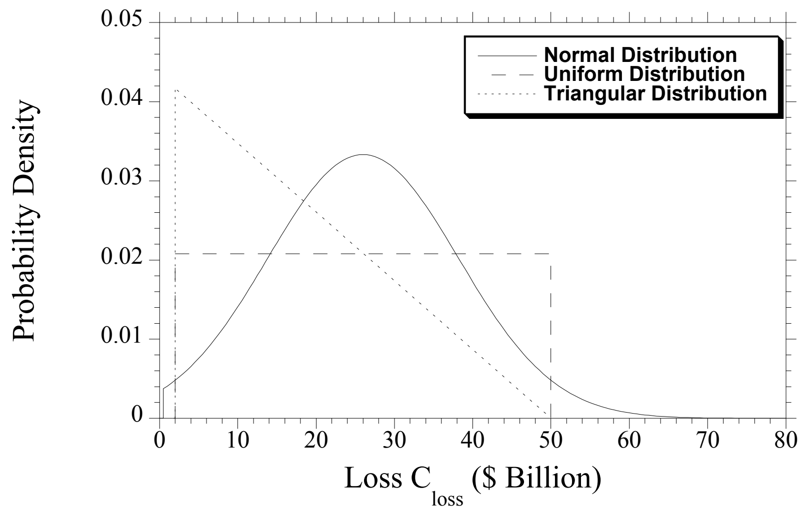


Figure 1. Alternative Loss Uncertainty Models.

Risk Reduction (ΔR)

A key motivation for the rapid deployment of AITs was the foiled 2009 Christmas Day plot by Umar Farouk Abdulmutallab to hide liquid explosives in his underwear to blow-up Northwest Airlines Flight 253. There is little doubt that that full-body scanners improve the ability to detect weapons and explosives, however, there is doubt about their ability to detect *all* explosives that may be hidden on a person. The GAO follows this line of reasoning by casting doubt on the ability of AITs to detect the weapon Abdulmutallab used in his attempted attack (Lord 2010). It is also suggested that existing screening methods, such as detectors that test swabs wiped on passengers and luggage for traces of explosives, would have detected the explosives used in the 2009 Christmas Day attack. Moreover, the search for a detonator is equally important and easier to detect since most detonators contain metal.

Also relevant is the fact that it is not necessarily easy to blow up an airliner even if a bomb detonates. Airplanes are designed to be resilient to shock, and attentive passengers and airline personnel complicate the terrorists' task further. Apparently, the explosion over Lockerbie was successful only because the suitcase bomb just happened to have been placed at the one place in the luggage compartment where it could do fatal damage (Bayles 1996). Logically, then, a terrorist will not leave such matters to luck, which may be why the shoe and underwear bombers both carried their bombs onto the planes and selected window seats that are, of course, right next to the fuselage. Yet even if their bombs had exploded, the airliner might not have been downed. The underwear bomber was reported to be carrying 80 grams of the explosive PETN (PETN or Pentaerythritol tetranitrate) and when his effort was duplicated on a decommissioned plane in a test set up by the BBC, the blast did not breach the fuselage (BBC 2010), although the explosive test was conducted while the aircraft was on the ground. Moreover, an aircraft may not be doomed even if the fuselage is ruptured. In 2008 an oxygen cylinder exploded on a Qantas flight blasting a two meter hole in the fuselage. In 1989, a cargo door opened on a United Airlines flight heading across the Pacific extensively damaging the fuselage and cabin structure adjacent to the door. In both instances the aircraft landed safely. Aircraft, like many types of infrastructure are more robust and resilient than we often give them credit for.

PETN has a long history of use in terrorist attacks but, like most stable explosives, it's not easy to ignite. Presumably because airport screening makes smuggling a metal detonator a risky proposition, the underwear bomber used a syringe filled with a liquid explosive like nitroglycerin. However, this adds to the difficulty of a successful detonation.

Since two Russian airliners were blown up by terrorists in 2004, the terrorist's task is obviously not impossible. However, it is a difficult one, and terrorists trying to detonate explosives in flight are likely to end up with more duds than successes. Moreover, although their explosion may cause real damage and loss of life, this result is by no means guaranteed: aircraft have shown themselves to be resilient to accidental explosions or other mid-air mishaps, and so 'blowing up' an airliner is more challenging than we imagine.

Although some terrorists are skilled and well trained, many terrorist attacks in the U.K, U.S. and Afghanistan were averted by the 'ineptitude' of the terrorists themselves. Moreover, many, but not all, terrorists lack bomb-making skills such as those behind the failed car bombings in London and Glasgow in 2007, and Times Square in 2010 (Kenney 2010). Assembling and detonating a small or miniaturized IED needed to minimize the chances of passenger screening detection is even more challenging than their larger compatriots. This all suggests that even if a terrorist can board an aircraft and attempt to detonate the device undetected, there is no 100% surety that the bomb will successfully detonate - poor training, lack of hands-on experience and poor tradecraft means there is a good chance that the IED will be a 'dud'.

Suicide bombers, like drug couriers, can go to inordinate lengths to conceal weapons or contraband - including body cavities. In August 2009 Abdullah Hassan al-Asiri attempted to assassinate a Saudi prince by detonating 100 grams of PETN, which according to some reports was concealed in his underwear, and other reports, his rectum. A Europol (2009) study confirmed that concealment of IEDs in rectal cavities was possible but that the body would absorb much of the blast. This explains why Asiri succeeded in only killing himself, while the Saudi prince who stood close by escaped unharmed. It would seem that a terrorist would need to remove explosives from their underwear for it to be fully effective against a target - an act which increases the odds of detection.

The TSA has arrayed '21 Layers of Security' to 'strengthen security through a layered approach'. This is designed to provide defense-in-depth protection of the travelling public and of the United States transportation system. Of these 21 layers, 15 are 'pre-boarding security' (i.e., deterrence and apprehension of terrorists prior to boarding aircraft): Intelligence, International Partnerships, Customs and border protection, Joint terrorism task force, No-fly list and passenger pre-screening, Crew vetting, Visible Intermodal Protection Response (VIPR) Teams, Canines, Behavioral detection officers, Travel document checker, Checkpoint/transportation security officers, Checked baggage, Transportation security inspectors, Random employee screening, and Bomb appraisal officers. The remaining six layers of security provide 'in-flight security': Federal Air Marshal Service, Federal Flight Deck Officers, Trained flight crew, Law enforcement officers, Hardened cockpit door, and Passengers.

The risk reduction (ΔR) is the additional risk reduction achieved by the presence of AITs when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all other security measures. If a combination of security measures will foil every threat then the sum of risk reductions is 100%. This soon becomes a multidimensional decision problem with many possible interactions between security measures, threat scenarios, threat probabilities, risk reduction and losses. Fault and event trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions. This is the approach used herein.

We start assessing risk reduction by developing a simple systems model of new (AITs) and existing aviation security measures. For a suicide bomber to succeed in downing a commercial airliner requires that all stages of the planning, recruiting and implementation of the plot go undetected. We will focus on three steps linked to aviation security:

1. success in boarding aircraft undetected
2. success in detonating IED
3. location and size of IED is sufficiently powerful to down the aircraft

The security measures in-place to foil, deter or disrupt these three steps are:

1. success in boarding aircraft undetected - 10 layers of security: intelligence, international partnerships, customs and border protection, joint terrorism

task force, no-fly list and passenger pre-screening, behavioral detection officer, travel document checker, checkpoint/transportation security officers (TSO), transportation security inspectors, bomb appraisal officers
2. success in detonating IED - trained flight crew and passengers
3. location and size of IED is sufficiently powerful to down the aircraft - aircraft resilience

If any one of these security measures are effective, or the capabilities of the terrorist are lacking, then the terrorist will not be successful. We do not include all 'layers' of TSA security such as checked baggage or canines, only those likely to stop a suicide bomber. Note that air marshals, hardened cockpit door, armed flight crew, and on-board law enforcement officers are designed to protect against hijackings or replication of a 9/11 style attack. Moreover, air marshals are on less than 10% of aircraft and so are unlikely to be deter, foil or disrupt a suicide bomber (Stewart and Mueller 2008).

Figure 2 shows a reliability block diagram used to represent the system of foiling, deterring or disrupting an IED terrorist attack on a commercial airplane. If a terrorist attack is foiled by any one of these layers of security, then this is viewed as a series system. Assume:

- Probability that a terrorist is successful in avoiding detection by any one of the 10 layers of pre-boarding TSA security is a high 90%.
- Passengers and trained flight crew have a low 50/50 chance of foiling a terrorist attempting to assemble or detonate an IED.
- Imperfect bomb-making training results in high 75% chance of IED detonating successfully.
- Aircraft resilience - a 75% chance of an airliner crashing if a bomb is successfully detonated.

Since there are uncertainties with quantifying these probabilities a sensitivity analysis is conducted later in the paper to assess robustness of results. For a series system where each event probability is statistically independent the probability of airliner loss is

$$\begin{aligned}&\Pr(\text{airliner loss}) = \prod_{i=1}^{10} \Pr(\text{non-detection for preboarding security measure } i)\\&\times \Pr(\text{Passengers/Crew non-detection}) \times \Pr(\text{IED detonates successfully}) \qquad (2)\\&\times \Pr(\text{aircraft downed by IED detonation}) = (0.9)^{10} \times 0.5 \times 0.75 \times 0.75 = 9.8\%\end{aligned}$$

The probability then that the plot is foiled, deterred or disrupted is 1-Pr(airline loss)=90.2% assuming existing security measures. Now, if the additional security measure is AITs, then we assume:

- The probability of this technology in preventing a suicide bomber boarding an aircraft is five times higher than any existing layer of TSA pre-boarding security - i.e., 50%.
- The probability of this technology in preventing a suicide bomber from successfully detonating an IED is 50% because AITs may deter a terrorist from using more reliable, but more detectable, detonator.
- The probability of this technology in preventing an IED from being sufficiently large to down the aircraft is 50%.

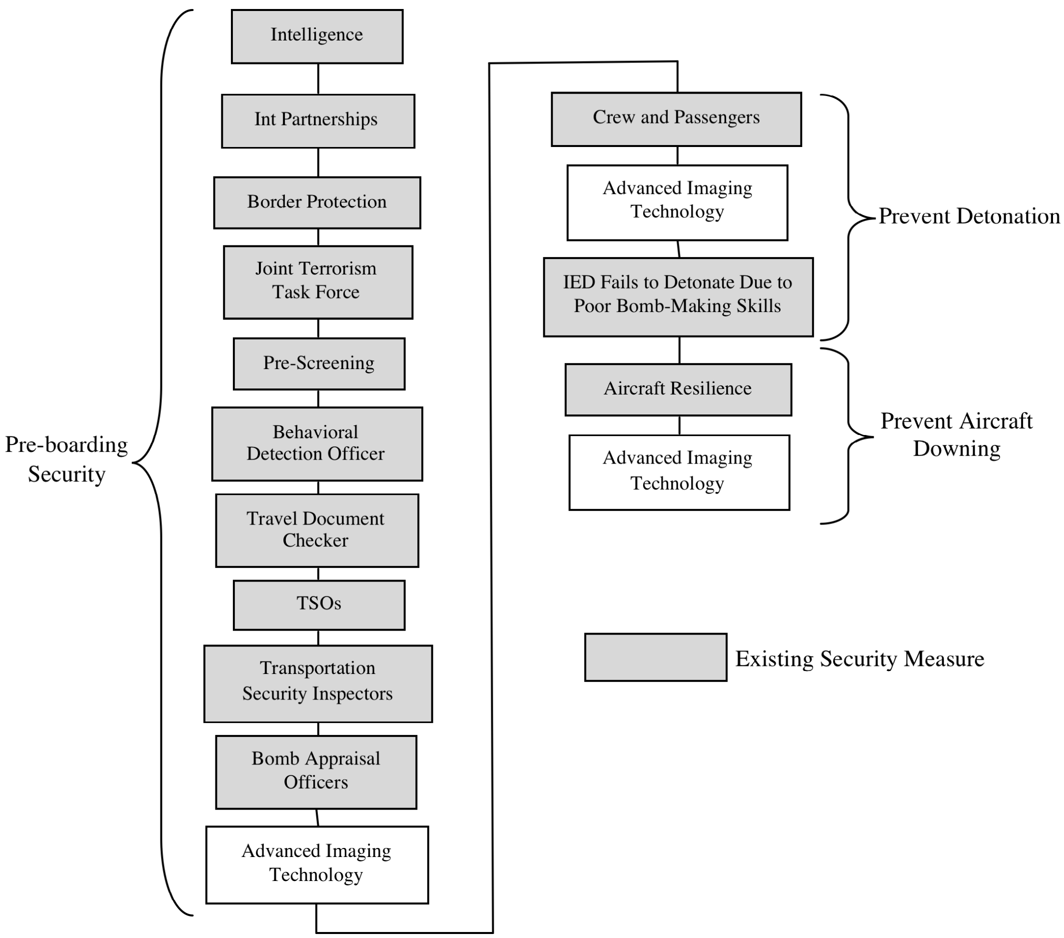


Figure 2. Reliability Block Diagram of Existing (shaded) and Enhanced Aviation Security Measures With Advanced Imaging Technology (AIT).

Again assuming a series system, and since Pr(AIT effectiveness) is 50%, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is $[1\text{-Pr(AIT effectiveness)}]^3=(1\text{-}0.5)^3=12.5\%$ and so probability of airliner loss is now calculated as 9.8%×12.5%=1.2%. Hence, the probability of preventing a terrorist attack and the downing of an airliner is now 100-1.2=98.8% due to AITs. The additional risk reduction from this single security measure is ΔR=98.8-90.2=8.6%. This is the risk reduction in stopping a suicide bomber boarding a plane in the U.S., detonating it successfully or the explosive energy is insufficient to down the aircraft. We have taken conservative assumptions about (i) efficacy of TSA pre-boarding security (only 10% chance of detection), (ii) flight crew and passenger vigilance in disrupting a suicide bomber, and (iii) the would-be terrorist shows more skill and tradecraft than many of his or her compatriots in keeping their plot secret and avoiding detection by the public, police or security services.

Information about risk reductions may also be inferred from expert opinions, scenario analysis, and statistical analysis of prior performance data, as well as system and reliability modeling. Nonetheless, the systems approach to modeling effectiveness of aviation security measures described herein is instructive.

Risk reduction is an uncertain variable. Using the figures above, the best case scenario is that AITs are 100% effective in eliminating this remaining risk then the best case risk reduction is ΔR=9.8%. If AITs are less effective than assumed above, but still twice as effective than any existing layer of TSA pre-boarding security [Pr(AIT effectiveness)=20%], then risk reduction is reduced to 4.8%. Lower and upper bound risk reductions is thus taken as 5% and 10%, respectively. We will also assume three alternate probability distributions of risk reduction (see Figure 3):

1. Normal Distribution - risk reduction is normally distributed with 95% confidence interval between 5% and 10%, then mean risk reduction is 7.5% and standard deviation is 1.3%.
2. Uniform Distribution - equal likelihood of any risk reduction between 5% and 10%, with mean risk reduction of 7.5%.
3. Triangular Distribution - higher likelihood of higher risk reduction bounded by 5% and 10%, with mean risk reduction of 8.3%.

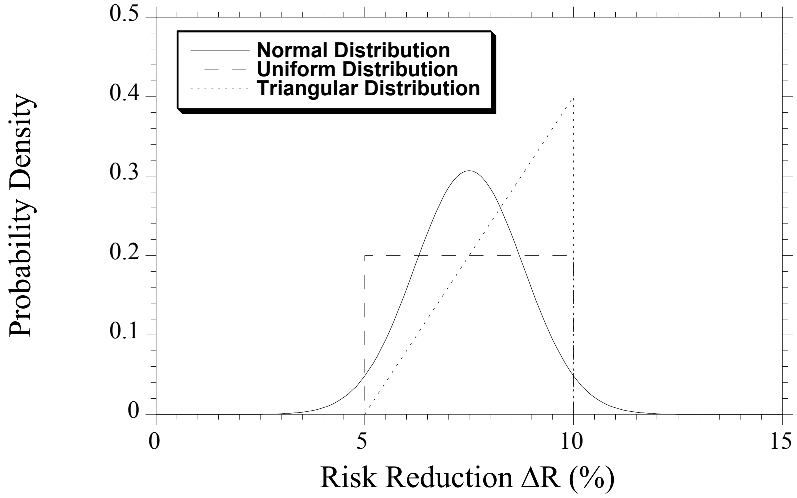


Figure 3. Alternative Risk Reduction Uncertainty Models.

Results

An expected value cost-benefit analysis is one that uses mean values. In this case, the minimum attack probability for full body scanners to be cost-effective is 61.5% per year calculated as $1.2 billion divided by $26 billion in losses divided by 7.5% risk reduction. Thus, full body scanners must deter or foil more than one otherwise successful attack every two years for the security measure to be deemed cost-effective. However, this type of cost-benefit analysis fails to consider the uncertainty of losses and risk reduction - this is now described in the following section. Note that the attack probability is the probability of an attack that originates in the U.S. and the bomber boards an aircraft in the U.S. and not elsewhere. This is an important distinction as the shoe and underwear bombers boarded their aircraft at international locations and not in the U.S.

Uncertainty Analysis

Monte-Carlo simulation analysis is used as the computational tool to propagate uncertainties through the cost-benefit analysis. The analysis assumes that losses and risk reductions are either normally, uniformly or triangularly distributed. If inputs are random variables then the output of the analysis (net benefit) will also be variable and so the probability that net benefit exceeds zero, Pr(cost-effectiveness), can be calculated for any attack probability. Figure 4 shows the probability of cost-effectiveness for attack probabilities from 0.1% to 1,000%. If attack probability is less than 20% per year then there is zero likelihood that AITs are cost-effective and so 100% likelihood of a net loss. On the other hand, if attack probabilities exceed 1,000% or ten attacks per year then AITs are certain to be cost-effective (i.e. Pr(cost-effective)=100%). Clearly, as attack probability decreases then benefit reduces thus reducing net benefit.

The decision problem can be recast another way. In a break-even analysis, the minimum attack probability for AITs to be cost effective is selected such that there is 50% probability that benefits equal cost (see Table 1). However, a decision-maker may wish the likelihood of cost-effectiveness to be higher before investing billions of dollars in a security measure - to say 90% so there is more certainty about a net benefit and small likelihood of a net loss. Table 1 shows the minimum attack probabilities needed for there to be a 90% chance that AITs are cost-effective. For all three uncertainty models, the attack probability needs to exceed 160-330% per year to be near certain that AITs are cost-effective. This means that there is 90% confidence that AITs will pass a cost-benefit analysis if the mean rate of attack is two to three attacks per year originating from U.S. airports. Conversely, Table 1 shows that if attack probability is less than 34-41% per year then there is only a 10% chance of a net benefit, and a 90% likelihood of a net loss. The results are not overly sensitive to the probabilistic models used.

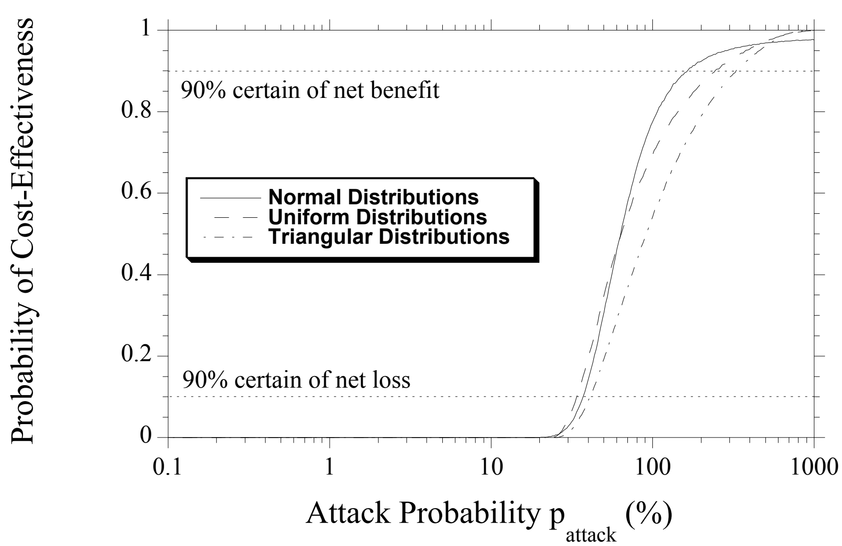


Figure 4. Probability of Cost-Effectiveness (Net Benefit Exceeds Zero).

Table 1. Minimum Attack Probability for AITs to be Cost-Effective.

Loss and Risk Reduction Distributions	Pr(cost-effective)=10%	Pr(cost-effective)=50%	Pr(cost-effective)=90%
Normal	37.2%	63.2%	161.8%[1]
Uniform	34.0%	63.9%	247.7%
Triangular	41.0%	91.2%	330.4%

[1] 1.62 attacks per year

Sensitivity Analysis

While we have tried to err on the generous side - i.e. towards improving the cost-effectiveness of full-body scanners - we recognize that the probability estimates for effectiveness of security measures are uncertain. If the effectiveness of pre-boarding security is reduced, then the additional risk reduction of AITs increases. Hence, assume that effectiveness of pre-boarding security measures is half of those used above (i.e. probability of avoiding detection increases from 90% to 95%), and (ii) effectiveness of AITs increases from 50% to 75% due to, for example, a higher deterrent capability. Then Pr(airliner loss) is 16.8% and 0.3% for existing and enhanced security measures, respectively. The risk reduction is ΔR=16.5%. If AITs are 100% effective then they reduce existing risk to zero and so ΔR=16.8%. Or if we assume that Pr(successful IED detonation) increases from 75% to 100% due to highly skilled and experienced terrorists, then risk reduction is ΔR=11.5%. If we modify the three alternative uncertainty models of risk reduction so that their range is 5-20%, then the attack probability needs to exceed 115-192% for there to be 90% confidence that AITs are cost-effective. A break-even analysis shows that the attack probability needs to exceed 39-53% for AITs to be cost-effective. However, if opportunity costs are considered then this would increase the threshold attack probabilities.

If the lower bound of loss is increased to \$5 billion, then the attack probability needs to exceed 131-201% for there to be 90% confidence that AITs are cost-effective. If the upper bound of loss is doubled to C_{loss}=\$100 billion, then the attack probability needs to exceed 89-209% for there to be 90% confidence that AITs are cost-effective. While doubling risk reduction or losses reduces threshold attack probabilities, they still remain at relatively high levels.

Discussion

The present paper has shown the utility of systems and uncertainty modeling for cost-benefit analysis for homeland security expenditure. The preliminary results suggest that the threat probability - the likelihood an attack will be otherwise successful - needs to be high for AITs to be cost-effective. But we recognize that the preliminary cost-benefit analysis conducted herein will not give a definitive answer to whether AITs are cost-effective. A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in aviation security. This paper provides a starting point for this type of analysis. The assumptions and quantifications made here can be queried, and alternate hypotheses can be tested in a manner which over time will minimize subjectivity and parameter uncertainty inherent in an analysis for which there are little accurate data. This should lead to more widespread understanding and agreement about the relative cost-effectiveness of aviation security measures.

CONCLUSIONS

The paper has developed a preliminary cost-benefit analysis of Advanced Imaging Technologies (AITs) using full-body scanners for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and security costs. Monte-Carlo simulation methods were used to propagate risk reduction and loss uncertainties in the calculation of net benefits, and the minimum attack probability necessary for full-body scanners to be cost-effective were inferred. It was found that, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. The uncertainty modeling also allowed the probability of cost-effectiveness to be calculated. It was found that the attack probability needs to exceed 160-330% per year to be 90% certain that AITs are cost-effective.

REFERENCES

Bayles, F. (1996), 'Planes Don't Blow Up' Aviation Experts Assert, *International Herald Tribune*, July 24, 1996.

BBC News (2010), Boeing 747 Survives Simulated 'Flight 253' Bomb Blast, 5 March 2010.

Blalock, G., Kadiyali, V. and Simon, D.H. (2007), The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel, *Journal of Law and Economics*, 50(4): 731-55.

Blomberg, S.B. and Rose, A.Z. (2009), Editor's Introduction to the Economic Impacts of the September 11, 2001, Terrorist Attacks, *Peace Economics, Peace Science, and Public Policy*, May 2009, 15(2):1-14.

Chow, J, Chiesa, J., Dreyer, P., Eisman, M., Karasik, T.W., Kvitky, J., Lingel, S., Ochmanek, D. and Shirley, C. (2005), *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*, RAND, Santa Barbara, 2005.

Cox, L.A. (2009), Improving Risk-Based Decision-Making for Terrorism Applications, *Risk Analysis*, 29(3): 336-341.

Dillon, R.L., Liebe, R. and Bestafka, T. (2009), Risk-based Decision Making for Terrorism Applications, *Risk Analysis*, 29(3): 321-335.

Ellig, J., Guiora, A, and McKenzie, K. (2006), *A Framework for Evaluating Counterterrorism Regulations*, Policy Resource No. 3, Mercatus Center, George Mason University, September 2006.

Ellingwood, B.R. (2006), Mitigating Risk from Abnormal Loads and Progressive Collapse, *Journal of Performance of Constructed Facilities*, 20(4), 315-323.

Enders, W. and Olsen, E. (2011), Measuring the Economic Costs of Terrorism, In M. Garfinkel and S. Skaperdas eds. *Oxford Handbook of the Economics of Peace and Conflict,* Forthcoming.

Europol (2009), *The Concealment of Improvised Explosive Devices (IEDs) in Rectal Cavaties*, Europol, The Hague, 18 September 2009, p.8

Farrow, S. and Shapiro, S. (2009), The Benefit-Cost Analysis of Security Focused Regulations, *Journal of Homeland Security and Emergency Management*, 6(1):Article 25.

Freidman, B.H. (2010), Managing Fear: the Politics of Homeland Security, in *Terrorizing ourselves: why U.S. counterterrorism policy is failing and how to fix it*, B.H. Friedman, J. Harper, and C.A. Preble (Eds.), Cato Institute, p. 211.

Gordon, P., Moore II J.E., Pak, J.Y. and Richardson, H.W. (2007), The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System, *Risk Analysis*, 27(3): 505-512.

Halsey, A. (2010), All check-points wont get body scanners, *The Washington Post*, December 2, 2010.

Kenney, M. (2010), "Dumb" yet Deadly: Local Knowledge and Poor Tradecraft among Islamist Militants in Britain and Spain, *Studies in Conflict and Terrorism*, 31:1-22.

Lord, S. (2010), *Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Areas of Aviation Security Remain*, United States Government Accountability Office, GAO-10-484T, March 17 2010, p.5

Mueller, J. (2010), Assessing Measures Designed o Protect the Homeland, *Policy Studies Journal*, 38(1), 1-21, February.

Mueller, J. and Stewart, M.G. (2011), *Terror, Security and Money: Balancing the Risks, Benefits and Costs of Homeland Security*, Oxford University Press, October 2011.

NRC (2010), *Review of the Department of Homeland Security's Approach to Risk Analysis*, National Research Council, National Academic Press, Washington.

OMB (1992), *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised)*, Circular No. A-94, October 29, 1992, Office of Management and Budget, Washington, DC.

Poole, R.W. (2008), *Towards Risk-Based Aviation Security Policy*, Discussion Paper No. 2008-23, OECD/ITF Round Table on Security, Risk Perception and Cost-Benefit Analysis, International Transport Forum, December 2008.

Robinson, L.A., Hammitt, J.K., Aldy, J.E., Krupnick, A. and Baxter, J. (2010), Valuing the Risk of Death from Terrorist Attacks, *Journal of Homeland Security and Emergency Management,* 7(1).

Rossides G. (2010), Advanced Imagining Technology - Yes, It's Worth It, *The Blog@Homeland Security*, April 1 2010.

Stewart, M.G., Netherton, M.D. and Rosowsky, D.V. (2006), Terrorism Risks and Blast Damage to Built Infrastructure, *Natural Hazards Review* 7(3):114-122.

Stewart, M.G. and Netherton, M.D. (2008), Security Risks and Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading, *Reliability Engineering and System Safety*, 93(4): 627-638.

Stewart, M.G. (2008), Cost-Effectiveness of Risk Mitigation Strategies For Protection of Buildings Against Terrorist Attack, *Journal of Performance of Constructed Facilities*, ASCE, 22(2):115-120.

Stewart, M.G. and Mueller, J. (2008), A Risk and Cost-Benefit Assessment of U.S. Aviation Security Measures, *J. of Transportation Security*, 1(3):143-159.

Stewart, M.G. (2010), Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure, *International Journal of Critical Infrastructure Protection*, 3(1): 29-40.

Stewart, M.G. (2011), Life Safety Risks and Optimisation of Protective Measures Against Terrorist Threats to Infrastructure, *Structure and Infrastructure Engineering,* 7(6): 431-440.

Sunstein. C.R. (2002), *The Cost-Benefit State: The Future of Regulatory Protection*, ABA Publishing, American Bar Association, Chicago.

TSA (2010), Passenger Screening Program: Program Specific Recovery Act Plan May 24 2010, Department of Homeland Security, Washington, DC, p.3

Willis, H. and LaTourette, T. (2008), Using Probabilistic Terrorism Risk-Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment*, Risk Analysis* 28:325.

von Winterfeldt, D. and O'Sullivan, T.M. (2006), Should WE Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists?, *Decision Analysis*, 3(2): 63-75.

VERSION - JUNE 23, 2013

FREEDOM TO TRAVEL USA

(http://fttusa.org)

Response to TSA NPRM Document ID TSA-2013-0004-0001

" If Tyranny and Oppression come to this land, it will be in the guise of fighting a foreign enemy."
- James Madison

"Those who would give up essential Liberty, to purchase a little temporary Safety, deserve neither Liberty nor Safety"
- Benjamin Franklin

"Never doubt that a small group of thoughtful, committed people can change the world. Indeed, it is the only thing that ever has."
- Margaret Mead

"Freedom To Travel USA" is a group of US citizens who are concerned about the actions of the Transportation Security Administration (TSA). We live all across the United States and are of many different political persuasions. We could comfortably live our lives without worrying about the TSA, but the TSA represents a federal agency that is, every day, violating the rights embodied in the US Constitution for which hundreds of thousands of Americans have died. If the TSA is not confronted now, the United States in which our children are growing up will be a more unpleasant place.

We hope you read this document with an open mind, arrive at the same conclusions we have, and join us in restoring our rights and our dignity while traveling.

Contents

Executive Summary

The intent of this document is to provide Freedom To Travel USA's public response to the TSA NPRM Document ID TSA-2013-0004-0001. The Notice of Public Rule Making was forced on the TSA by Court Order (http://epic.org/privacy/body_scanners/EPIC_v_DHS_Decision_07_15_11.pdf) .

Freedom To Travel USA (FTTUSA) has deep awareness and expertise about the TSA's unconstitutional Nude Body Scanners and the criminal pat downs which are an integral part of the Nude Body Scanner program. Our organization has supported cancer victim Sharon Cissna on her trip to a state legislature convention, given a briefing at Capitol Hill, and presented oral arguments just recently, in April 2013, to the 1st Circuit Court of Appeals in a rarely granted Amicus appearance concerning the TSA's Nude Body Scanner program.

In response to its unlawful deployment of Nude Body Scanners (NBS), the TSA has proposed the following addition to the Federal Code of Regulations (FCR):

> *Proposed Addition in § 1540.107, add paragraph (d) to read as follows:*
>
> *(d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.*

Freedom To Travel USA's evaluation shows the suggested rule is **useless, unnecessary, and unresponsive to the Court order**. It **fails to protect the Constitutional rights of Americans** and **does not adequately address or prevent the abuses which have unarguably occurred ALREADY** since the Nude Body Scanners and criminal pat downs have been deployed unlawfully for over two and half years now.

Conclusions

Our **conclusions** are that the proposed TSA rule is…

- ✓ Useless and unnecessary because the TSA already has the authority to conduct screening generally and it ALREADY has no current prohibition against using technology without requiring physical contact. The Walkthrough Metal Detectors (WTMDs) do not make physical contact and have been widely used for decades.
- ✓ Unresponsive to the Court order because the proposed NPRM rule does not address Nude Body Scanners in the submitted change for the FCR. The submitted documents do discuss the current Nude Body Scanner technology, but the proposed rule change does not address scanners specifically. The NPRM also does not address any proposed limits on the technologies, for example, such as the use of ATR software which was a legislative change initiated by Congress.

The proposed rule ignores this current Congressional restriction on the defined "advanced imaging technology"; as written, is wholly inadequate to meet the Court's order.

✓ Violating Americans' inalienable rights as protected by the United States Constitution's 4th Amendment because the TSA is conducting dragnet, administrative searches **without detecting weapons, explosives, or incendiary devices at the end of the initial search**.

Quite simply, the proposed "concealed anomalies" wording is **too broad and unreasonable.** Even when using the "ATR" technology, which does not display the nude images, this technology CANNOT identify what exactly it "thinks" it found. **At the end of the ATR search, there is ZERO identification that a weapon or explosive was found. There is ALWAYS a secondary search based on any number of reasons that a person's outline does not conform to a vague and unspecified "normal"**. The Nude Body Scanner ATR search is an **entirely new level of search never before performed in the United State of America** ; essentially, the Nude Body Scanner's search **falsely establishes** suspicion for further searching because it cannot, by current definition, positively identify objects it is supposed to be searching for! According to the TSA documents in the NPRM, the scanner deployment already existing affects **HUNDREDS OF MILLIONS OF AMERICANS – EACH YEAR**.

It is unreasonable to accept a search which has a 0% success rate at identifying objects which the search is intended to find, while simultaneously "identifying" millions upon millions of false positives.

✓ Violating all Americans' PRIVACY and ***especially*** profiling the medically disabled because ALL of the deployed scanner technology – AIT with and without ATR – leads to millions of secondary searches each year due to false positives and detecting "concealed anomalies" which are NOT weapons, explosives, or incendiary devices.

The secondary searches violate ALL Americans' privacy because they often involve criminal pat downs which are **coerced touching of female breasts, vulvae (female external sex organs), penises, testicles, and buttocks**. This unwanted touching is **a criminal act in ALL 50 states** when performed in any other context by anyone, including truly authorized law enforcement staff.

Make no mistake – this is coerced touching as a traveler does not know if they will be subject to a criminal pat down before they start airport screening. Then, when the screening starts, there are possible legal penalties (administrative fines or possible arrest) for avoiding pat downs, in addition to the real threat to one's freedom to travel within the United States, a freedom defined in the 5th Amendment's use of the word "liberty" in several court cases. The right to traverse the airspace is also embodied in the FCR.

Another violation of American's privacy is that those with medical conditions such as mastectomy patients, diabetics, colostomy patients, amputees, and other medical issues are "profiled" at a higher (100%) rate for further secondary screening when compared to those without medical issues.

HISTORICAL RECORD OF PRIVACY VIOLATION OF PASSENGERS WITH MEDICAL CONDITIONS

The proposed TSA NPRM Rule has already been active and used in the United States for two and a half years so we can measure its effectiveness. Freedom To Travel USA respectively submits the following two incidents, out of many thousands of documented complaints (ACLU, EPIC, TSA Complaint Forms, and Google Searchable on the Internet) since the proposed rule has been in effect.

Beginning Time Line Incident: LATE 2010

http://www.huffingtonpost.com/2011/02/24/rep-sharon-cissna-tsa_n_827934.html

This State Representative received a sexual assault pat down AFTER going through a Nude Body Scanner. Her mastectomy scar was the apparent threat that required further investigation. When she encountered the SAME situation, she decided to take a stand. Reading the article from February, 2011, one will see that she already had the same experience 3 months earlier, in late 2010. The article also relates over 1,000 complaints by passengers.

Ending Time Line Incident: MAY, 2013 DURING THIS PUBLIC COMMENTING PERIOD!

http://www.kens5.com/news/Woman-with-prosthesis-claims-TSA-agent-made-her-feel-uncomfortable-210892231.html

This cancer victim had her false breast examined and touched after going through a Nude Body Scanner. **Her private medical condition was forcibly revealed** by an AIT screening.

Privacy is more than looking at naked pictures by voyeuristic TSA agents. It is also invaded by the most invasive inch-by-inch searches of one's body, no matter how it is done, whether through physical contact or not! Privacy is also invaded by being forced to share personal secrets that are not otherwise observable in public - – especially sensitive medical and transgender issues.

It is OBVIOUS that the TSA implementation of the proposed rule results in invasion of privacy since the "anomalies" continually detected millions of times a year lead to invasion of privacy and criminal acts in all 50 states.

It is OBVIOUS the TSA implementation of the proposed rule has ALREADY repeatedly violated privacy through suspicionless Nude Body Scanners – for the ENTIRE TIME of their existence.

Freedom To Travel USA –Reasons For Changes To The Proposed Rule

Because we contend **any primary screening, without reasonable, articulable suspicion, which examines the entire body of a passenger is unconstitutional**, Freedom To Travel USA suggests a more restrictive PREFERRED rule which actually addresses the Nude Body Scanners as requested by the Court.

We are also suggesting a MINIMUM ALTERNATIVE change to the proposed NPRM rule to bring it closer to previous Court decisions and accepted administrative search doctrine. The critical principles and reasons for the suggested rule or any changes are as follows:

a) **Better alignment with previously approved administrative searches under the 4th Amendment**

The current reality of the NPRM rule is that the TSA has implemented the most invasive, general searches of any travelers at any time in our country's history, affecting hundreds of millions of Americans each year. As we documented, the molestation and criminal pat downs – direct results of the implementation of AIT – have led to thousands of invasions of privacy.

In the context of balancing the security benefits to the overwhelmingly documented invasions of privacy – just as newsworthy in May, 2013 as they were newsworthy back in late 2010 – we submit the following facts on the effectiveness of identifying non-metallic liquid and powder bomb threats:

- **FACT 1**: The number of discovered non-metallic bombs carried by suicidal airline passengers on US domestic flights SINCE the AIT Nude Body Scanners were implemented: **Zero**

- **FACT 2**: The number of fatalities caused by airline passengers with working non-metallic bombs on US domestic flights in the LAST 50 YEARS (and the 47 years BEFORE AIT): **Zero**

- **FACT 3**: The GLOBAL number of fatalities caused by airline passengers with working non-metallic bombs - covering 402,800,813 commercial flights and 34,487,566,845 passengers - in the entire world since 1980: **Two**

(SOURCE**:** Manual curation of data from www.iata.org, www.bts.gov ,http://aviation-safety.net)

In essence, **the introduction of AIT has NOT measurably increased security** (due to AIT) as there has been **no change** in the rate of airline passenger non-metallic bombings on US domestic flights when compared to the 47 year period prior to AIT deployment.

Because the whole intent of the AIT Nude Body Scanners is to stop suicidal airline passengers with working non-metallic bombs on US domestic flights, the documented, nearly immeasurable risk dictates there should be a strong interest in maintaining the rights of individuals. The NPRM does not take any reasonable analysis of the risk into its wording.

The TSA has never found one passenger with intent to kill other passengers, and has never found one instance of non-metallic explosives with AIT, and has never identified one instance of preventing a viable working non-metallic bomb with AIT. Yet, the currently deployed AIT technologies under this NPRM has substantially impacted millions of Americans by forcing hundreds of millions of inch-by-inch body searches, a substantial subset of which have led to many privacy violations. Simply put, those with medical issues are unusually singled out as the "**sacrificial lambs**" under the AIT technologies deployed under this NPRM rule already. And, many able-bodied Americans have also found themselves subjected to gross violations and criminal pat downs as a result of the Nude Body Scanner introduction.

b) **Better alignment with other search technologies' effectiveness**

The current wording of "anomalies" is completely misleading. The NPRM documents talk about what Congress has authorized in the following:

FROM TSA NRPM DOCUMENT (Section C): "The Secretary of Homeland Security shall 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"

The main problem with the AIT currently deployed as would be officially permitted WITHOUT CHANGE to the NPRM rule is that it detects….NOTHING.

A stopped watch is right twice a day. That is better than the current AIT scanners, with ATR technology, which **cannot identify** any "nonmetallic, chemical, biological, and radiological weapons" when their search is complete. There is ALWAYS a further search.

For example, the AIT Nude Body Scanners do NOT detect explosive materials; they just use software to find "anomalies", which are mathematically-determined discrepancies to some assumed parameter of what the human body looks like. And, when the scanners identify something real, it often leads to more PRIVACY INVASIONS such as exposure of medical conditions (mastectomy scars, prosthetics (breast or limb), medical devices (colostomy bags, insulin pumps, back braces), and unusual sex organ characteristics as has been reported.

Contrast this with Walkthrough Metal Detectors (WTMDs). They nearly always find metal – which is the goal of their search. There may be a secondary screening to identify what kind of metallic object was identified, but WTMDs identify a metal object. They don't overwhelmingly "alarm" at a high rate on non-metallic objects, or medical devices, or colostomy bags, or false breasts. No reasonable person would put up with WTMDs that always alarmed on paper, rubber bands, or plastic buttons.

Or, consider blood alcohol tests. They are highly correlated with finding the blood alcohol level and nothing else. They don't first identify the possible presence of AIDS, Hepatitis, or Leukemia and depend on a secondary test to measure blood alcohol levels. In short, they find what they are looking for at nearly 100% effectiveness.

The AIT, permitted under the proposed NPRM rule, has already proved it is wholly inadequate to 'detect[s] nonmetallic, chemical, biological, and radiological weapons, and explosives' at the end of its search**. In fact, unlike any other search technology, it is a universal failure at identifying what it is supposed to find despite hundreds of millions of searches each year**.

c) Better alignment with Americans' opinions

Quite simply, a majority of Americans are against Nude Body Scanners and the associated criminal pat downs which result in invading privacy. From 2010, we measured a New York Times article comments section. The New York Times Op-Ed by Maureen Dowd (http://www.nytimes.com/2011/04/20/opinion/20dowd.html , NY Times, April 19th, 2011) generated many comments. Out of all the comments on this article, 61 out of 377 were Pro-TSA, which makes **83% against the current TSA procedures**. [NOTE: One of the authors of this document read every comment to arrive at the numbers]. Clearly, out of the people who care by voicing their opinion, there is an overwhelming majority AGAINST AIT for primary screening.

But, we don't have to depend on an early opinion to measure how Americans feel about this subject. Freedom To Travel USA **suggests the government COUNT UP THE OPINIONS – for and against – THAT ARE SUBMITTED FOR THIS NPRM**. That will give you the answer concerning the despicability of this wholly inadequate and unnecessary rule.

Freedom To Travel USA –Suggested Changes To Proposed Rule

Freedom To Travel USA suggests two alternatives to the proposed NPRM rule. We have provided template wording which can be easily fit into the FCR format by the appropriate government agency.

PREFERRED ALTERNATIVE

The purpose of the preferred alternative is to clearly restrict the most invasive general search, using advanced imaging technology, ever offered for non-law enforcement purposes. It is modeled after legislation introduced by Rep. Rush Holt (D – New Jersey) and Rep. Jason Chaffetz (R - Utah) in 2011.

This rule preserves the idea of reasonable, articulable suspicion based on previous information prior to fully examining one's body; this maintains some integrity of the 4th amendment. This is analogous, for example, to the Supreme Court ruling against a search of one's house using thermal scanning unless there is prior suspicion. **The same concept should apply equally to one's person, since there are no house-by-house, warrantless administrative searches for illegal weapons allowed by law in the United States.**

Proposed Addition in § 1540.107, add paragraph (d) to read as follows:
(d) The screening and inspection described in (a) may only include the use of advanced imaging technology under the following conditions:

(1) ADVANCED IMAGING TECHNOLOGY.—Advanced imaging technology may not be used as a method of screening a passenger under this section unless—
(A) the National Academy of Sciences determines that the technology poses no threat to public health;
(B) the technology is equipped with a privacy filter or other privacy-protecting technology; and
(C) another method of screening, such as metal detection or explosive trace detection, demonstrates reasonable cause for utilizing advanced imaging technology to detect a possible threat to aviation security. "Reasonable Cause" as used herein is defined in the same manner, and shall carry the same legal restrictions, as for sworn Law Enforcement Officers.

(2) ENHANCED PAT-DOWN SEARCHES.—An enhanced pat-down search may not be used as a method of screening a passenger under this section unless another method of screening, such as metal detection or explosive trace detection, or use of advanced imaging technology in accordance with paragraph (1), demonstrates reasonable cause for utilizing advanced imaging technology to detect a possible threat to aviation security . "Reasonable Cause" as used herein is defined in the same manner, and shall carry the same legal restrictions, as for sworn Law Enforcement Officers.

(3) PROVISION OF INFORMATION.—A passenger for whom screening by advanced imaging technology is permissible under paragraph (1) shall be provided, prior to the utilization of such technology with respect to such passenger, information on—
(A) the operation of such technology;
(B) the image generated by such technology;
(C) privacy policies relating to such technology;
(D) the right to request an advanced pat-down search under paragraph (5); and
(E) the right to view the actual generated whole-body image of their person.

(4) PAT-DOWN SEARCH OPTION.—A passenger for whom screening by advanced imaging technology is permissible under paragraph (1) shall be offered an advanced pat-down search in lieu of such screening.

(5) PROHIBITION ON USE OF IMAGES.—An image of a passenger generated by advanced imaging technology may not be stored, transferred, shared, or copied in any form after the boarding determination with respect to such passenger is made.

MINIMUM ALTERNATIVE

The purpose of the minimum alternative is to "at the least" bring AIT to the same general effectiveness level as other technology searches. To be precise, AIT needs to identify specific threats at the end of its search – not just the presence of something with zero correlation to a threat characteristic.

Proposed Addition in § 1540.107, add paragraph (d) to read as follows:

(d) The screening and inspection described in (a) may include the use of advanced imaging technology under the restrictions in subparagraphs (1), (2), and (3). For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed items without requiring physical contact with the individual being screened.

(1)) AIT cannot be a general search for identifying anomalies, but must instead search for weapons, explosives, and incendiary items specifically

(2)The advanced imaging technology search MUST have a highly effective rate at specifically identifying the items for the search is intended.

(3) AIT cannot generate a high rate of false positives OR misidentification of "alarmed" items, such that a secondary screening reveals that specific item(s) searched for were not found

POST-NPRM Request for Legal Action To Restore America's Freedoms

We ask that all concerned legislators and citizens join **Freedom To Travel USA** (http://fttusa.org) in restoring freedoms in our great country and to stand up against the fear of terrorism, instead of helping terrorists "win" by changing the nature of America.

Our goals are to restore legal airline passenger security, reinforce our constitutional rights against warrantless, unreasonable searches, and promote dignified procedures for those with medical issues.

The elected officials sworn to uphold the United States Constitution should be strongly supportive of the freedoms that make America a great country, and should not be afraid to preserve these constitutional rights as well as common decency for citizens. The **specific legislative goals** for airport security that we support and are asking you to support are:

- ✓ Provide for airline passenger screenings using **long-standing and effective legal means** which existed prior to strip search scanners and sexual assault pat downs, specifically magnetometer (metal detector) screening. We also support effective explosive detection technology, “bomb sniffing” dogs, and cargo screening for passenger flights.
- ✓ **Forbid primary screening strip searches** (including searches using Nude Body Scanners) of U.S. citizens, including children, except that law enforcement officers may perform strip searches under current legal authority and circumstances. This means no Nude Body Scanners that perform inch-by-inch searches of a traveler’s body.
- ✓ **Forbid physical searches** of U.S. citizens, including children, except that law enforcement officers may perform physical searches under current legal authority and circumstances. This means *no “TSA pat downs”*, which are criminal touching under ANY other circumstance, for primary screening.
- ✓ We are especially **concerned** that U.S. citizens who are in wheelchairs or with ‘medical metal’ – think of metal joint replacements (knee, hip, and surgery metal), artificial limbs, and similar medical issues - are currently profiled 100% of the time by strip search scanners and sexual assault pat downs. We propose a pre-flight clearance procedure be developed that will protect those with medical assistive devices from needing to violate their privacy rights in order to exercise their right to travel.

ADDENDUM: Comments From FTTUSA Media Kit

FTTUSA has excerpted some background comments from our Media Kit, which was released prior to the Congress forcing the TSA to use ATR filters.

NOTE: The proposed rule under this NPRM would allow graphic, naked pictures.

4th Amendment

The United States Transportation Security Administration (TSA) formally announced, in November 2010, that it would move forward with an aggressive implementation of "pat-downs" and "full-body scans" using Advanced Imaging Technology (AIT), formerly called 'whole body imaging' (the original name was changed by the TSA after a couple of months in order to project a less intrusive connotation in their official documents.)

NOTE: We have promised not to use hyperbole, but please be aware that we will use the following terms as we feel they **EXACTLY describe** – no more and no less – the TSA procedures fairly and accurately.

Strip Search Scanners – these are what the TSA refers to as AIT scanners. From www.merriam-webster.com , the definition of "strip search" is "a search for something concealed on a person made after removal of the person's clothing". The AIT scanners use technology to remove your clothing; no matter how convenient in terms of your time and effort, it is a strip search procedure and exposes your naked body to a government stranger.

Sexual Assault Pat Down – this is what the TSA refers to as "pat down". Laws vary from state to state, but we have used one of our largest states, California, to define "sexual assault". An excerpt from http://www.ehow.com/about_6623976_definition-california-law-sexual-assault.html is that "sexual assault is defined as a non-consensual sexual act. Sexual assault includes ….. unwanted touching on an intimate area of a person's body." We do acknowledge that criminal sexual assault often includes intent of the perpetrator, but we hope that you would agree that anyone touching your intimate areas without your consent is inappropriate at the least.

Naturally, many US Citizens who value all of our rights – as enumerated in the United States Constitution - questioned these new procedures. They became alarmed that our 4th amendment rights were being infringed upon by the aggressive TSA policy.

To be clear, the 4th amendment is:

"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

We do not expect you to go to law school and study thousands of pages of legal cases and opinions. However, it is important to clarify some of the history of airport security screenings, the legal cases behind it, some interesting analogies and facts on security risks, and the implications for maintaining and securing the basic rights of US citizens.

History of Administrative Searches

The idea of an "administrative search" has its genesis in the rights of cities to conduct searches necessary to promote public health and safety. For example, cities have traditionally been able to inspect dwellings to see if they conform to fire codes, for it is clear that dangerous conditions may lead to endangering the lives of others in the surrounding buildings. An often referenced case is ***Camara vs Municipal Court and City of San Francisco*** (http://openjurist.org/387/us/523). The result of this case upheld that government can institute "administrative searches" as long as they are general schemes and it also said the defendant had the right to require an administrative warrant before his premises could be entered. Essentially, the public safety concerns supported the administrative search, and in this case the city STILL had a requirement to get a warrant because that did not substantially make it impractical to carry out inspections since most people agreed to inspections.

History of Airport Screenings

There was a time when United States airports did not have any substantial security screening processes. However, in the late 1960s, the incidences of hijackings increased substantially and alarmed the government, public, and aviation industry. We quote from a legal decision , ***United States vs Davis***, which we will explore in more detail:

"Between 1961 and 1968, hijackings of United States aircraft averaged about one per year. In 1968, however, the number rose to 18. In 1969 there were 40 attempted hijackings of United States aircraft, 33 successful."

The government continued to refine screening requirements, and by 1972 the standard system we are familiar with was instituted and has been the backbone of our security ever since. Quoting again:

"On December 5, 1972, the FAA ordered that searches of all carry-on items and magnetometer screening of all passengers be instituted by January 5, 1973."

United States vs Davis

In 1971, a passenger was arrested and fined for having a gun in his briefcase. The passenger argued that the gun was found illegally based on his circumstances. Eventually, this case (http://openjurist.org/482/f2d/893/united-states-v-davis) made it to the United States Courts of Appeal, Ninth Circuit and has been an oft-cited case for transportation security. We invite you to read the link for details, and we have extracted the salient assertions from this lower-level (not Supreme Court) court ruling:

- The essential basis of airport screenings is based on an administrative search.
- The Ninth Circuit Court of Appeal stated:

  ” The essence of these decisions is that searches conducted as part of a general regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation to secure evidence of crime, may be permissible under the Fourth Amendment though not supported by a showing of probable cause directed to a particular place or person to be searched.

  As we have seen, screening searches of airline passengers are conducted as part of a general regulatory scheme in furtherance of an administrative purpose, namely, to prevent the carrying of weapons or explosives aboard aircraft, and thereby to prevent hijackings. The essential purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all”
- The court was clear when it said: “It follows that airport screening searches are valid only if they recognize the right of a person to avoid search by electing not to board the aircraft.” NOTE: The reason for this is that the search would be elevated to a criminal search and thus require a warrant; so the intent of the search cannot be to prosecute a crime. They further conclude “In sum, airport screening searches of the persons and immediate possessions of potential passengers for weapons and explosives are reasonable under the Fourth Amendment provided each prospective boarder retains the right to leave rather than submit to the search.”
- The court concluded about the right to travel: “This Court long ago recognized that the nature of our Federal Union and our constitutional concepts of personal liberty unite to require that all citizens be free to travel throughout the length and breadth of our land uninhibited by statutes, rules, or regulations which unreasonably burden or restrict this movement."
- The Ninth Circuit Court also stated: “These doctrines dictate a critical examination of each element of the airport security program to make certain that neither the passenger's right to travel nor his right to personal privacy is burdened beyond the clear necessities of current circumstances.

  As we have seen, however, the need for some limitations upon these rights is clear. In light of that need, a screening of passengers and of the articles that will be accessible to them in flight does not exceed constitutional limitations provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to fly.”

- This particular case is about the current state of the proposed administrative search and the court offered: "To pass constitutional muster, an administrative search must meet the Fourth Amendment's standard of reasonableness." Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." Camara v. Municipal Court, supra, 387 U.S. at 536-537, 87 S.Ct. at 1735.

  The need to prevent airline hijacking is unquestionably grave and urgent. The potential damage to person and property from such acts is enormous. The disruption of air traffic is severe. There is serious risk of complications in our foreign relations."

Discussion of United States vs Davis

We have several comments about what was written by the lower court.

1) The idea of an administrative search arose originally from property searches. However, the warrantless search of a "person" has been carved out in several legal cases under the administrative doctrine, such as when preventing the spread of communicable diseases. We do not think the courts will overturn the administrative search doctrine as it applies to general security screenings.

2) We think the court contradicts itself when it says "screening searches of airline passengers are conducted as part of a general regulatory scheme in furtherance of an administrative purpose, namely, **to prevent the carrying of weapons or explosives aboard aircraft**, and thereby to prevent hijackings. The essential **purpose of the scheme is not to detect weapons or explosives or to apprehend those who carry them**, but to deter persons carrying such material from seeking to board at all".

   Frankly, it is twisted logic to say the purpose of equipment to detect explosives is not to detect explosives, but to stop persons from having explosives. How else would one prevent the carrying of explosives unless one put in equipment to detect explosives? The actual effect is that you are still looking to detect explosives. Regardless of the express purpose, we do not believe weapons detection and explosive detection will be stopped.

3) The court reaffirms a passenger's right to leave as an alternative. The TSA disagrees on when your consent to search is given. Our research on actual incidents shows inconsistency in written policy and practice. For example, the written policy is that you consent when you stand in a security line after having your boarding pass checked. Yet, Alaskan State Senator Sharon Cissna was allowed to leave the airport without completing a scanner strip search and subsequent sexual assault pat down, although she had entered a security line. She was not arrested , nor was she fined $11,000 as is threatened by the TSA.

We do believe if you are in line for a metal detector for example, and then a Transportation Security Officer (TSO) asks you to go through a strip search scanner, you have the right to refuse and leave.

4) We agree with the right to travel. It should be noted that it can be argued that airline travel is a unique form of transportation which has grown to be a significant requirement to conduct business, to maintain physical relationships with family and relatives, and to go on leisure vacations. There is no alternative to covering significant distances in such a short time frame. For this reason, the restrictions on airplane travel should be **especially scrutinized** for impact to our citizens.

5) A main TSA argument put forth concerning strip search scanners is based on the 1973 lower court opinion which stated "…-screening…does not exceed constitutional limitations provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose…"

   We think this bears some discussion. The original opinion is based ONLY on magnetometer technology which was available at the time of the decision. At no time was a strip search contemplated as the standard primary screening, despite the fact that an explosive like PETN had been around since the early 1900s and was used by the Germans as early as World War 1.

   Apparently, the decision had been made decades ago to forego strip searches of airline passengers, despite the presence of non-metallic explosives. Is this because of the enhanced time to perform the physical search or the intrusion on privacy by forcing airline passengers to show their naked bodies to government strangers?

   Regardless of the answer, the new strip search scanners are completely different technologies with a different level of intrusiveness from magnetometers.

6) What the TSA does not state, is the lower court also said: "These doctrines dictate a critical examination of each element of the airport security program to make certain that **neither the passenger's right to travel nor his right to personal privacy is burdened beyond the clear necessities of current circumstances**.

   The necessities of current circumstances were 33 successful hijackings out of 40 hijackings in one year. We will discuss today's necessities based on non-metallic explosives in the RISKS sections. Clearly, we do have a right to travel and the lower court recognized a right to personal privacy.

7) Which leads us to what is probably the major issue concerning the "doctrine" of administrative searches. The reference to the Camara case said: ' "To pass constitutional muster, an

administrative search must meet the Fourth Amendment's standard of reasonableness." Unfortunately, there can be no ready test for determining reasonableness other than by balancing the need to search against the invasion which the search entails." Camara v. Municipal Court, supra, 387 U.S. at 536-537, 87 S.Ct. at 1735.'

There are really two parts to "carving out" the 4th Amendment. One is to measure the "need to search" and the other is to measure the "invasion" which the search entails. The former is the security risk, and the latter is the method of the search.

The assertion in the Camara case is that **even an administrative search must meet the standard of reasonableness**. The issue in the Camara case was that a gentleman had his private domicile searched without a warrant as we discussed earlier. The point is that if an administrative search is allowed to be conducted without a warrant, it must still meet the standards of the 4th amendment.

NPRM Ignores Body Images, Yet TSA Scanners Are "Strip Searches"

Our society has an expectation of privacy, especially of our bodies. This is why we wear clothing in public, why we break laws when we expose our bodies without clothing, and why TV stations are subjected to large fines for displaying nude bodies. Our teachers do not teach in the nude, our government does not make a government job contingent on working without clothes, and we have voyeurism laws against strangers viewing one naked without one's permission.

Furthermore, we teach our children to "not let strangers touch you" from an early age. Also, generally we do not share nude pictures of our children with strangers. There are laws against unwanted touching by strangers, especially touching of a sexual nature. Again, there is a well-established custom and expectation of privacy for ourselves and especially for our children.

In the (www.epic.org) EPIC vs DHS lawsuit, EPIC notes:

' "The desire to shield one's unclothed figure from view of strangers, and particularly strangers of the opposite sex, in impelled by elementary self-respect and personal dignity," said the U.S. Ninth Circuit Court of Appeals in 1958. The law of privacy, according to a federal judge in California in 1976, "encompasses the individual's regard for his own dignity; his resistance to humiliation and embarrassment; his privilege against unwanted exposure of his nude body and bodily functions." Both courts were discussing dignity in prisons, even though other rights of privacy are not accorded inmates. '

Meanwhile, the TSA has tried to make strip search scanners a mandatory tool of airport screenings. The strip search scanners completely violate our expectations of privacy and customs and are applied to travelers who are not under arrest or even under the remotest suspicion. The TSA website describes the strip search scanners (http://www.tsa.gov/approach/tech/ait/faqs.shtm) as "..advanced imaging technology..screens passengers..for..threats..concealed under a passengers' clothing." The TSA clearly is performing a search after removing your clothing, and in fact, they are "..highly confident in its detection capability."

We agree with the TSA that they take images of your naked body. On April 15th, 2008 the TSA blog (http://blog.tsa.gov/2008/04/first-significant-deployment-of.html) suggested that "These images are friendly enough to post in a preschool. Heck, it could even make the cover of Reader's Digest and not offend anybody." Since that time, the TSA has made it clear the images are invasive to the point that "The officer who views the image is remotely located in a secure resolution room." according to the TSA FAQ (Frequently Asked Questions). Although actual high-resolution photos have not been released, a sample low-resolution photograph is shown below from the EPIC vs DHS lawsuit discovery.

The actual detection capabilities highlighted by the TSA include the comment (http://blog.tsa.gov/2010/03/advanced-imaging-technology-yes-its.html?commentPage=4): "Using AIT, our officers are finding things like small packages of powder-based drugs hidden on the body. When I say small, I mean that one packet was smaller than a thumb print." So, the images we have obtained obviously are not at the quality level hinted at in the TSA statement.

One consequence of the graphic nature of the strip search scanner images is that a Miami TSA worker assaulted a co-worker after his coworkers made fun of the size of his genitalia after he walked through a strip search scanner during training (http://www.nbcmiami.com/news/local/TSA-Fracas-After-Body-Scanner-Reveals-TMI-92971929.html). Another incident occurred in London (http://news.bbc.co.uk/2/hi/uk_news/england/london/8584484.stm)when a female security agent accidentally (NOTE: Apparently, the people using the scanners know they completely invade privacy) entered a scanner, and was subsequently harassed by a male coworker.

Let there be no doubt about the intrusiveness of the strip search.

The intrusive strip searches used by the TSA are not even allowed for police. The police may perform strip searches on prisoners, or in certain circumstances on people under arrest. There is some debate, even within the courts, on what offenses and in what conditions police may strip search people under arrest. For example, people under arrest for jaywalking, failure to pay a parking ticket, and other misdemeanors may not necessarily be strip searched. **One would think that a non-law enforcement agency could not use methods, which are prohibited to police, on people who are not under arrest.**

Sexual Assault Pat Downs

It is a little known fact that a passenger is not required to go through a strip search scanner – the TSA offers an "opt out" to have your person searched. As previously stated, this is not the "pat down" you might get at a sporting event where they touch your outer clothing to feel for prohibited items such as alcohol containers. Instead, the Transportation Security Officer (TSO) follows a secret procedure that has not been made public. We can assure you that the procedure includes having a TSO touch your genitals and breasts – if you searched your neighbors and your neighbors' children this way for potential weapons when they visited your house, you would be arrested.

In another Supreme Court decision *Terry vs State of Ohio* (http://openjurist.org/392/us/1/terry-v-state-of-ohio), the Supreme Court ruled that police are allowed to "frisk" potential suspects, even if not under arrest, based on the potential for an immediate threat of injury or death to a police officer. Under the administrative search doctrine, the TSA is asserting the government right to perform a "Terry frisk" without remotely reaching the relaxed 4th amendment standards that the Supreme Court carefully laid out in this decision. It is important to note that the Supreme Court justified the frisk method based on the fact that many officers were killed every year by people with hidden weapons. A police frisk should not be allowed by non-law enforcement government workers, especially using more relaxed standards than those which police must follow.

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-4962

Tracking Number: 1jx-862q-cb44

Document Information

Date Posted:
Jul 1, 2013

RIN:
1652-AA67

Show More Details

Comment

It's sad what has happened to this country. At our airports, train stations, subway stations, etc., the TSA treats us all like criminals. We're assumed to be terrorists, strip-searched and patted down until we prove our innocence. This is backwards. The Fourth Amendment stipulates that there must be "probable cause" to search and seize, and all we've done is buy a plane ticket. I should not have to pose for a naked picture or undergo a sexual assault in order to get on an airplane. The TSA workers bark orders at us, bully us, shuffle us through lines like cattle, pose us like mannequins, and treat us without an ounce of dignity. The whole thing is humiliating. Every time I go through airport security, I feel like I'm being processed for prison. I now avoid flying at all costs and recently drove nine hours instead of flying one. TSA screening has not caught a SINGLE terrorist or prevented a SINGLE terrorist attack. It is security theater and a complete waste of taxpayer money.

C

John Hand

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5188

Tracking Number: 1jx-851x-zlqk

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
John Hand

City:
Metuchen

Country:
United States

State or Province:
NJ

ZIP/Postal Code:
08840

Comment

1) I fly less fearing that my civil liberties will be violated especially when it comes to the body scanners. As a result, I travel less and when I do have to travel, I drive. Statistically, driving is a much more dangerous activity than flying. Whether you agree with my reasons or not, the TSA policies are causing me (and quite possibly like minded people) to travel less which hurts the economy and it also causes me to drive more which in turn causes more motor traffic and accidents.

2) I don't believe the TSA policies make me any safer. I feel it is all "security theater". It has been shown that people can easily circumvent the body scanners.

3) I feel the TSA can make us safer using less expensive means such as: Israeli style airport security and passenger questioning, bomb/explosive sniffing dogs, etc. It was found that the TSA body sniffer machines didn't work after a bunch had already been ordered, costing us millions. Low tech security is sometimes more efficient AND is much less costly.

4) I am tired of taking off my shoes and throwing out my water bottles. Surely by now, the TSA could have figured out a way inconvenience passengers less: i.e. by using bomb sniffing dogs.

5) I feel a government agency should determine a single centralized airport security protocol but airports should be able to hire and pay for private security contractors who should follow those security protocols. Airports used to be able to opt out of TSA-employees lining their security lines; they used to be able to hire private contractors. But then the TSA stopped allowing airports from opting out for no apparent reason. Some of surmised that the reason was because the TSA feared that all airports would eventually do this and it would reduce the TSA's budget.

Please eliminate expensive screening methods that can be easily circumvented. Please do not make us give up our freedoms when there are ways to avoid it. Please reduce the TSA's role in screening passengers!!!

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5215

Tracking Number: 1jx-8630-rvei

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Comment

I consider the AIT tipe search extremely abusive towards the public, and useless in the fight against explosives and weapons, especially when compared to alternative technology

regulations.gov
Your Voice in Federal Decision-Making

Anonymous

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule:

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5215

Tracking Number: 1jx-8630-rvei

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Comment

I consider the AIT tipe search extremely abusive towards the public, and useless in the fight against explosives and weapons, especially when compared to alternative technology

Jason Sonenshein

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5221
Tracking Number: 1jx-8632-v2p1

Comment

Your policy of forcing passengers to submit to voyeurism, sexual imposition, or both as a condition of boarding a commercial aircraft is a violation of the Fourth Amendment and an affront to human dignity.

It might also be killing people. As a result of this policy, I am more likely to drive rather than to fly, and automobile travel is much more dangerous than air travel.

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Jason Sonenshein

City:
Cleveland

Country:
United States

State or Province:
OH

ZIP/Postal Code:
44135

C

Gillian Conway

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5270

Tracking Number: 1jx-8632-qvpm

Comment

The AIT technology is no more effective at locating and deterring suspicious activity than a regular metal detector and wastes time in airports. The alternative of a pat down is degrading and a violation of freedom. Regardless if the pat down is done by a same-sex individual or not, it is a violation of individual rights to be touched by strangers against our will, especially when an alternative (metal detector) is more effective.

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Gillian Conway

Mailing Address:
63 Clinton Street #7

City:
New York

Country:
United States

State or Province:
NY

ZIP/Postal Code:
10002

USJF United States Justice Foundation

June 24, 2013
Via upload to regulations.gov

The Honorable John S. Pistole
Administrator
Transportation Security Administration
U.S. Department of Homeland Security
Washington, D.C. 20528

Subject: Transportation Security Administration: Use of Dangerous Body Scanners, Invasive Patdowns, and other Abuses of Constitutional Rights

Dear Mr. Pistole:

Due to a federal court order,[1] TSA has been compelled to give notice and invite comments on the use of "millimeter-length radio wave" scanners, known as whole body imaging, or advanced imaging technology ("AIT").[2]

The public should have been informed and allowed to fully participate in a discussion about airline security before the order was given to subject all commercial air travelers to these machines. The public should not have to wait years, until some advocates take the agency to court, to be given notice and the opportunity to comment.

Statutory Standards

When prescribing a regulation, the TSA is required by law to "consider whether a proposed regulation is consistent with the public interest in promoting air transportation and intrastate air transportation." 49 U.S.C. §44903(b)(2)(B). The TSA is required by law "to the maximum extent practicable, require a uniform procedure for searching and detaining passengers and property to ensure courteous and efficient treatment." 49 U.S.C. §44903(b)(3)(B).

[1] *See* Electronic Privacy Information Center v. U.S. Dept. of Homeland Security, 653 F.3d 1 (D.C. Cir. 2011).
[2] *See* http://www.gpo.gov/fdsys/pkg/FR-2013-03-26/pdf/2013-07023.pdf

932 "D" St., Suite 3 • Ramona, CA 92065 • Tel (760) 788-6624 • Fax (760) 788-6414 • www.usjf.net

New Scanners

These new scanning machines, the L-3 Pro Vision, were scheduled to have been fully deployed by June 1, 2013. TSA requires all commercial air travelers in the United States to be processed by one of these machines, as a condition of travel. Those who object are subjected to invasive "pat-downs" by TSA employees. The only exception appears to be certain minors who may use Walk Through Metal Detectors ("WTMD"). (This new generation of scanners is replacing the Rapiscan Secure 1000 which uses backscatter technology.)

The U.S. Justice Foundation finds the new scanners just as objectionable as the former scanners. It also objects to the entire "security" airline system run by the Transportation Security Administration ("TSA"). The TSA has proven itself capable only of harassing ordinary citizens, and incapable of producing demonstrable benefits to national security.

Optional Opt-Out

The TSA notice states that "AIT screening is **currently** optional, but when opting out of AIT screening, a passenger will receive a pat-down." 78 *Fed. Reg.* 18296 (emphasis added). The use of the word "currently" is ominous, indicating that TSA believes that it could impose mandatory AIT screening on all air travelers.

> No matter how invasive a pat-down search may be,[3] the option to avoid potentially dangerous AIT screening must be preserved.

Constitutional Right to Travel

TSA often overlooks the fact that Title 49, under which the existence of the TSA is authorized, also recognizes that "a citizen of the United States has a public right of transit through the navigable airspace." 49 U.S.C. § 40103(a)(2). TSA does not respect that right to travel, and these comments begin with a constitutional analysis of the right to travel.

American citizens have a constitutional right to travel, a right which has been repeatedly recognized by the U.S. Supreme Court. "The right to travel is a part of the 'liberty' of which the citizen cannot be deprived without due process of law under the Fifth Amendment." The right to travel was described as "deeply engrained in our history" by the time the Constitution was written, since "[i]n Anglo-Saxon law that right was emerging at least as early as the Magna Carta." Kent v. Dulles, 357 U.S. 116, 125-126 (1958). Indeed, such a right was expressly stated in the Articles of Confederation.

In the course of examining a law passed by Congress, the U.S. Supreme Court declared that, because the right to travel is an "exercise by an American citizen of an activity included in constitutional protection," the Court would "not readily infer that Congress gave" government agencies "unbridled discretion to grant or withhold" that right. Kent v. Dulles, 357 U.S. at 129. The Court stated that "[w]here activities or enjoyment, natural and often necessary to the well

[3] *See, e.g.*, http://www.huffingtonpost.com/2013/05/29/ashley-jessica-tsa-video_n_3354522.html?icid=maing-grid7|main5|dl12|sec1_lnk3%26pLid%3D320262

being of an American citizen, such as travel, are involved, we will construe narrowly all delegated powers that curtail or dilute them." *Id.* at 129. This means that in the United States, we give the benefit of the doubt to the citizen, not the government agency, when it is not entirely clear what conditions Congress has authorized to be placed on travel.

Furthermore, the U.S. Supreme Court has declared that if a law "too broadly and indiscriminately restricts the right to travel" it "thereby abridges the liberty guaranteed by the Fifth Amendment." Aptheker v. Secretary of State, 378 U.S. 500, 505 (1964). The Court also said that "in determining the constitutionality of" a law, it is "important to consider that Congress has within its power 'less drastic' means of achieving the congressional objective of safeguarding our national security." Aptheker, 378 U.S. at 512-513.

Thus, any law or other government action must be one that intrudes least upon the rights of American citizens to travel. The U.S. Supreme Court has declared that "even though the governmental purpose be legitimate and substantial, that purpose cannot be pursued by means that broadly stifle fundamental personal liberties when the end can be more narrowly achieved. The breadth of legislative abridgment must be viewed in the light of less drastic means for achieving the same basic purpose." *See, e.g.,* Shelton v. Tucker, 364 U.S. 479, 488 (1960).

The current system is certainly not the "most narrow" or least intrusive system to prevent terrorist attacks. Old women, young children, military personnel, veterans, people in wheelchairs, and others who are obviously not terrorists are targeted. A United States Senator was detained by the TSA after he refused a "pat-down" when the TSA machine malfunctioned.[4] Even a former Vice President of the United States has been forced to go through TSA screening.[5]

TSA Procedure

The TSA claims that the new millimeter wave technology scanners are safe, and protect our privacy. How are the American people to trust this representation, when similar representations were made by the TSA about the previous Rapiscan Secure 1000 machines, which now have been removed amidst allegations of their health risks? It even has been alleged that the TSA faked its safety data on its X-ray airport scanners, deceiving the public about the safety of such devices.[6] It has added to public suspicion of TSA that it refused to allow these scanners to be tested independently by outside scientists.[7]

The TSA claims that the images of travelers generated by their machine are not saved. Yet, members of other federal agencies have been caught saving images, and some have even

---

[4] Why Rand Paul refused a TSA pat down, missed flight to D.C., The Christian Science Monitor, January 23, 2012.

[5] Gore, Staff Led Past Airport Security, The Associated Press, Thursday, March 1, 2007.

[6] *See* letter signed by five professors. http://www.propublica.org/article/ scientists-cast-doubt-on-tsa-tests-of-full-body-scanners

[7] Andrew Tarantola, Did the TSA Ignore Early X-Ray Scanner Cancer Risks?, Gizmodo, November 2, 2011.

been leaked to the public.[8] It is impossible to believe TSA employees do not use these machines to save and then store these images of some travelers.

If a citizen declines to go through a machine, or if a machine malfunctions, or even on the whim of TSA agents, citizens are subjected to pat-downs that approach molestation.[9] If off-duty TSA agents were to touch a child in the same manner as employed in their security procedures, they would very likely be arrested for this shameful conduct.[10] Texas has considered enacting a law to forbid security pat-downs of private parts of air travelers — and has been threatened by the U.S. Justice Department.[11]

Overblown Threat to Public

The value of TSA security measures is highly questionable. "Most of these security features are for public consumption," says Vahid Motevalli, co-founder of the Aviation Institute at George Washington University and now a professor at Purdue University. "In many cases, if you don't catch these issues well in advance of the airport, it's too late."

Indeed, ordinary passengers have proven more effective than the federal government in stopping terrorist attacks.[12] Richard Reid, cited in the TSA notice, the "shoe bomber," was stopped by passengers on the plane, not by TSA personnel or other federal agents.[13] The TSA notice also mentions the so-called "underwear bomber" who managed to make it past security onto a flight from Amsterdam to Detroit, even though other passengers overheard the man's companion telling airport staff that he did not have a passport.[14] When he attempted to set off the device, he was subdued by other passengers. Other passengers on the plane, who were interviewed by TSA when the flight landed, question the peculiar circumstances by which this passenger was escorted onto the plane by officials over the objections of the airline.

Trevor Aaronson's widely acclaimed, most careful study of FBI claims of stopping terrorist plots, published earlier this year (The Terror Factory, IG Publishing (2013)) demonstrates that many of the "terrorist plots" claimed to be foiled by federal agents were largely the invention of federal informants and agents, rather than the subjects of their investigations. To date, there is remarkably little evidence that any actual terrorists have been caught by any part of the TSA, including undercover armed air marshals riding on planes.

---

[8] Joel Johnson, One Hundred Naked Citizens: One Hundred Leaked Body Scans, Gizmodo, November 16, 2010.

[9] Matt Johnson, Woman records video of controversial TSA pat-down in San Diego, CBS 8 (San Diego), May 29, 2013.

[10] Derek Kravitz, Airport 'pat-downs' cause growing passenger backlash, The Washington Post, November 13, 2010.

[11] http://abcnews.go.com/Business/texas-legislators-tsa-mess-texas/story?id=13695896#.UcjbsZzNlPc

[12] Kurt Haskell, The Truth About Flight 253 Has Been Revealed, LewRockwell.com, February 2, 2010.

[13] Michael Elliott, The Shoe Bomber's World, Time, February 16, 2002.

[14] Paul Egan, Passenger Says Accused Terrorist Got Help Boarding, Detroit News, December 28, 2009.

The previous machines in use, the backscatter x-ray machines, had "glaring blind-spots and … difficulty distinguishing explosives from human tissue."[15] If these machines could not detect the current explosive devices being used by al-Qaeda, why did the TSA spend so much money to acquire them? Many have wondered if this procurement was related in any way to the fact that former Secretary of Homeland Security Michael Chertoff's consulting agency, Chertoff Group, represented Rapiscan, the manufacturer of the scanners.

Fourth Amendment

The TSA regulations violate the Fourth Amendment to the U.S. Constitution. Universal screening of all passengers is not appreciably different from the infamous and tyrannical general warrants that empowered British government officials to search of homes, persons, and possessions without probable cause and without individual justification for the search. Although the U.S. Supreme Court has carved out an administration search exception to the Fourth Amendment, neither history nor text supports such an exception. Indeed, the general warrant was misused not just in the enforcement of the criminal law, but also in the enforcement of tariffs on the importation and exportation of goods.

We would urge TSA to take the lead to restore full Fourth Amendment protection by abandoning its general search policy in favor of one that limits screening to those persons who the TSA has reason to believe are a threat to interstate travel.

[15] Leon Kaufman and Joseph W. Carlson, An evaluation of airport x-ray backscatter units based on image characteristics, Journal of Transportation Security, Volume 4, Issue 1, pp 73-94, March 2011.

Cost-Benefit Analysis

Executive Order Nos. 12866 and 13563 require agencies to assess the costs and benefits of regulatory alternatives. TSA has not weighed the full costs of its program. A 2007 study found that TSA security procedures "reduced passenger volume by about 6 percent on all flights and by about 9 percent on flights departing from the nation's 50 busiest airports."[16] These estimates may well be understated. Many airlines are in desperate financial struggles, due to the increased costs and loss of passengers. The federal government has already given the industry a $15 billion bailout, and has been asked for more funds since then.[17] Many airlines are in bankruptcy. It does not benefit the airlines or the American economy when the TSA discourages flying.

Conclusion

The entire TSA system imposes an unnecessary barrier to the right to travel that Americans possess. TSA should not only abolish its imaging scanner/invasive pat down program, but the TSA itself should be abolished, and responsibility for airline security should be returned to the airlines, where it belongs.

Sincerely,

Michael Connelly

Michael Connelly
Executive Director

---

[16] Garrick Blalock, Vrinda Kadiyali, and Daniel H. Simon, The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel, The Journal of Law and Economics, April 30, 2007.

[17] Jaime Holguin, 9/11 Airline Bailout: So, Who Got What?, CBS News, February 11, 2009.

C

Gayle Martin

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I shouldn't be treated like a criminal for buying a ticket on an airliner!

I shouldn't be subjected to a naked body scanner that reveals and stores images of my private parts to a total stranger, who may or may not be the same gender as me.

I should not be exposed to cancer-causing radiation when I have a family history of melanoma.

I should not be patted down like a common criminal when I have done nothing wrong, and when there is no probably cause.

Because of the TSA, I NOW DRIVE MY CAR INSTEAD OF FLY.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5327

Tracking Number: 1jx-85d2-qoez

Document Information

Date Posted:
Jul 2, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Gayle Martin

Mailing Address:
P.O. Box 12195

City:
Tucson

Country:
United States

State or Province:
AZ

ZIP/Postal Code:
85732

Comments of Thomas A. Burns Regarding
NPRM: Passenger Screening Using Advanced Imaging Technology
TSA-2013-0004-0001 (RIN 1652-AA67)

I have the following comments regarding the proposed rulemaking by TSA:

1) Administrative searches at airports are legally defined by US vs Davis 482 F.2d 893, 1973, as not exceeding Constitutional limits "provided that the screening process is no more extensive nor intensive than necessary, in the light of current technology, to detect the presence of weapons or explosives, that it is confined in good faith to that purpose, and that potential passengers may avoid the search by electing not to fly." Nude Body Scanning, i.e. the viewing by a government actor of a nude image of the traveler's body, no matter how fuzzy or indistinct, are far too invasive to fit that legal definition.

2) Nude Body Scanners are ineffective. They detect objects on the surface of the body, but cannot reliably distinguish harmless objects from objects dangerous to commercial air travel such as guns or explosives. As a result, guns and explosives can be brought through the checkpoint in cavities, under skin folds, under fake skin, with use of a pancake, on the side of the body, etc. This has been recently (and convincingly) demonstrated on several occasions at TSA checkpoints by Jonathan Corbett (link: https://tsaoutofourpants.wordpress.com/2012/06/20/watch-tsa-nude-body-scaners-get-defeated/). The use of scanners instead of walk-through metal detectors is thus making it easier to bring guns on an airplane.

3) Because Nude Body Scanners detect surface objects, but not their nature, persons with objects on their body are subjected to invasive secondary screens. Objects include prosthetic breasts, ostomies, bandages, maxipads, and adult diapers, among others (even scars and body abnormalities such as bony knees seem to appear). As a result, persons with a myriad of conditions that are in no way a threat to airport security are subjected to possibly invasive "secondary" screenings. In fact, the TSA has been constantly in the news for mistreating persons with disabilities and medical conditions. False positives are common.

4) The only alternative to Nude Body Scanning currently allowed by TSA is an invasive violation of a passenger’s civil rights. Persons sent to secondary screening, who opt-out, or who have medical conditions that don´t allow them to use the scanners (insulin pumps, inability to stand still, inability to hold arms above head, claustrophobia, etc.) are submitted to what is called a "pat-down", but is actually a full body rub, including intimate areas, and the insertion of the officer´s hands into the passenger´s pants. In most states this level of uninvited contact by another person outside of the checkpoint would be recognized as sexual assault.

5) Nude Body Scanning machines are slow, create long passenger lines, and require more TSA personnel to operating than traditional walk-through metal detectors. In order to reduce the high number of false positives, they require full removal of everything from pockets, belts, etc. They also create security risks for passengers by separating persons from their belongings for a prolonged period without the ability to keep them in sight. Use of the NBS in many cases also forces the separation of adults from children.

6) The TSA proposal appears to give the agency the authority to use Nude Body Scanners without any privacy safeguards. But the federal court made clear that TSA may not require individuals to undergo Nude Body Scanning. Passengers MUST be allowed the right to opt-out of being screened by Nude Body Scanners. Congress also said that NBS may not be deployed without privacy filters. The TSA must revise its proposal to acknowledge the ruling of the court and the act of Congress. Additionally, passengers opting-out should not be forced to undergo humiliating invasive "pat-downs" as the only alternative.

7) Nude Body Scanners have not been demonstrated to be safe. One type of Nude Body Scanners uses backscatter technology, which involves the use of x-rays (a form of ionizing radiation that is a known carcinogen). X-ray radiation exposure is cumulative over a person's lifetime. No amount of exposure is "safe"; even guidelines for therapeutic medical exposure to ionizing radiation limit use to "the lowest possible exposure and the minimum number of images". No legitimate scientific research would be allowed to universally expose pregnant women and young children to radiation without good reason to believe the benefits outweigh the risks. TSA should not do so either. The other type of Nude Body Scanner uses millimeter-wave technology (MMW). The risks of MMW exposure are presently unknown. However, scientific studies has shown a trend toward higher rates of brain and other tumors in those who used cellphones (which produce a similar form of non-ionizing radiation). TSA has to date not produced a proper, thorough, and INDEPENDENT review of the safety of either type of Nude Body Scanning machines.

8) The only acceptable screening option described by TSA is Regulatory Alternative #3: "Under this alternative, TSA continues to use WTMDs as the primary passenger screening technology. In addition, TSA supplements the WTMD screening by conducting ETD screening on a randomly selected portion of passengers after screening by a WTMD." All other options put forward by TSA are unacceptable based on legal, privacy, efficacy, and safety considerations.

Thomas A. Burns
June 23, 2013

Sandra Mendyk

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5457

Tracking Number: 1jx-852n-h91b

Document Information

Date Posted:
Jul 9, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Sandra Mendyk

Mailing Address:
627 N. Lincoln St.

City:
Arlington

Country:
United States

ZIP/Postal Code:
22201

Comment

Comment regarding FR Doc.2013-07023, Passenger Screening Using Advanced Imaging Techology

Since the Transportation Security Administration (TSA) installed the so-called Advanced Imaging Technology (AIT) or full-body scanners at American airports, I have avoided air travel altogether. For example, last year I drove nearly 6,000 miles on two separate trips to avoid being subjected to what clearly is a violation of privacy by this intrusive form of airport passenger inspection. Of course, the alternative to the scanners offered passengers is the even more intrusive and humiliating prison-style (so called "enhanced) pat-downs.

I certainly understand the necessity of carefully checking passengers and their possessions given the concern about acts of terrorism. However, I have read little to convince me that the items the TSA has discovered to date by the use of the full-body scanners or "enhanced" pat-downs warrant the infringement of privacy rights to which passengers have been subjected.

As the outstanding forensic work following the Boston Marathon bombings has demonstrated, modern technology is so far advanced that there are alternatives to full-body scanners and "enhanced" pat-downs that both protect the flying public and their privacy rights. I personally recommend the use of metal detectors as a primary screening technology combined with explosive trace detection tests on randomly-selected passengers.

I appreciate the opportunity to comment on the proposed Passenger Screening Using Advanced Imaging Technology rule. I hope and trust the TSA will take my comments and the opinions of others into serious consideration prior to reaching a final conclusion.

Sandra L. Mendyk

C

Mary

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

I would like to go back to primary screening with metal detectors and conducting explosive trace detection tests on random passengers. My reason for my huge dislike of the full body scanners is because they always show something for which I have to get a full pat down. I never have any metal on when I travel. I don't wear jewelry. I don't wear anything with a zipper. I have not had any body parts replaced. I have no metal inside of my body. Yet every time I have to go through this invasion of my privacy with the pat down. Sometimes it shows something on my arms. Sometimes on my hip. Sometimes on my butt. It's never in the same place. When there were just metal detectors, I never made the buzzer go off. The TSA patdowns have never found anything. I have been the random passenger chosen for the explosive trace test and those have always come back negative. (Let me state I do not have a problem with this test!) They do this test on my carry-ons after I get a pat down and they never find anything. Because of these patdowns, I have stopped flying and I choose to drive. One of my family members or friends would have to be dying for me to go through this hassle of strangers feeling me up before I will ever fly again. However, if we go back to metal detectors, I will start flying again...and I would put myself in the part of the population that flys about 4-5 times a year. PLEASE get rid of the full body scanners. Using me as an example, you can see that they don't do what they are supposed to be doing. I'm over it.

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5467

Tracking Number: 1jx-85ah-gh5p

Document Information

Date Posted:
Jul 10, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Mary

State or Province:
Missouri

Darian Turner

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment

The AIT system is invasive, as are the enhanced pat downs that are currently the only other option. Numerous videos have surfaced showing that the intrusive technology is not fool-proof, and I strongly support a metal detector/explosive detection alternative.

Comments Not Accepted

ID: TSA-2013-0004-5489

Tracking Number: 1jx-85an-nrf2

Document Information

Date Posted:
Jul 10, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Darian Turner

Mailing Address:
36342 Tunbridge Drive

City:
Newark

Country:
United States

State or Province:
CA

ZIP/Postal Code:
94560

C

Jennifer Moore

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5529

Tracking Number: 1jx-85cg-j2mn

Document Information

Date Posted:
Jul 15, 2013

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Jennifer Moore

Mailing Address:
22031 Woodbine St. NW

City:
Oak Grove

Country:
United States

State or Province:
MN

ZIP/Postal Code:
55303

Comment

I ask that the Agency abandon the use of full-body scans and return to the use of metal detectors, supplemented by random explosive trace detection screening.

Full-body scans have been demonstrated to be no better than metal detectors at discovering the presence of weapons. We are told to minimize our exposure to x-ray technology in order to manage cancer risks, yet the government's increasing reliance on this technology makes it difficult to avoid.

Perhaps more concerning is the way these machines and pat-downs violate our privacy without really improving airline security. There is nothing that the present security measures detect that would not be detected with metal detectors and random explosive trace detection screening.

What is most concerning is the bizarre attitude adopted by TSA checkpoint employees. They bark orders at us. They scold us for every perceived violation of the elaborate security regulations. Our children and elderly are picked out for pat-downs, and separated from traveling members who could facilitate the process. I've seen attractive women obviously singled out for special attention by male TSA employees.

And while news reports are full of stories about TSA employees stealing our belongings, I have struggled to keep my eyes on my property while I have been singled out for a pat-down.

We need to travel. Travel is not only a fundamental right, but it's also key to the health of our economy. For several years, I have chosen to drive whenever possible to avoid the humiliation of airport security. That closes my business down for up to four days longer than my typical vacation would last. That's lost income and lost tax revenue. That's eight days per year lost productivity! And I know there are many other people who make the same decision.

C

Donna Ellis

The is a Comment on the **Transportation Security Administration** (TSA) Proposed Rule: **NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

For related information, **Open Docket Folder**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

ID: TSA-2013-0004-5580

Tracking Number: 1jx-8612-u6fe

Document Information

Date Posted:
Dec 16, 2015

RIN:
1652-AA67

Show More Details

Submitter Information

Submitter Name:
Donna Ellis

Country:
United States

ZIP/Postal Code:
85226

Comment

"Dear TSA:

As member of the LGBT and allied community, I am deeply concerned that the TSA's proposed rule does nothing to protect passenger privacy and merely expands the agency's power. Transgender travelers especially are put in fear of being outed, humiliated, and facing additional screening because of their appearance, physical characteristics, or necessary personal items.

TSA should conduct a new cost-benefit analysis that fully considers the impact of both body scanners and pat-downs on traveler privacy.

I urge TSA to adopt Regulatory Alternative #3, using walk-through metal detectors and explosive trace detection instead of body scanners and pat-downs. Alternatively, TSA should consider additional regulatory solutions that reduce reliance on body scanners and prison-style pat-downs as primary screening methods.

To the extent TSA continues the use of body scanners and pat-downs, the final rule should codify minimum protections, including guaranteeing individual passenger image data is not retained; that all physical searches are conducted by officers of the same self-identified gender; that secondary screening will be conducted in private at passenger's election; that no passenger is required to expose sensitive areas under clothing to display any item; that searches to resolve an anomaly are no more intrusive then necessary to resolve the anomaly; that screeners receive training on working with diverse populations; and that no traveler will be subject to discrimination on the basis of gender identity.

Sincerely,
Donna

epic.org
ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

DEPARTMENT OF HOMELAND SECURITY

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA-021 TSA PreCheck Application Program System of Records

Notice of Privacy Act System of Records and Notice of Proposed Rulemaking

[Docket Nos. DHS-2013-0040 and 0041]

Privacy Act of 1974; Department of Homeland Security/Transportation Security Administration—DHS/TSA-019 Secure Flight Records System of Records

[Docket No. DHS-2013-0020]

October 10, 2013

By notice published on September 10, 2013,[1] the Department of Homeland Security ("DHS") proposes to establish a new Privacy Act system of records titled, "Department of Homeland Security/Transportation Security Administration—DHS/TSA—021 TSA PreCheck Application Program System of Records" ("TSA PreCheck Application Database" or "TSA Database"). By notice published on September 11, 2013,[2] DHS proposes to exempt the TSA PreCheck Application Database from several significant provisions of the Privacy Act of 1974. And by a separate notice published on September 10, 2013, DHS proposes to update and reissue a current DHS system of records titled, "Department of Homeland Security/Transportation Security Administration—DHS/TSA—019 Secure Flight Records

[1] Notice of Privacy Act System of Records, 78 Fed. Reg. 55,274 (proposed Sept. 10, 2013) (hereinafter "PreCheck SORN").
[2] Notice of Proposed Rulemaking, 78 Fed. Reg.55,657 (proposed Sept. 11, 2013) (hereinafter "PreCheck NPRM").

System of Records."[3] Pursuant to DHS's notices, the Electronic Privacy Information Center ("EPIC") submits these comments to: (1) address the substantial privacy and security issues raised by the database; (2) urge DHS to significantly narrow the Privacy Act exemptions for the TSA PreCheck Application Database; and (3) recommend that DHS withdraw unlawful and unnecessary proposed routine use disclosures.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has previously opposed other DHS passenger profiling programs,[4] and has called for an independent audit to determine whether the Transportation Security Administration ("TSA") airport screeners engage in racial profiling.[5] EPIC highlighted the problems inherent in passenger profiling systems like Secure Flight in previous testimony and comments. In testimony before the National Commission on Terrorist Attacks Upon the United States (more commonly known as "the 9/11 Commission"), EPIC President Marc Rotenberg explained, "there are specific problems with information technologies for monitoring, tracking, and profiling. The techniques are imprecise, they are subject to abuse, and they are invariably applied to purposes other than those originally intended."[6]

---

[3] Notice of Modified Privacy Act System of Records, 78 Fed. Reg. 55,270 (proposed Sept. 10, 2013) (hereinafter "Secure Flight SORN"). Although these comments focus primarily on TSA PreCheck, certain portions of the Secure Flight SORN implicate TSA PreCheck and EPIC has addressed those portions in these comments.

[4] *See, e.g.*, EPIC et al., *Comments on the Terrorist Screening Database System of Records, Notice of Privacy Act System of Records and Notice of Proposed rulemaking, Docket Nos. DHS 2011-0060 and DHS 2011-0061* (Aug. 5, 2011), *available at* http://epic.org/privacy/airtravel/Comments_on_DHS-2011-0060_and_0061FINAL.pdf; EPIC, *Comments on Secure Flight*, *Docket Nos. TSA-2007-28972, 2007-28572* (Sept. 24, 2007), *available at* http://epic.org/privacy/airtravel/sf_092407.pdf; EPIC, *Secure Flights Should Remain Grounded Until Security and Privacy Problems are Resolved, Spotlight on Surveillance Series* (August 2007), *available at* http://epic.org/privacy/surveillance/spotlight/0807/default.html; EPIC: Passenger Profiling, http://epic.org/privacy/airtravel/profiling.html; EPIC: Secure Flight, http://epic.org/privacy/airtravel/secureflight.html; EPIC: Air Travel Privacy, http://epic.org/privacy/airtravel/.

[5] Letter from EPIC et al., to Secretary Janet Napolitano and Honorable Charles K. Edwards, Department of Homeland Security (Dec. 1, 2011), *available at* http://epic.org/privacy/airtravel/12-01-11-Coalition-Racial-Profiling-Audit-DHS-Letter.pdf.

[6] Marc Rotenberg, President, EPIC, *Prepared Testimony and Statement for the Record of a Hearing on Security & Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003), *available at* http://www.epic.org/privacy/terrorism/911commtest.pdf.

Despite EPIC's recommendations and empirical evidence of the ineffectiveness of passenger profiling, DHS continues to expand its passenger profiling capabilities and now proposes broad Privacy Act exemptions to the operation of the TSA PreCheck Application Database.

Purpose and Scope of the TSA PreCheck Application Database

According to DHS, the TSA PreCheck Application Database "will use the information provided by applicants to the [TSA PreCheck] Program to perform a security threat assessment to identify individuals who present a low risk to transportation security. This passenger prescreening enables TSA to determine the appropriate level of security screening the passenger will receive before the passenger receives a boarding pass."[7] DHS states that passengers that qualify for expedited screening "typically will receive more limited physical screening, *e.g.*, will be able to leave on their shoes, light outerwear, and belt, to keep their laptop in its case, and to keep their 3-1-1 compliant liquids/gels bag in a carry-on."[8]

To qualify for PreCheck, applicants provide their biographic and biometric information to DHS and, as described by DHS, TSA will use applicant information to perform a "security threat assessment" of "law enforcement, immigration, and intelligence databases, including a fingerprint-based criminal history check conducted through the Federal Bureau of Investigation."[9] The agency states it will use the security threat assessment to "identify individuals who present a low risk to transportation security."[10] TSA will then provide a "Known Traveler Number" ("KTN") to "low risk" individuals.[11]

After having received a KTN, passengers will supply their KTNs to commercial airlines when making flight reservations.[12] The airline will then send passenger Secure Flight Passenger Data ("SFPD"), which includes KTNs, name, gender, date of birth, available passport information, available redress number, "reservation control number, record sequence number, record type, passenger update indicator,

---

[7] PreCheck NPRM, 78 Fed. Reg. at 55,657.
[8] PreCheck SORN, 78 Fed. Reg. at 55,275.
[9] PreCheck NPRM, 78 Fed. Reg. at 55,657.
[10] PreCheck SORN, 78 Fed. Reg. at 55275.
[11] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[12] *Id.*

traveler reference number, and itinerary information" to the TSA.[13] The TSA will then compare SFPD to the TSA PreCheck Application Program and various undisclosed watch lists.[14] DHS further states that in comparing SFPD against PreCheck Application Program and various watch lists, it will review that information "using intelligence-driven, risk-based analysis to determine whether individual passengers will receive expedited, standard, or enhanced screening; the results will be indicated on the passenger's boarding pass."[15] Although DHS states that the "primary result of the risk-based analysis will be the identification of passengers who are eligible for expedited screening,"[16] DHS also acknowledges that "watch list matches will receive screening appropriate for their watch list status."[17]

TSA PreCheck Application Database would contain "any or all" of the following information:

> (a) Name (including aliases or variations of spelling); (b) Gender; (c) Current and historical contact information (including, but not limited to, address, telephone number, and email address); (d) Date and place of birth; (e) Physical description, fingerprint and/or other biometric identifier, including photograph; (f) Control number, Social Security Number (SSN), or other unique identification number assigned to an individual; (g) Information necessary to assist in tracking submissions, payments, and transmission of records; (h) Other data as required by Form FD-258 (fingerprint card) or other standard fingerprint cards used by the federal government; (i) Information provided by individuals covered by this system in support of their application, such as driver's license, passport or other documents used to verify identity, confirm immigration status, or other eligibility requirements; (j) Criminal history records; (k) Records obtained from the Terrorist Screening Center of known or suspected terrorists in the Terrorist Screening Database; and records regarding individuals identified on classified and unclassified governmental watch lists used or maintained by TSA; (l) Records containing the matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental databases, such as law enforcement, immigration, or intelligence databases, and individuals who have been distinguished from individuals on a watch list through a redress process or other means; (m) Other information provided by federal, state, local, tribal, territorial, and foreign government agencies or other entities relevant to the security threat assessment and adjudication of the application; (n) Results of any analysis performed for security threat assessments and adjudications; and (o) Communications between TSA and applicants regarding the results of the security threat assessments and adjudications.[18]

---

[13] *Id.*
[14] *Id.*
[15] Secure Flight SORN, 78 Fed. Reg. at 55,271.
[16] *Id.*
[17] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[18] PreCheck SORN, 78 Fed. Reg. at 55,276.

TSA has presented has five purposes for collecting, maintaining, using, and disclosing this personally identifiable information:

> (a) perform[ing] security threat assessments and to identify individuals who are a low risk to transportation or national security and are therefore eligible to receive expedited security screening; (b) assist[ing] in the management and tracking of the status of security threat assessments of individuals who apply to the TSA PreCheck Application Program; (c) permit[ting] the retrieval of the results of security threat assessments, including criminal history records checks and searches in other governmental data systems, performed on the individuals covered by this system;
> (d) permit[ting] the retrieval of information from other terrorist-related, law enforcement, immigration, and intelligence databases on the individuals covered by this system; and (e) track the fees incurred, and payment of those fees, when appropriate, for services related to security threat assessments.[19]

Information contained in the TSA PreCheck Application Database may be obtained from "TSA PreCheck Application Program applicants, the [Terrorist Screening Center] TSC, law enforcement, immigration, and intelligence agency record systems, other government databases, and other DHS systems," as well as the Federal Bureau of Investigation ("FBI").[20]

Incredibly, DHS proposes to exempt this database containing detailed, sensitive personal information from well-established Privacy Act safeguards. It is inconceivable that the drafters of the Privacy Act would have permitted a federal agency to propose a profiling system on U.S. citizens and be granted broad exemptions from Privacy Act obligations. Consistent and broad application of Privacy Act obligations are the best means of ensuring accuracy and reliability of the data used in a system that profoundly affects millions of individuals as they travel throughout the United States on a daily basis.

I. The DHS's Notice of Proposed Rulemaking Fails to Fairly Apprise the Public of DHS's Proposal

As a preliminary matter, DHS's proposal is procedurally deficient because the agency has failed to provide sufficient notice of its proposal. Specifically, DHS proposes to exempt the TSA PreCheck

---

[19] *Id*.
[20] PreCheck SORN, 78 Fed. Reg. at 55,278.

Application Program System of Records from certain Privacy Act provisions pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2). The Privacy Act permits agencies to promulgate rules exempting system of records from certain Privacy Act provisions, but those rules must be "in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e)" of the Administrative Procedure Act ("APA").[21]

The APA general notice requirements mandate that Notices of Proposed Rulemaking ("NPRMs") contain "either the terms or substance of the proposed rule or description of the subjects and issues involved."[22] "The adequacy of the notice must be tested by determining whether it would fairly apprise interested persons of the 'subjects and issues' before the agency."[23] Proposals that are "too general and open-ended to have fairly apprised the public" do not meet the APA standard of requisite notice.[24] As discussed below, DHS's proposed rule contains ambiguous key terms that do not fairly apprise the public of the proposed TSA PreCheck Application Database proposals. Accordingly, DHS's proposal violates the APA. DHS must therefore issue an unambiguous proposal and again solicit public comments, or abandon its current proposal because it has not fairly apprised the public of the system of records Privacy Act exemptions.

Throughout the NPRM, DHS states that TSA PreCheck prescreens and identifies "low risk passengers" that are "eligible to receive expedited screening."[25] After conducting a "security threat assessment" on these individuals, TSA will provide "individual[s] [who] pose [] a low risk to transportation or national security" a KTN.[26] Known Traveler Numbers are "unique number assigned to an individual for whom the Federal government has conducted a security threat assessment and

---

[21] 5 U.S.C.§ 552a(k).
[22] 5 U.S.C. § 553(b).
[23] *Prometheus Radio Project v. F.C.C.*, 652 F.3d 431, 449 (3d Cir. 2011) (*quoting Prometheus Radio Project v. F.C.C.*, 373 F.3d 372, 411 (3d Cir. 2004)).
[24] *Prometheus Radio Project*, 652 F.3d at 453.
[25] *See, e.g.*, PreCheck NPRM, 78 Fed. Reg. at 55,657-55,658. *See also* Secure Flight SORN, 78 Fed. Reg. at 55,274.
[26] PreCheck NPRM, 78 Fed. Reg. at 55,658.

determined *does not* pose a security threat."[27] Pursuant to federal Secure Flight regulations, Known Traveler Numbers are reserved for passengers who do "not pose a security threat."[28] With TSA PreCheck, DHS has expanded Known Traveler Numbers to individuals who pose some risk—albeit "low"— to transportation security. Practically speaking, DHS has amended a prior legislative rule—without conducting a public rulemaking as required by law—by granting Known Traveler Numbers to individuals who pose a "low risk" security threat.[29]

Notwithstanding this procedural deficiency, DHS fails to define "low risk passengers"—a key term used throughout the NPRM. Moreover, TSA states "[e]ligibility for the TSA PreCheck Application Program is within the sole discretion of the TSA" and that the TSA will only advise applicants if FBI criminal records disclose information "that would disqualify [applicants] from the TSA PreCheck Application Program."[30] By maintaining discretion over who is a "low risk passenger," failing to define "low risk passenger," and maintaining an opaque algorithm to determine individual risk, DHS's proposal is "too general and open-ended to have fairly apprised the public" on the scope and subject matter of the agency's proposal.[31]

Additionally, the TSA's proposal is "too general and open-ended to have fairly apprised the public" because it fails to disclose the watch lists that TSA uses to determine the level of passenger screening.[32] The TSA acknowledges that it will perform watch list matching analyses against "classified and unclassified governmental watch lists used or maintained by the TSA" including the Terrorist Screening Database, but fails to provide additional information.[33] DHS must reissue its NPRM and disclose the watch lists to fairly apprise individuals of the proposed rule and its impact. Specifically, by

[27] 49 C.F.R. § 1560.3 (emphasis added).
[28] *Id.*
[29] *Elec. Privacy Info. Ctr. v. U.S. Dep't of Homeland Sec.*, 653 F.3d 1, 6-7 (D.C. Cir. 2011).
[30] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[31] *Prometheus Radio Project,* 652 F.3d at 453.
[32] *Id.*
[33] PreCheck SORN, 78 Fed. Reg. at 55,275.

disclosing the TSA PreCheck Application watch lists, individuals can raise arguments concerning the appropriateness of certain watch list database comparison. For example, pursuant to a FOIA lawsuit, EPIC uncovered that one of the main watch lists TSA PreCheck uses for comparison—the Terrorist Screening Database ("TSDB")—uses "particularized derogatory information" to place individuals on the watch list.[34] Alarmingly, this is a standard that has never been recognized by a court of law. EPIC's FOIA documents also revealed that individuals might remain on the TSDB watch list even if charges are dropped or a case is dismissed.[35] For the aforementioned reasons, DHS must reissue its NPRM clarifying the definition of "low risk passengers" and providing additional information on its watch lists.

II. DHS Must Provide Transparency in the TSA PreCheck Algorithm and Must Make Public the Factors Used for TSA PreCheck "Risk Assessments"

There is no publicly available information on how DHS uses its algorithms to determine which individuals will be scrutinized upon traveling throughout the United States. The key characteristics of TSA PreCheck system – including the risk and security threat assessment and the basis for the assessments– are secret. DHS evaluates personally identifiable information to determine whether individual passengers will receive "expedited, standard, or enhance screening."[36] The result of the "risk-based" analysis that determines the individual level of screening is opaque. DHS fails to clearly articulate how personally identifiable information factors into DHS risk assessments.

TSA PreCheck operates via automated data processing. This troubling practice will ultimately violate important personal rights as enumerated in such well-established privacy provisions as Article 15.1 of the 1995 EC Directive on Data Protection. The Directive, which provoked many European countries to enact provisions along the lines of article 15.1,[37] states that "Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or

---

[34] *EPIC FOIA - FBI Watchlist*, EPIC, http://epic.org/foia/fbi_watchlist.html (last visited Oct. 10, 2013).
[35] *Id*.
[36] Secure Flight SORN, 78 Fed. Reg. at 55,271.
[37] Lee A. *Bygrave, Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling*, 17 COMPUTER LAW & SOC. REP. 17, 18 (2001).

significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc."[38] In particular, Article 12.1 of the EU Data Protection Directive also grants individuals the right to obtain "the logic," *i.e.* the algorithm, of the processing of personal data.

TSA PreCheck screening would directly violate this right because the decision of which persons should undergo additional screening is entirely automated. DHS must ensure transparency and make public the algorithm that it has established to assign "risk-based" profiles to individuals so as to not further violate personal rights.

III. DHS Should Impose Strict Information Security Safeguards on its Biometric Information Collection and Limit its Dissemination of Biometric Information

Information security is a critical consideration for any organization that collects digital records and data, and it is even more important when government agencies collect sensitive and personally identify information. Government agencies must make every effort to safeguard sensitive information. Without proper safeguards, individuals and groups with malicious intent to intrude, access, and obtain sensitive information may disrupt operations or launch attacks against computer systems and networks. This concern is validated by an ever-increasing number of security incidents, the ease of obtaining hacking tools, and their growing sophistication.[39]

TSA PreCheck collects biometric identifiers, including fingerprints and photographs. Over the last several years, TSA and DHS have repeatedly encountered security failures. For example, in 2007, the TSA reported that an external hard drive containing Social Security numbers, payroll information, and

[38] Council Directive 95/46, On the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, art. 15, 1995 O.J. (L 281) 11.23.1995 (EC).
[39] *See, e.g.*, Ben Weitzenkorn, *How to Hack an iPhone With a USB Charger,* TECHNEWSDAILY (June 3, 2013, 05:43 PM), http://www.technewsdaily.com/18241-iphone-malicious-charger.html; Harry Kazianis, *Spear phishing: How the non-nerds hack into you,* THE NATION (June 14, 2013, 1:00 AM), http://www.nationmultimedia.com/opinion/Spear-phishing-How-the-non-nerds-hack-into-you-30208233.html.

bank data for about 100,000 TSA employees was stolen from a "secure area."[40] Moreover, in 2008 the TSA suffered significant security problems with its passenger redress website when the TSA failed to secure the website; large amounts of personal information were leaked, exposing hundreds of travelers to identity theft.[41] And earlier this year DHS again encountered issues securing personal and sensitive information of its employees as recently as last month. Tens of thousands of DHS employees and contractors who submitted background investigation information were at risk of having their personal data stolen, exposing them to identify theft. An internal DHS notice sent to employees noted that "[a]s a result of this vulnerability, information including name, Social Security numbers (SSN) and date of birth (DOB), stored in the vendor's database of background investigations was potentially accessible by an unauthorized user since July 2009."[42]

These weaknesses in DHS databases increase the risk that unauthorized individuals could read, copy, delete, add, and modify sensitive information, including biometric information. Accordingly, to the extent that DHS continues to collect biometric information, DHS should limit biometric information to only those agencies and government actors that require the information as a necessity. Further, DHS should strictly limit biometric information to uses for which it was originally collected.

IV. DHS Proposes Broad Exemptions for the TSA PreCheck Application Database, Contravening the Intent of the Privacy Act of 1974

DHS proposes broad Privacy Act exemptions for the TSA PreCheck Application Database, thus contravening the intent of the Privacy Act of 1974. DHS asserts these claims for "law enforcement or national security purposes."[43] DHS claims that "[n]o exemption shall be asserted with respect to information maintained in the system that is submitted by a person if that person, or his or her agent,

---

[40] Spencer S.Hsu, *TSA Hard Drive With Employee Data Is Reported Stolen*, WASHINGTON POST (May 5, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/05/04/AR2007050402152.html.
[41] U.S HOUSE COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM. INFORMATION SECURITY BREACH AT TSA, THE TRAVELER REDRESS WEBSITE (January 2008), *available at* http://www.hsdl.org/?view&did=482286.
[42] Jason Miller, *Data Breach puts DHS employees at Risk of Identity Theft*, FEDERAL NEWS RADIO (May 22, 2013, 4:05 PM), http://www.federalnewsradio.com/473/3332836/Data-breach-puts-DHS-workers-at-risk-of-identity-theft.
[43] PreCheck NPRM, 78 Fed. Reg. at 55,658.

seeks access to or amendment of such information."[44] DHS, however, further states "[t]his system . . . may contain records or information created or recompiled from information contained in other systems of records that are exempt from certain provisions of the Privacy Act" and that DHS will also claim the original Privacy Act exemptions for those records.[45]

Notwithstanding access or amendment rights to information that TSA PreCheck Applicants submit, DHS will not provide individuals access to the following records:

> (j) Criminal history records; (k) Records obtained from the Terrorist Screening Center of known or suspected terrorists in the Terrorist Screening Database; and records regarding individuals identified on classified and unclassified governmental watch lists used or maintained by TSA; (l) Records containing the matching analyses and results of comparisons of individuals to the TSDB and other classified and unclassified governmental databases, such as law enforcement, immigration, or intelligence databases, and individuals who have been distinguished from individuals on a watch list through a redress process or other means; (m) Other information provided by federal, state, local, tribal, territorial, and foreign government agencies or other entities relevant to the security threat assessment and adjudication of the application; (n) Results of any analysis performed for security threat assessments and adjudications; (o) Communications between TSA and applicants regarding the results of the security threat assessments and adjudications.[46]

DHS will, however, provide an opportunity for individuals to correct inaccurate immigration records or FBI criminal records.[47]

Furthermore, DHS proposes to claim Privacy Act exemptions to:

> preclude subjects of investigations from learning of and exploiting sensitive investigatory material that would interfere with the investigative process; avoid disclosure of investigative techniques; protect sensitive and classified information compiled during the investigation; protect Transportation Security Administration Office of Intelligence and Analysis and other federal agency information; ensure DHS's and other federal agencies' ability to obtain information from third parties and other sources; protect the privacy of third parties; and safeguard Sensitive Security Information pursuant to 49 U.S.C. 114(r).[48]

---

[44] *Id.*
[45] *Id.*
[46] PreCheck SORN, 78 Fed. Reg. at 55,276.
[47] PreCheck NPRM, 78 Fed. Reg. at 55,658.
[48] *Id.*

Specifically, pursuant to 5 U.S.C. §§ 552a(k)(1) and (k)(2), DHS proposes to exempt the TSA PreCheck Application Database from: "5 U.S.C. 552a(c)(3); (d); e (1); e (4)(G), (H), (I), and (f)." These provisions of the Privacy Act ensure that:

- an agency must give individuals access to the accounting of disclosure of their records;[49]
- an individual may request access to records an agency maintains about him or her, as well as have a copy made;[50]
- the agency must permit the individual to amend a record about him or her and acknowledge the request in writing within 10 days, as well as timely correct the record if necessary or provide a reason for refusal of the proposed amendment, as well as allow a review of the refusal;[51]
- an agency must make notes of requested amendments within the records;[52]
- an agency must collect records "about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President";[53]
- an agency must publish the establishment or revision of the notice of the existence of records in the Federal Register, along with the procedures to be followed to obtain access, contest content, and learn the categories of sources or records in the system;[54]
- the agency shall promulgate rules establishing procedures that notify an individual in response to record requests pertaining to him or her, including "reasonable times, places, and requirements for identifying an individual", instituting disclosure procedures for medical and psychological records, create procedures, review amendment requests, as well as determining the request, the status of appeals to denial of requests, and establish fees for record duplication, excluding the cost for search and review of the record;[55]

DHS attempts to circumvent the intent of the Privacy Act in order to create a massive database that lacks accountability. DHS's proposed exemptions from 5 U.S.C. § 552a(c)(3), (d), (e)(4)(G), (H), (I), and (f) only serve to increase the secrecy of the database. DHS claims that accounting for disclosures,

[49] 5 U.S.C. § 552a(c)(3).
[50] 5 U.S.C. § 552a(d)(1).
[51] 5 U.S.C. §§ 552a(d)(2), (d)(3).
[52] 5 U.S.C. § 552a(d)(4).
[53] 5 U.S.C. §552a(e)(1).
[54] 5 U.S.C. §§ 552a(e)(4)(G), (H), (I).
[55] 5 U.S.C. §§ 552a(f)(1), (2), (3), (4), (5).

granting individuals access to their records, and implementing notification regulations may put entities on notice that they are being investigated, thereby hindering their investigative efforts.[56]

While EPIC recognizes the need to withhold notice during the period of the investigation, individuals should be able to know, after an investigation is completed or made public, the information stored about them in the system. Access to records of a completed investigation, with appropriate redactions to protect the identities of witnesses and informants, would provide individuals and entities with the right to address potential inaccuracies. And because the investigations have already been completed, DHS's law enforcement purposes would not be undermined and DHS could still protect individual privacy rights.

When Congress enacted the Privacy Act in 1974, it sought to restrict the amount of personal data that Federal agencies were able to collect, and furthermore, required agencies to be transparent in their information practices.[57] In 2004, the Supreme Court underscored the importance of the Privacy Act's restrictions upon agency use of personal data to protect privacy interests, noting that: "in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary … to regulate the collection, maintenance, use, and dissemination of information by such agencies." [58]

The Privacy Act is intended to guard the privacy interests of citizens and lawful permanent residents against government intrusion. By allowing DHS to encroach on an individual's right to access and amend their information, DHS violates the intent of the Privacy Act. If DHS claims these exemptions, then the government fails to ensure the reliability of the data and fails to provide citizens with access to their personal data and opportunities to correct inaccurate or incomplete data.

---

[56] PreCheck NPRM, 78 Fed. Reg. at 55,658-59.
[57] S. Rep. No. 93-1183 at 1 (1974).
[58] *Doe v. Chao*, 540 U.S. 614, 618 (2004).

V. DHS's Proposed Routine Uses Contravene the Intent of the Privacy Act and Exceed the Authority of the Agency

The Privacy Act's definition of "routine use" is precisely tailored, and has been narrowly prescribed in the Privacy Act's statutory language, legislative history, and relevant case law. The TSA PreCheck Application Database contains a broad category of personally identifiable information. By disclosing information in a manner inconsistent with the purpose for which the information was originally gathered, DHS exceeds its statutory authority to disclose personally identifiable information without obtaining individual consent.

When it enacted the Privacy Act in 1974, Congress sought to restrict the amount of personal information that federal agencies could collect and required agencies to be transparent in their information practices.[59] Congress found that "the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and recognized that "the right to privacy is a personal and fundamental right protected by the Constitution of the United States."[60]

The Privacy Act prohibits federal agencies from disclosing records they maintain "to any person, or to another agency" without the written request or consent of the "individual to whom the record pertains."[61] The Privacy Act also provides specific exemptions that permit agencies to disclose records without obtaining consent.[62] One of these exemptions is "routine use."[63] The TSA PreCheck Application system of records notice states that "all or a portion of the records or information contained in this system may be disclosed outside DHS as a routine use pursuant to 5 U.S.C. 552a(b)(3)."[64] "Routine use" means

---

[59] S. Rep. No. 93-1183 at 1 (1974).
[60] Pub. L. No. 93-579 (1974).
[61] 5 U.S.C. § 552a(b).
[62] *Id*. §§ 552a(b)(1) – (12).
[63] *Id*. § 552a(b)(3).
[64] PreCheck SORN, 78 Fed. Reg. at 55,276.

"with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected."[65]

The Privacy Act's legislative history and a subsequent report on the Act indicate that the routine use for disclosing records must be specifically tailored for a defined purpose for which the records are collected. The legislative history states that:

> [t]he [routine use] definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information . . . or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to another person or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.[66]

The Privacy Act Guidelines of 1975—a commentary report on implementing the Privacy Act—interpreted the above Congressional explanation of routine use to mean that a "'routine use' must be not only compatible with, but related to, the purpose for which the record is maintained."[67]

Subsequent Privacy Act case law interprets the Act's legislative history to limit routine use disclosure based upon a precisely defined system of records purpose. In *United States Postal Service v. National Association of Letter Carriers, AFL-CIO*, the Court of Appeals for the D.C. Circuit relied on the Privacy Act's legislative history to determine that "the term 'compatible' in the routine use definitions contained in [the Privacy Act] was added in order to limit interagency transfers of information."[68] The Court of Appeals went on to quote the Third Circuit as it agreed, "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure."[69]

[65] 5 U.S.C. § 552a(a)(7).
[66] *Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy*, 1031 (1976).
[67] *Id*.
[68] *U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, AFL-CIO*, 9 F.3d 138, 144 (D.C. Cir. 1993).
[69] *Id*. at 145 (quoting *Britt v. Natal Investigative Serv*., 886 F.2d 544, 549-50 (3d. Cir. 1989). *See also Doe v. U.S. Dept. of Justice*, 660 F.Supp.2d 31, 48 (D.D.C. 2009) (DOJ's disclosure of former AUSA's termination letter to Unemployment Commission was compatible with routine use because the routine use for collecting the personnel

DHS proposes to disclose TSA PreCheck Application information for purposes that do not relate to aviation security and screening. DHS states that it may disclose information within the TSA PreCheck Application Database with "other DHS components that have a need to know the information to carry out their national security, law enforcement, immigration, intelligences, or other homeland security functions."[70] These proposed disclosures transform the TSA PreCheck Application Database from a narrowly defined aviation security system of records to a general law enforcement repository. With its proposal, DHS fashions the TSA PreCheck Application Database as a virtual line up that law enforcement agencies may access for purposes other than aviation security. So, while TSA PreCheck applicants volunteer their sensitive information in the hopes of obtaining expedited airport screening, DHS intends to grant law enforcement blanket access to this information for non-TSA PreCheck purposes. The agency therefore exceeds its authority with this purpose and should not adopt it.

VI. Proposed Routine Uses G, I, and J Remove Privacy Act Safeguards by Disclosing Records to Foreign and International Agencies That are Not Subject to the Privacy Act

Proposed Routine Use G would permit DHS to disclose information:

> [t]o an appropriate federal, state, tribal, local, territorial, or foreign government law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, when a record, either on its face or in conjunction with other information, indicates a violation or potential violation of law, including criminal, civil, or regulatory violations, and such disclosure is proper and consistent with the official duties of the person making the disclosure.[71]

Proposed Routine Use I would permit DHS to disclose information:

> [t]o the appropriate federal, state, local, tribal, territorial, foreign governments, or other appropriate authority, regarding or to identify individuals who pose, or are under reasonable suspicion of posing, a risk to transportation or national security.[72]

---

file was to disclose to income administrative agencies); *Alexander v. F.B.I*, 691 F. Supp.2d 182, 191 (D.D.C. 2010) (FBI's routine use disclosure of background reports was compatible with the law enforcement purpose for which the reports were collected).

[70] PreCheck SORN, 78 Fed. Reg. at 55,275-6.

[71] *Id*. at 55,277.

[72] *Id*.

Proposed Routine Use J would permit DHS to disclose information:

> [t]o foreign governmental and international authorities, in accordance with law and formal or informal agreements.[73]

The provisions in these Routine Uses that would permit DHS to disclose information to foreign agencies and international agencies must be removed. The Privacy Act only applies to records maintained by United States government agencies.[74] Releasing information to foreign entities does not protect individuals covered by TSA PreCheck Application Database from Privacy Act violations. DHS does not have jurisdiction over foreign agents. Therefore, the provisions in these Routine Uses that would permit DHS to disclose information to foreign or multilateral entities must be removed.

VII. DHS's Proposed Routine Use K Contravenes the Legislative Intent of the Privacy Act

Proposed Routine Use K would permit the agency to disclose information:

> [t]o the news media and the public, with the approval of the Chief Privacy Officer in consultation with counsel, when there exists a legitimate public interest in the disclosure of the information or when disclosure is necessary to preserve confidence in the integrity of DHS or is necessary to demonstrate the accountability of DHS's officers, employees, or individuals covered by the system, except to the extent it is determined that release of the specific information in the context of a particular case would constitute an unwarranted invasion of personal privacy. [75]

The limitations on disclosure in proposed Routine Use K is too broad to have any substantive effect, creates opportunities for violations of statutory rights, and goes against the legislative intent of the Privacy Act. As it stands, Routine Use K directly contradicts Congressman William Moorhead's testimony that the Privacy Act was "intended to prohibit gratuitous, ad hoc, disseminations for private or otherwise irregular purposes."[76]

---

[73] *Id.*
[74] 5 U.S.C. § 552a(b).
[75] PreCheck SORN, 78 Fed. Reg. at 55,277.
[76] Legislative History of the Privacy Act of 1974 S, 3418 (Public Law 93-579): Source Book on Privacy, 1031 (1976).

The phrase "when disclosure is necessary to preserve confidence in the integrity of DHS"[77] in Routine Use K is discordant with the Privacy Act because it gratuitously puts the face of the agency above an individual's right to privacy. The term "necessary" is overly ambiguous; DHS could take advantage of this criterion to unduly influence its image. DHS should remove this phrase from the proposed Routine Use because creating a category that is too broad can easily lead to the abuse of privacy rights of individuals whose data has been gathered and stored by DHS.

Conclusion

For the foregoing reasons, the proposed TSA PreCheck Application Database is contrary to the core purpose of the federal Privacy Act. Accordingly, DHS must narrow the scope of its proposed Privacy Act exemptions and not adopt its proposed unlawful routine use disclosures.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Administrative Law Counsel

Electronic Privacy Information Center (EPIC)
1718 Connecticut Avenue NW, Suite 200
Washington, D.C. 20009
(tel) 202 – 483 – 1140
(fax) 202 – 483 –1248

[77] PreCheck SORN, 78 Fed. Reg. at 55,277.

STATEMENT OF JOHN ROTH

INSPECTOR GENERAL

DEPARTMENT OF HOMELAND SECURITY

BEFORE THE

COMMITTEE ON OVERSIGHT AND GOVERNMENT REFORM

U.S. HOUSE OF REPRESENTATIVES

CONCERNING

TSA: Security Gaps

November 3, 2015

Good morning Chairman Chaffetz, Ranking Member Cummings, and Members of the Committee.

Thank you for inviting me here today to discuss our work on the Transportation Security Administration (TSA). Our reviews have given us a perspective on the obstacles facing TSA in carrying out an important — but incredibly difficult — mission to protect the Nation's transportation systems and ensure freedom of movement for people and commerce.

Throughout this year, I have testified — before this Committee and others — regarding my concerns about TSA's ability to execute its important mission. I highlighted the challenges TSA faced. I testified that these challenges were in almost every area of TSA's operations: its problematic implementation of risk assessment rules, including its management of TSA Precheck; failures in passenger and baggage screening operations, discovered in part through our covert testing program; TSA's controls over access to secure areas, including management of its access badge program; its management of the workforce integrity program; TSA's oversight over its acquisition and maintenance of screening equipment; and other issues we have discovered in the course of over 115 audit and inspection reports.

My remarks were described as "unusually blunt testimony from a government witness," and I will confess that it was. However, those remarks were born of frustration that TSA was assessing risk inappropriately and did not have the ability to perform basic management functions in order to meet the mission the American people expect of it. These issues were exacerbated, in my judgment, by a culture, developed over time, which resisted oversight and was unwilling to accept the need for change in the face of an evolving and serious threat. We have been writing reports highlighting some of these problems for years without an acknowledgment by TSA of the need to correct its deficiencies.

We may be in a very different place than we were in May, when I last testified before this Committee regarding TSA. I am hopeful that Administrator Neffenger brings with him a new attitude about oversight. Ensuring transportation safety is a massive and complex problem, and there is no silver bullet to solve it. It will take a sustained and disciplined effort. However, the first step in fixing a problem is having the courage to critically assess the deficiencies in an honest and objective light. Creating a culture of change within TSA, and giving the TSA workforce the ability to identify and address risks without fear of retribution, will be the new Administrator's most critical and challenging task.

I believe that the Department and TSA leadership have begun the process of critical self-evaluation and, aided by the dedicated workforce of TSA, are in a position to begin addressing some of these issues. I am hopeful that the days of

TSA sweeping its problems under the rug and simply ignoring the findings and recommendations of the OIG and GAO are coming to an end.

Our Most Recent Covert Testing

In September 2015, we completed and distributed our report on our most recent round of covert testing. The results are classified at the Secret level, and the Department and this Committee have been provided a copy of our classified report. TSA justifiably classifies at the Secret level the validated test results; any analysis, trends, or comparison of the results of our testing; and specific vulnerabilities uncovered during testing. Additionally, TSA considers other information protected from disclosure as Sensitive Security Information.

While I cannot talk about the specifics in this setting, I am able to say that we conducted the audit with sufficient rigor to satisfy the standards contained within the Generally Accepted Government Auditing Standards, that the tests were conducted by auditors within our Office of Audits without any special knowledge or training, and that the test results were disappointing and troubling. We ran multiple tests at eight different airports of different sizes, including large category X airports across the country, and tested airports using private screeners as part of the Screening Partnership Program. The results were consistent across every airport.

Our testing was designed to test checkpoint operations in real world conditions. It was not designed to test specific, discrete segments of checkpoint operations, but rather the system as a whole. The failures included failures in the technology, failures in TSA procedures, and human error. We found layers of security simply missing. It would be misleading to minimize the rigor of our testing, or to imply that our testing was not an accurate reflection of the effectiveness of the totality of aviation security.

The results were not, however, unexpected. We had conducted other covert testing in the past:

- In September 2014, we conducted covert testing of the checked baggage screening system and identified significant vulnerabilities in this area caused by human and technology based failures. We also determined that TSA did not have a process in place to assess or identify the cause for equipment-based test failures or the capability to independently assess whether deployed explosive detection systems are operating at the correct detection standards. We found that, notwithstanding an intervening investment of over $550 million, TSA had not improved checked baggage screening since our 2009 report on the same issue. (*Vulnerabilities Exist in TSA's Checked Baggage Screening Operations*, OIG-14-142, Sept. 2014)

- In January 2012, we conducted covert testing of access controls to secure airport areas and identified significant access control vulnerabilities, meaning uncleared individuals could have unrestricted and unaccompanied access to the most vulnerable parts of the airport — the aircraft and checked baggage. (*Covert Testing of Access Controls to Secured Airport Areas*, OIG-12-26, Jan. 2012)

- In 2011, we conducted covert penetration testing on the previous generation of AIT machines in use at the time; the testing was far broader than the most recent testing, and likewise discovered significant vulnerabilities. (*Penetration Testing of Advanced Imaging Technology*, OIG-12-06, Nov. 2011)

The DHS Response

The Department's response to our most recent findings has been swift and definite. For example, within 24 hours of receiving preliminary results of OIG covert penetration testing, the Secretary summoned senior TSA leadership and directed that an immediate plan of action be created to correct deficiencies uncovered by our testing. Moreover, DHS has initiated a program — led by members of Secretary Johnson's leadership team — to conduct a focused analysis on issues that the OIG has uncovered, as well as other matters. These efforts have already resulted in significant changes to TSA leadership, operations, training, and policy, although the specifics of most of those changes cannot be discussed in an open setting, and should, in any event, come from TSA itself.

TSA has put forward a plan, consistent with our recommendations, to improve checkpoint quality in three areas: technology, personnel, and procedures. This plan is appropriate because the checkpoint must be considered as a single system: the most effective technology is useless without the right personnel, and the personnel need to be guided by the appropriate procedures. Unless all three elements are operating effectively, the checkpoint will not be effective.

We will be monitoring TSA's efforts to increase the effectiveness of checkpoint operations and will continue to conduct covert testing. Consistent with our obligations under the Inspector General Act, we will report our results to this Committee as well as other committees of jurisdiction.

TSA has also been making significant progress on many additional, outstanding recommendations from prior reports.

The Importance of Independent Oversight

I have been gratified by the Department's response to our most recent covert testing and believe that this episode serves as an illustration of the value of the Office of Inspector General, particularly when coupled with a Department leadership that understands and appreciates objective and independent oversight. This review, like the dozens of reviews before it, was possible only because my office and my auditors had unfettered access to the information we needed.

As this Committee knows, our ability to gain access to information is under attack as a result of a recent memorandum by the Department of Justice's Office of Legal Counsel. This memorandum, purporting to interpret Congressional intent, comes to a conclusion that is absurd on its face: that the reference to "all records" in section 6(a) of the *Inspector General Act of 1978* somehow does not really mean "all records." The underpinning and backbone of our work – proven to be effective for more than 30 years – has now been called into question. The Department of Justice apparently believes that it is up to those being audited to determine what information gets disclosed. This is an inherent conflict of interest and upends the professional standards for auditors and investigators. Inspectors General need to follow the facts wherever they lead, and must have unfettered access to all of the agency's information to do so.

I believe I speak for the entire IG community in expressing my gratitude to this Committee for the legislation currently pending in the House, HR 2395, the *Inspector General Empowerment Act of 2015*. This legislation would fix the misguided attempt to restrict access to records, and would restore IG independence and empower IGs to conduct the kind of rigorous, independent and thorough oversight that taxpayers expect and deserve.

The legislation would also improve and streamline the way we do business. For example, it exempts us from some of the requirements when matching data from two or more data systems within the federal government. This will allow us to be able to complete some audits far more quickly than we would otherwise be able. For example, we conducted an audit that compared TSA's aviation worker data against information on individuals who were known to the Intelligence Community. Specifically, we asked the National Counterterrorism Center (NCTC) to perform a data match of over 900,000 airport workers with access to secure areas against the NCTC's Terrorist Identities Datamart Environment (TIDE). As a result of this match, we identified 73 individuals with terrorism-related category codes who also had active credentials.

According to TSA officials, current interagency policy prevents the agency from receiving all terrorism-related codes during vetting. TSA officials recognize that not receiving these codes represents a weakness in its program, and informed us that TSA cannot guarantee that it can consistently identify all questionable individuals without receiving these categories. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015).

Our audit broke new ground and was able to identify an area of significant vulnerability. However, under the current rules, it took *eighteen months* to receive authorization to match the data sets of the two agencies to look for overlaps. The *Inspector General Empowerment Act of 2015* would eliminate those barriers and equip us with an important and powerful analytic tool in our quest to identify waste, fraud, and abuse within the federal government.

TSA and the Asymmetric Threat

Nowhere is the asymmetric threat of terrorism more evident than in the area of aviation security. TSA cannot afford to miss a single, genuine threat without potentially catastrophic consequences, and yet a terrorist only needs to get it right once. Securing the civil aviation transportation system remains a formidable task — TSA is responsible for screening travelers and baggage for more than 1.8 million passengers a day at 450 of our Nation's airports. Complicating this responsibility is the constantly evolving threat by adversaries willing to use any means at their disposal to incite terror.

The dangers TSA must contend with are complex and not within its control. Recent media reports have indicated that some in the U.S. intelligence community warn terrorist groups like the Islamic State (ISIS) may be working to build the capability to carry out mass casualty attacks, a significant departure from — and posing a different type of threat — than simply encouraging lone wolf attacks. According to these media reports, a mass casualty attack has become more likely in part because of a fierce competition with other terrorist networks: being able to kill opponents on a large scale would allow terrorist groups such as ISIS to make a powerful showing. We believe such an act of terrorism would likely be designed to impact areas where people are concentrated and vulnerable, such as the Nation's commercial aviation system.

Mere Intelligence is Not Enough

In the past, officials from TSA, in testimony to Congress, in speeches to think tanks, and elsewhere, have described TSA as an intelligence-driven organization. According to TSA, it continually assesses intelligence to develop countermeasures in order to enhance these multiple layers of security at airports and onboard aircraft. This is a necessary thing, but it is not sufficient.

In the vast majority of the instances, the identities of those who commit terrorist acts were simply unknown to or misjudged by the intelligence community. Terrorism, especially suicide terrorism, depends on a cadre of newly-converted individuals who are often unknown to the intelligence community. Moreover, the threat of ISIS or Al Qaeda inspired actors — those who have no formal ties to the larger organizations but who simply take inspiration from them — increases the possibilities of a terrorist actor being unknown to the intelligence community.

Recent history bears this out:

- 17 of the 19 September 11th hijackers were unknown to the intelligence community. In fact, many were recruited specifically because they were unknown to the intelligence community.

- Richard Reid, the 2002 "shoe bomber," was briefly questioned by the French police, but allowed to board an airplane to Miami. He had the high explosive PETN in his shoes, and but for the intervention of passengers and flight crew, risked bringing down the aircraft.

- The Christmas Day 2009 bomber, who was equipped with a sophisticated non-metallic explosive device provided by Al Qaeda, was known to certain elements of the intelligence community but was not placed in the Terrorist Screening Database, on the Selectee List, or on the No Fly List. A bipartisan Senate report found there were systemic failures across the Intelligence Community, which contributed to the failure to identify the threat posed by this individual.

- The single most high profile domestic terrorist attack since 9/11, the Boston Marathon bombing, was masterminded and carried out by Tamerlan Tsarnaev, an individual who approximately two years earlier was judged by the FBI not to pose a terrorist threat, and who was not within any active U.S. Government databases.

Of course, there are instances in which intelligence can foil plots that screening cannot detect — such as the 2006 transatlantic aircraft plot, utilizing liquid explosives; the October 2010 discovery of U.S.-bound bombs concealed in printer cartridges on cargo planes in England and Dubai; and the 2012 discovery that a second generation nonmetallic device, designed for use onboard aircraft, had been produced.

What this means is that there is no easy substitute for the checkpoint. The checkpoint must necessarily be intelligence driven, but the nature of terrorism today means that each and every passenger must be screened in some way.

Beyond the Checkpoint

Much of the attention has been focused on the checkpoint, since that is the primary and most visible means of entry onto aircraft. But effective checkpoint operations simply are not of themselves sufficient. Aviation security must also look at other areas to determine vulnerabilities.

Assessment of passenger risk

We applaud TSA's efforts to use risk-based passenger screening because it allows TSA to focus on high-risk or unknown passengers instead of known, vetted passengers who pose less risk to aviation security.

However, we have had deep concerns about some of TSA's previous decisions about this risk. For example, we recently assessed the Precheck initiative, which is used at about 125 airports to identify low-risk passengers for expedited airport checkpoint screening. Starting in 2012, TSA massively increased the use of Precheck. Some of the expansion, for example allowing Precheck to other Federal Government-vetted or known flying populations, such as those in the CBP Trusted Traveler Program, made sense. In addition, TSA continues to promote participation in Precheck by passengers who apply, pay a fee, and undergo individualized security threat assessment vetting.

However, we believe that TSA's use of risk assessment rules, which granted expedited screening to broad categories of individuals unrelated to an individual assessment of risk, but rather on some questionable assumptions about relative risk based on other factors, created an unacceptable risk to aviation security.[1] Additionally, TSA used "managed inclusion" for the general public, allowing random passengers access to Precheck lanes with *no* assessment of risk. Additional layers of security TSA intended to provide, which were meant to compensate for the lack of risk assessment, were often simply not present.

We made a number of recommendations as a result of several audits and inspections. Disappointingly, when the report was issued, TSA did not concur with the majority of our 17 recommendations. At the time, I testified that I believed this represented TSA's failure to understand the gravity of the risk that they were assuming. I am pleased to report, however, that we have recently made significant progress in getting concurrence and compliance with these recommendations.

---

[1] As an example of Precheck's vulnerabilities, we reported that, through risk assessment rules, a felon who had been imprisoned for multiple convictions for violent felonies while participating in a domestic terrorist group was granted expedited screening through Precheck.

For example, I am pleased to report that TSA has stopped using one form of Managed Inclusion and has deactivated certain risk assessment rules that granted expedited screening through PreCheck lanes. However, TSA continues to use other risk assessment rules that we recommended it discontinue. We are communicating with TSA officials about these risk assessment rules; TSA recently told us it is reevaluating its position and we are awaiting formal documentation to that effect. I urge TSA to concur with our recommendations to address Precheck security vulnerabilities we identified during our review. As you may know, the House passed the *Securing Expedited Screening Act* (HR 2127), legislation that would eliminate Managed Inclusion altogether and limit risk assessment rules.

Access to secure areas

TSA is responsible, in conjunction with the 450 airports across the country, to ensure that the secure areas of airports, including the ability to access aircraft and checked baggage, are truly secure. In our audit work, we have had reason to question whether that has been the case. We conducted covert testing in 2012 to see if auditors could get access to secure areas by a variety of means. While the results of those tests are classified, they were similar to the other covert testing we have done, which was disappointing.

Additionally, as we discuss below, TSA's oversight of airports when it comes to employee screening needs to be improved. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015)

We are doing additional audit and inspection work in this area, determining whether controls over access media badges issued by airport operators is adequate. We are also engaging in an audit of the screening process for the Transportation Worker Identification Credential program (TWIC) to see whether it is operating effectively and whether the program's continued eligibility processes ensures that only eligible TWIC card holders remain eligible.

Other questionable investments in aviation security

TSA uses behavior detection officers to identify passenger behaviors that may indicate stress, fear, or deception. This program, Screening Passengers by Observation Techniques (SPOT), includes more than 2,800 employees and has cost taxpayers about $878 million from FYs 2007 through 2012.

We understand the desire to have such a program. Israel is foremost in their use of non-physical screening, although the differences in size, culture, and attitudes about civil liberties make such a program difficult to adopt in this country. In the United States, sharp-eyed government officials were able to assess behavior to prevent entry to terrorists on two separate occasions:

- Ahmed Ressam's plot to blow up the Los Angeles International Airport on New Year's Eve 1999 was foiled when a U.S. Customs officer in Port Angeles, Washington, thought Ressam was acting "hinky" and directed a search of his car, finding numerous explosives and timers.

- In 2001, a U.S. immigration officer denied entry to the United States to Mohammed al Qahtani, based on Qahtani's evasive answers to his questions. Later investigation by the 9/11 Commission revealed that Qahtani was to be the 20th hijacker, assigned to the aircraft that ultimately crashed in Shanksville, Pennsylvania.

However, we have deep concerns that the current program is both expensive and ineffective. In 2013, we audited the SPOT program and found that TSA could not ensure that passengers were screened objectively, nor could it show that the program was cost effective or merited expansion. We noted deficiencies in selection and training of the behavior detection officers. Further, in a November 2013 report on the program, the Government Accountability Office (GAO) reported that TSA risked funding activities that had not been determined to be effective. Specifically, according to its analysis of more than 400 studies, GAO concluded that SPOT program behavioral indicators might not be effective in identifying people who might pose a risk to aviation security. TSA has taken steps to implement our recommendations and improve the program. However, we continue to have questions with regard to the program and this fiscal year will conduct a Verification Review, with regard to — among other things — performance management, training, and financial accountability, and selection, allocation, and performance of the Behavior Detection Officers.

Likewise, the Federal Air Marshal Program costs the American taxpayer more than $800 million per year. The program was greatly expanded after 9/11 to guard against a specific type of terrorist incident. In the intervening years, terrorist operations and intentions have evolved. We will be auditing the Federal Air Marshal Program this year to determine whether the significant investment of resources in the program is justified by the risk.

TSA's role as regulator

TSA has dual aviation security responsibilities, one to provide checkpoint security for passengers and baggage and another to oversee and regulate airport security provided by airport authorities. The separation of responsibility for airport security between TSA and the airport authorities creates a potential vulnerability in safeguarding the system. Concern exists about which entity is accountable for protecting areas other than checkpoints in relation to airport worker vetting, perimeter security, and cargo transport. We have also assessed whether TSA is appropriately regulating airports, such as whether it ensures airports' compliance with security regulations. We have found shortfalls.

In the case of airport worker vetting, for example, TSA relies on airports to submit complete and accurate aviation worker application data for vetting. In a recent audit, we found TSA does not ensure that airports have a robust verification process for criminal history and authorization to work in the United States, or sufficiently track the results of their reviews. TSA also did not have an adequate monitoring process in place to ensure that airport operators properly adjudicated credential applicants' criminal histories. TSA officials informed us that airport officials rarely or almost never documented the results of their criminal history reviews electronically. Without sufficient documentation, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events.

As a result, TSA is required to conduct manual reviews of aviation worker records. Due to the workload at larger airports, this inspection process may look at as few as one percent of all aviation workers' applications. In addition, inspectors were generally reviewing files maintained by the airport badging office, which contained photocopies of aviation worker documents rather than the physical documents themselves. An official told us that a duplicate of a document could hinder an inspector's ability to determine whether a document is real or fake because a photocopy may not be matched to a face and may not show the security elements contained in the identification document.

Additionally, we identified thousands of aviation worker records that appeared to have incomplete or inaccurate biographic information. Without sufficient documentation of criminal histories or reliable biographical data, TSA cannot systematically determine whether individuals with access to secured areas of the airports are free of disqualifying criminal events, and TSA has thus far not addressed the poor data quality of these records. (*TSA Can Improve Aviation Worker Vetting (Redacted)*, OIG-15-98, June 2015)

Further, the responsibility for executing perimeter and airport facility security is in the purview of the 450 local airport authorities rather than TSA. There is no clear structure for responsibility, accountability, and authority at most airports, and the potential lack of local government resources makes it difficult for TSA to issue and enforce higher standards to counter new threats. Unfortunately, intrusion prevention into restricted areas and other ground security vulnerabilities is a lower priority than checkpoint operations.

Conclusion

Making critical changes to TSA's culture, technology, and processes is not an easy undertaking. However, a commitment to and persistent movement towards effecting such changes — including continued progress towards complying with our recommendations — is paramount to ensuring transportation security. We recognize and are encouraged by TSA's steps towards compliance with our recent recommendations. Without a sustained commitment to addressing known vulnerabilities, the agency risks compromising the safety of the Nation's transportation systems.

Mr. Chairman, this concludes my prepared statement. I welcome any questions you or other Members of the Committee may have.

Appendix A
Recent OIG Reports on the Transportation Security Administration

Covert Testing of the TSA's Passenger Screening Technologies and Processes at Airport Security Checkpoints (Unclassified Summary), OIG-15-150, September 2015

Use of Risk Assessment within Secure Flight (Redacted), OIG-14-153, June 2015

TSA Can Improve Aviation Worker Vetting (Redacted), OIG-15-98, June 2015

The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program, OIG-15-86, May 2015

Allegation of Granting Expedited Screening through TSA PreCheck Improperly (Redacted), OIG-15-45, March 2015

Security Enhancements Needed to the TSA PreCheck Initiative (Unclassified Summary), OIG-15-29, January 2015

Vulnerabilities Exist in TSA's Checked Baggage Screening Operations (Unclassified Spotlight), OIG-14-142, September 2014

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-11-47	DHS Department-wide Management of Detection Equipment	3/2/2011	We recommend that the Deputy Under Secretary for Management reestablish the Joint Requirements Council.	Closed	Agreed
OIG-11-47	DHS Department-wide Management of Detection Equipment	3/2/2011	We recommend that the Deputy Under Secretary for Management: Establish a commodity council for detection equipment, responsible for: Coordinating, communicating, and, where appropriate, strategically sourcing items at the department level or identifying a single source commodity manager; Standardizing purchases for similar detection equipment; and Developing a data dictionary that standardizes data elements in inventory accounts for detection equipment.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	No Response

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-12-06	Transportation Security Administration Penetration Testing of Advanced Imaging Technology	11/21/2011	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a comprehensive strategic plan for the Screening of Passengers by Observation Techniques (SPOT) program that includes—Mission, goals, objectives, and a system to measure performance; A training strategy that addresses the goals and objectives of the SPOT program; A plan to identify external partners integral to program success, such as law enforcement agencies, and take steps to ensure that effective relationships are established; and A financial plan that includes identification of priorities, goals, objectives, and measures; needs analysis; budget formulation and execution; and expenditure tracking.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement controls to ensure completeness, accuracy, authorization, and validity of referral data entered into the Performance Measurement Information System.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan that provides recurrent training to Behavior Detection Officer (BDO) instructors and BDOs.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a plan to assess BDO instructor performance in required core competencies on a regular basis.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities monitor and track the use of BDOs for non-SPOT related duties to ensure BDOs are used in a cost-effective manner and in accordance with the mission of the SPOT program.	Closed	Agreed
OIG-13-91	Transportation Security Administration's Screening of Passengers by Observation Techniques	5/29/2013	We recommend that the Assistant Administrator, Office of Security Capabilities develop and implement a process for identifying and addressing issues that may directly affect the success of the SPOT program such as the selection, allocation, and performance of BDOs.	Closed	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-13-99	Transportation Security Administration's Screening Partnership Program	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator expedite developing and implementing procedures to ensure that decisions on Screening Partnership Program applications and procurements are fully documented according to applicable Department and Federal guidance.	Closed	Agreed
OIG-13-99	Transportation Security Administration's Screening Partnership Program	6/20/2013	We recommend that the Transportation Security Administration Deputy Administrator establish and implement quality assurance procedures to ensure that the most relevant and accurate information is used when determining eligibility and approving airports' participation in the Screening Partnership Program.	Closed	Agreed
OIG-13-120	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and approve a single, comprehensive deployment strategy that addresses short- and long term goals for screening equipment.	Closed	Agreed
OIG-13-120	Transportation Security Administration's Deployment and Use of Advanced Imaging Technology	9/16/2013	We recommend that the Deputy Administrator, Transportation Security Administration: Develop and implement a disciplined system of internal controls from data entry to reporting to ensure PMIS data integrity.	**Closed***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	Closed	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	Open - Resolved	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	9/9/2014	This recommendation is classified.	**Closed***	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	12/16/2014	This recommendation is classified.	Open – Resolved	Agreed
OIG-14-142	(U) Vulnerabilities Exist in TSA's Checked Baggage Screening Operations	12/16/2014	This recommendation is classified.	Open – Unresolved	Agreed
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	Closed	Agreed
OIG-14-153	Use of Risk Assessment within Secure Flight	9/9/2014	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Unresolved	Disagreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Open – Resolved***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Employ exclusion factors to refer TSA PreCheck ® passengers to standard security lane screening at random intervals.	**Open – Resolved***	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	**Closed***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Security Operations: Develop and implement a strategy to address the TSA PreCheck ® lane covert testing results.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	Recommendation includes Sensitive Security Information.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Provide an explanation of TSA PreCheck ® rules and responsibilities to all enrollment center applicants and include this information in eligibility letters.	Open – Resolved	Agreed
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Assistant Administrator for the Office of Intelligence and Analysis: Coordinate with Federal Government and private partners to ensure all TSA PreCheck ® eligible populations receive the rules and responsibilities when notifying participants of eligibility.	Open – Resolved	**Agreed****
OIG-15-29	Security Enhancements Needed to the TSA PreCheck™ Initiative	1/28/2015	We recommend that the TSA Chief Risk Officer: Develop consolidated guidance outlining processes and procedures for all offices involved in the TSA PreCheck ® initiative.	Open – Resolved	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-45	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679)	3/16/2015	Recommendation includes Sensitive Security Information.	Open – Unresolved	Disagreed
OIG-15-45	Allegations of Granting Expedited Screening through TSA PreCheck Improperly (OSC File No. DI-14-3679)	3/16/2015	We recommend that the TSA Assistant Administrator for Security Operations: Modify standard operating procedures to clarify Transportation Security Officer (TSO) and supervisory TSO authority to refer passengers with TSA PreCheck boarding passes to standard screening lanes when they believe that the passenger should not be eligible for TSA PreCheck screening.	**Closed***	Agreed
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations develop and implement a preventive maintenance validation process to verify that required routine maintenance activities are completed according to contractual requirements and manufacturers' specifications. These procedures should also include instruction for appropriate TSA airport personnel on documenting the performance of Level 1 preventive maintenance actions.	**Open – Resolved***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

Report No.	Report Title	Date Issued	Recommendation	Current Status	Mgmt. Response
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend that TSA's Office of Security Capabilities and Office of Security Operations: Develop and implement policies and procedures to ensure that local TSA airport personnel verify and document contractors' completion of corrective maintenance actions. These procedures should also include quality assurance steps that would ensure the integrity of the information collected.	**Open – Resolved***	Agreed
OIG-15-86	The Transportation Security Administration Does Not Properly Manage Its Airport Screening Equipment Maintenance Program	5/6/2015	We recommend TSA's Office of Acquisition enhance future screening equipment maintenance contracts by including penalties for noncompliance when it is determined that either preventive or corrective maintenance has not been completed according to contractual requirements and manufacturers' specifications.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA follow up on its request to determine if its credential vetting program warrants the receipt of additional categories of terrorism related records.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA issue guidance requiring annual security inspection process to include verification of original documentation supporting airport adjudication of an applicant's criminal history and work authorization.	**Open – Resolved***	Agreed

Appendix B
Status of Recommendations for Selected OIG Reports on TSA
(As of 10.28.15)

OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA pilot FBI's Rap Back program and take steps to institute recurrent vetting of criminal histories at all commercial airports.	**Open – Resolved***	No Response
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA require airports to put an end date to credentials of individuals allowed to work in the United States temporarily.	**Open – Resolved***	Agreed
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend TSA analyze denials of credentials due to lawful status issues to identify airports with specific weaknesses, and address these weaknesses with airport badging officials as necessary.	**Open – Resolved***	No Response
OIG-15-98	TSA Can Improve Aviation Worker Vetting	6/4/2015	We recommend that TSA implement all necessary data quality checks necessary to ensure that all credential application data elements required by TSA Security Directive 1542-04-08G are complete and accurate.	**Open – Resolved***	No Response
OIG-15-150	(U) Covert Testing of the Transportation Security Administration's Passenger Screening Technologies and Processes at Airport Security Checkpoints	9/22/2015	This recommendation is classified.	Open-Unresolved	Agreed

***These recommendations were either resolved or closed within the last six months.**

****TSA management changed their response from disagreed to agreed.**

Appendix C
Current and Planned OIG Work on TSA

Projects In-Progress:

Project Topic	Objective
TSA Security Vetting of Passenger Rail Reservation Systems	Determine the extent to which TSA has policies, processes, and oversight measures to improve security at the National Railroad Passenger Corporation (AMTRAK).
Reliability of TWIC Background Check Process	Determine whether the screening process for the Transportation Worker Identification Credential program (TWIC) is operating effectively and whether the program's continued eligibility processes ensure that only eligible TWIC card holders remain eligible.
TSA's Security Technology Integrated Program (STIP)	Determine whether TSA has incorporated adequate IT security controls for passenger and baggage screening STIP equipment to ensure it is performing as required.
TSA's Controls Over Access Media Badges	Identify and test selected controls over access media badges issued by airport operators.
TSA's Risk-Based Strategy	Determine the extent to which TSA's intelligence-driven, risk-based strategy informs security and resource decisions to protect the traveling public and the Nation's transportation systems.
TSA's Office of Human Capital Contracts	Determine whether TSA's human capital contracts are managed effectively, comply with DHS' acquisition guidelines, and are achieving expected goals.

Upcoming Projects:

Project Topic	Objective
Federal Air Marshal Service's Oversight of Civil Aviation Security	Determine whether the Federal Air Marshal Service adequately manages its resources to detect, deter, and defeat threats to the civil aviation system.
TSA Carry-On Baggage Penetration Testing	Determine the effectiveness of TSA's carry-on baggage screening technologies and checkpoint screener performance in identifying and resolving potential security threats at airport security checkpoints.
Airport Security Capping Report	Synthesize the results of our airport security evaluations into a capping report that groups and summarizes identified weaknesses and root causes and recommends how TSA can systematically and proactively address these issues at airports nationwide.
TSA's Classification Program	Determine whether TSA is effectively managing its classification program and its use of the Sensitive Security Information designation.
TSA's Office of Intelligence and Analysis	Determine whether TSA's Office of Intelligence and Analysis is effectively meeting its mission mandates.

John Roth – Inspector General, Department of Homeland Security

The U.S. Senate on March 6, 2014 confirmed the nomination of John Roth to be Inspector General of the Department of Homeland Security.

Mr. Roth, who most recently served as Director of the Office of Criminal Investigations at the Food and Drug Administration , was nominated to lead the DHS Office of Inspector General by President Barack Obama.

Prior to his move to the FDA in June 2012, Mr. Roth had a 25-year career as a federal prosecutor and senior leader in the Department of Justice. He began his career in 1987 as Assistant U.S. Attorney for the Eastern District of Michigan. From 1994 to 1999, he was Chief of the Narcotics Section at the U.S. Attorney's Office for the Southern District of Florida.

From 1999 to 2004, Mr. Roth served as Section Chief at DOJ's Criminal Division for the Narcotic and Dangerous Drugs Section and the Asset Forfeiture and Money Laundering Section. During that time, he served on a detail as Senior Counsel and Team Leader for the congressionally chartered 9/11 Commission and helped to write a well-regarded monograph on terrorist financing, and assisted in completing the Commission's final report.

In 2004, Mr. Roth became the chief of the Fraud and Public Corruption section at the U.S. Attorney's Office in the District of Columbia, supervising a staff of prosecutors investigating fraud and public corruption cases. In 2007, he served as Acting Deputy Assistant Attorney General in the Criminal Division and became chief of staff to the Deputy Attorney General in 2008.

Mr. Roth culminated his DOJ career as the department's lead representative on the Financial Action Task Force in Paris, France, an intergovernmental organization fighting against money laundering and terrorist financing.

Mr. Roth earned a B.A. and a law degree from Wayne State University in Detroit.

Privacy Impact Assessment Update
for

TSA Advanced Imaging Technology

DHS/TSA/PIA-032(d)

December 18, 2015

Contact Point
Jill Vaughan
Assistant Administrator
Office of Security Capabilities
OSCCommunications@dhs.gov

Reviewing Official
Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security
(202) 343-1717

Abstract

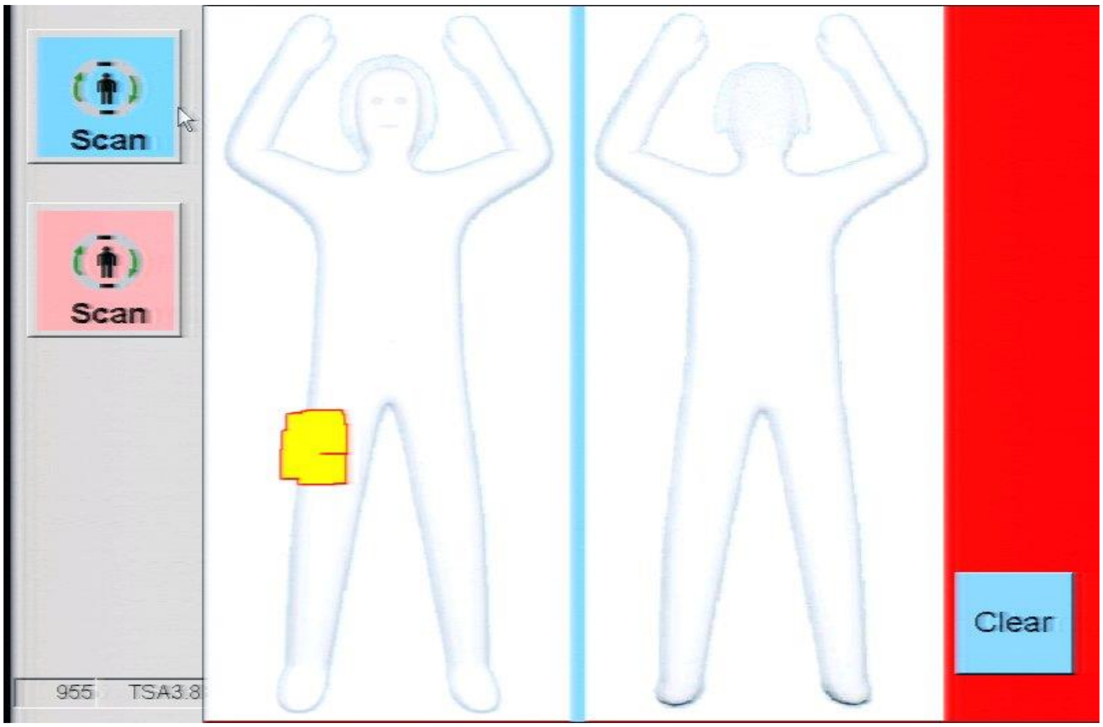
The Transportation Security Administration (TSA) has deployed Advanced Imaging Technologies (AIT) for operational use to detect threat objects carried on persons entering airport sterile areas. AIT identifies potential threat objects on the body using Automatic Target Recognition (ATR) software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt opt-out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers. TSA does not store any personally identifiable information from AIT screening.

Introduction

Under the Aviation and Transportation Security Act (ATSA),[1] TSA is responsible for security in all modes of transportation, and must assess threats to transportation, enforce security-related regulations and requirements, and ensure the adequacy of security measures at airports and other transportation facilities. TSA has deployed AIT for operational use to detect threat objects carried on persons entering airport sterile areas.[2] AIT identifies potential threat objects on the body using ATR software to display the location of the object on a generic figure as opposed to displaying the image of the individual. TSA currently uses AIT equipped with ATR to quickly, and without physical contact, screen passengers for prohibited items including weapons, explosives, and other metallic and non-metallic threat objects hidden under layers of clothing. ATR software identifies objects on the body and highlights the location of the object with bounding boxes on a generic figure.[3] ATR eliminates the need for a remote image since it is a generic image that can be presented on a monitor connected to the AIT and co-located with the officer assisting the screened individual. The individual will undergo physical screening if ATR alarms for the presence of an object.

[1] Pub. L. 107-71
[2] "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.
[3] For additional information, *see* DHS/TSA/PIA-032 TSA Advanced Imaging Technology and associated updates, *available at* www.dhs.gov/privacy.

A sample image from a system using ATR appears below:



Storage of images

The AIT devices at airports do not have the ability to store images..[4] The ATR generic image is maintained on the monitor only for as long as it takes to resolve any alarms. The AIT equipment does not generate or retain an underlying image of the individual.

What to expect

Because the ATR software replaces the individual's image with that of a generic figure, the monitor will be co-located with the individual being screened. The screening officer will view both the individual and the ATR image. If there is an alarm, the physical screening will target the location indicated by the ATR software. If there are multiple alarms, the individual may receive a full screening.

---

[4] Initial versions of AIT were manufactured with storage functions that TSA required manufacturers to disable prior to installation at the airport. Current versions of the software installed at airports do not include any storage function to disable, and eliminate the need to perform the disabling of the storage function.

Reason for this Update

TSA is updating the AIT PIA to reflect a change to the operating protocol regarding the ability of individuals to opt out of AIT screening in favor of physical screening. While passengers may generally decline AIT screening in favor of physical screening, TSA may direct mandatory AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

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. Section 222(2) of the Homeland Security Act of 2002 states that the Chief Privacy Officer shall assure that information is handled in full compliance with the fair information practices 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 that 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 information on AIT technologies on its website (www.TSA.gov), and published an original PIA on AIT in January 2008 with subsequent updates reflecting operational or technology changes.[5] In 2013, TSA published a Notice of Proposed Rule Making on the use of AIT in screening operations which received more than 5500 comments from the public. TSA expects to publish its Final Rule in 2016. This PIA update reflects TSA's continued transparency on its use of AIT.

[5] For all TSA Privacy Impact Assessments, please visit http://www.dhs.gov/privacy-documents-transportation-security-administration-tsa.

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 screening using AIT generally will have the option to decline an AIT screening in favor of physical screening. Given the implementation of ATR and the mitigation of privacy issues associated with the individual image generated by previous versions of AIT not using ATR, and the need to respond to potential security threats, TSA will nonetheless mandate AIT screening for some passengers as warranted by security considerations in order to safeguard transportation security.

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.[6] 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.[7] AIT technologies are being used to identify prohibited items, particularly non-metallic threat objects and liquids secreted on the body. ATR software identifies the location of the potential prohibited item on a generic figure. Because of the greater privacy protections provided by a generic figure, the image monitor for ATR is co-located with the AIT so that the screening officer can view it.

4. Principle of Data 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).

TSA does not collect PII with this technology. AIT with ATR does not generate an individual image but rather overlays the location of objects on a generic image.

---

[6] 49 U.S.C. § 114(d).
[7] 49 U.S.C. § 44912 note.

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.

TSA uses AIT solely for purposes of identifying objects that may be threat items. Once an alarm is resolved, the generic image is cleared from the screen, and therefore cannot be used for any other purpose or shared with anyone. Because there are no images to share, they cannot be used in any other context inside DHS or 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 ATR generated image is accurate, timely, and complete and is directly relevant to the identification of threat objects. Potential threat items are resolved through a directed physical screening before the individual is cleared to enter the sterile 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.

AIT data is transmitted in a proprietary format to the viewing monitor, and cannot be lost, modified, or disclosed. TSA's decision not to retain images mitigates further data storage security issues.

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.

No PII is generated by AIT using ATR.

Conclusion

AIT technology improves threat detection capabilities for both metallic and non-metallic threat objects, while improving the passenger experience for those passengers for whom a physical screening is uncomfortable. ATR software provides even greater privacy protections by eliminating the human image that appeared with previous AIT technologies.

Responsible Officials

Jill Vaughan
Assistant Administrator
Office of Security Capabilities

Approval Signature

Original signed copy on file with the DHS Privacy Office

____

Karen L. Neuman
Chief Privacy Officer
Department of Homeland Security