
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
Attorney 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	
Passenger Screening Using Advanced Imaging Technology, Final Rule (Mar. 3, 2016) (81 Fed. Reg. 11364)	JA 000001
Passenger Screening Using Advanced Imaging Technology; Regulatory Impact Analysis and Final Regulatory Flexibility Analysis (Feb. 18, 2016)	JA 000044
Privacy Impact Assessment for TSA Whole Body Imaging (Jan. 2, 2008)	JA 000203
TSA Blog, <i>Pilot Program Tests Millimeter Wave for Primary Passenger Screening</i> (Feb. 20, 2009).....	JA 000212
Memorandum from TSA Acting Administrator Gale D. Rossides to DHS Secretary Janet Napolitano (Feb. 27, 2009)	JA 000215
Letter from EPIC <i>et al.</i> to Secretary Janet Napolitano (May 31, 2009).....	JA 000217
Letter from Acting TSA Administrator Gale Rossides to EPIC (Jun. 19, 2009).....	JA 000220
TSA, Imaging Technology Airport Brief, slide 6 (Jul. 2009),	JA 000222
<i>Intelligence Reform: The Lessons and Implications of the Christmas Day Attack: Hearing Before the Senate Committee on Homeland Security and Government Affairs, 111th Congress</i> (Post-hearing questions submitted to the Honorable Janet A. Napolitano from Senator Daniel K. Akaka) (Jan. 20, 2010)	JA 000223

<i>Intelligence Reform: The Lessons and Implications of the Christmas Day Attack: Hearing Before the Senate Committee on Homeland Security and Government Affairs</i> , 111 th Congress (Post-hearing questions submitted to the Honorable Janet A. Napolitano from Senator Tom Coburn) (Jan. 20, 2010)	JA 000227
Letter from Representative Bennie G. Thompson to Gail Rossides, TSA Acting Administrator (Jan. 21, 2010)	JA 000234
Letter from EPIC <i>et al.</i> to Secretary Janet Napolitano and Chief Privacy Officer Mary Ellen Callahan (Apr. 21, 2010)	JA 000236
Letter from Secretary Janet Napolitano to Senator Susan Collins (Apr. 27, 2010)	JA 000245
Letter from Francine Francine J. Kerner, TSA Chief Counsel to EPIC <i>et al.</i> (May 28, 2010).....	JA 000246
TSA Blog, <i>Opt Out Turns Into Opt In</i> (Nov. 24, 2010)	JA 000257
<i>TSA Recent Scanner Trouble: Rea Strategy or Wasteful Smokescreen: Hearing Before the Subcommittee on Transportation Security the Comm. Of the Homeland Security</i> , 114 th Cong. (statement of Rep. Danny Davis on behalf of Ranking Member Sheila Jackson Lee) (Nov. 15, 2012)	JA 000264
TSA, <i>Passenger Screening Using AIT: Initial Regulatory Impact Analysis</i> (Mar. 19, 2013).....	JA 000265

VOLUME II

<i>Passenger Screening Using Advanced Imaging Technology</i> , 78 Fed. Reg. 18,287 (Mar. 26, 2013)	JA 000416
Comment of Anonymous (posted Apr. 1, 2013) (TSA-2013-0004-0114)	JA 000432
Comment of Milton John Schick (posted Apr. 2, 2013) (TSA-2013-0004-0162)	JA 000433

Comment of Mary Graham (posted Apr. 2, 2013) (TSA-2013-0004-0168)	JA 000434
Comment of Jean L. Cooper (posted Apr. 2, 2013) (TSA-2013-0004-0193)	JA 000435
Comment of Fred (posted Apr. 3, 2013) (TSA-2013-0004-0246)	JA 000438
Comment of Barbara Sheridan (posted Apr. 3, 2013) (TSA-2013-0004-0279)	JA 000439
Comment of Allison J. Jones (posted Apr. 4, 2013) (TSA-2013-0004-0327)	JA 000440
Comment of Dan (posted Apr. 4, 2013) (TSA-2013-0004-0342)	JA 000441
Comment of Anonymous (posted Apr. 4, 2013) (TSA-2013-0004-0343)	JA 000442
Comment of Anonymous (posted Apr. 8, 2013) (TSA-2013-0004-0390)	JA 000443
Comment of Michael Alan Muller (posted Apr. 8, 2013) (TSA-2013-0004-0401)	JA 000444
Comment of Donna A. Harrison (posted Apr. 10, 2013) (TSA-2013-0004-0478)	JA 000445
Comment of Donald Eugene Ryan (posted Apr. 17, 2013) (TSA-2013-0004-0596)	JA 000446
Comment of T.A. (posted Apr. 17, 2013) (TSA-2013-0004-0597)	JA 000447
Comment of Martin A. Dyckman (posted Apr. 17, 2013) (TSA-2013-0004-0599)	JA 000448
Comment of James L. Bareuther (posted Apr. 17, 2013) (TSA-2013-0004-0614)	JA 000449

Comment of Anonymous (posted Apr. 19, 2013) (TSA-2013-0004-0644)	JA 000450
Comment of Jeffress B. Hailand (posted Apr. 22, 2013) (TSA-2013-0004-0686)	JA 000454
Comment of Sola Egunyomi (posted Apr. 22, 2013) (TSA-2013-0004-0740)	JA 000455
Comment of Anonymous (posted Apr. 23, 2013) (TSA-2013-0004-0774)	JA 000460
Comment of Todd Edward Heimann (posted Apr. 23, 2013) (TSA-2013-0004-0916)	JA 000461
Comment of Ben Fox (posted Apr. 24, 2013) (TSA-2013-0004-1039)	JA 000462
Comment of Gayle M. (posted May 7, 2013) (TSA-2013-0004-1439)	JA 000463
Comment of Michael Gingrich (posted May 7, 2013) (TSA-2013-0004-1460)	JA 000464
Comment of Anonymous (posted May 7, 2013) (TSA-2013-0004-1490)	JA 000465
Comment of Anonymous (posted May 13, 2013) (TSA-2013-0004-1617)	JA 000466
Comment of Kaitlin Duck Sherwood (posted May 15, 2013) (TSA-2013-0004-1641)	JA 000467
Comment of Lloyd L. Jordan (posted May 16, 2013) (TSA-2013-0004-1643)	JA 000468
Comment of Chris Doyle (posted May 16, 2013) (TSA-2013-0004-1737)	JA 000469
Comment of W. Hughes (posted May 16, 2013) (TSA-2013-0004-1741)	JA 000470

Comment of Melissa E. Teates (posted May 20, 2013) (TSA-2013-0004-1823)	JA 000471
Comment of Abraham Richards Burnette (posted May 21, 2013) (TSA-2013-0004-1886)	JA 000472
Comment of Kaye Beach (posted May 21, 2013) (TSA-2013-0004-1901)	JA 000473
Comment of Rebecca Downing (posted May 21, 2013) (TSA-2013-0004-1976)	JA 000474
Comment of Anonymous (posted May 22, 2013) (TSA-2013-0004-2074)	JA 000475
Comment of Grejdi Gjura (posted May 22, 2013) (TSA-2013-0004-2109)	JA 000476
Comment of Robin Whitlock (posted May 22, 2013) (TSA-2013-0004-2169)	JA 000477
Comment of Karen Julie Lewis (posted May 23, 2013) (TSA-2013-0004-2197)	JA 000478
Comment of Vincent Wilkinson (posted May 28, 2013) (TSA-2013-0004-2288)	JA 000479
Comment of Marianne Cherrier Burns (posted May 29, 2013) (TSA-2013-0004-2397)	JA 000480
Comment of Bobbie Kent (posted May 29, 2013) (TSA-2013-0004-2442)	JA 000481
Comment of Anonymous (posted May 30, 2013) (TSA-2013-0004-2542)	JA 000482
Comment of Wade Allen (posted Jun. 3, 2013) (TSA-2013-0004-2702)	JA 000483
Comment of Anonymous (posted Jun. 3, 2013) (TSA-2013-0004-2721)	JA 000484

Comment of Kate (posted Jun. 4, 2013) (TSA-2013-0004-2740)	JA 000485
Comment of Anonymous (posted Jun. 4, 2013) (TSA-2013-0004-2785)	JA 000486
Comment of E. Kelly (posted Jun. 4, 2013) (TSA-2013-0004-2798)	JA 000487
Comment of Josh Schreibman (posted Jun. 5, 2013) (TSA-2013-0004-3066)	JA 000488
Comment of Daniel Linder (posted Jun. 6, 2013) (TSA-2013-0004-3196)	JA 000489
Comment of VSM (posted Jun. 7, 2013) (TSA-2013-0004-3218)	JA 000490
Comment of Anonymous (posted Jun. 10, 2013) (TSA-2013-0004-3303)	JA 00491
Comment of Joanne Frances Gladney-Naumer (posted Jun. 11, 2013) (TSA-2013-0004-3318)	JA 00492
Comment of Mary Kennedy (posted Jun. 11, 2013) (TSA-2013-0004-3427)	JA 000493
Comment of Vicki Warthen (posted Jun. 11, 2013) (TSA-2013-0004-3465)	JA 000494
Comment of Tom (posted Jun. 12, 2013) (TSA-2013-0004-3559)	JA 000495
Comment of Allyson Ramage (posted Jun. 12, 2013) (TSA-2013-0004-3585)	JA 000496
Comment of J. Hatfield (posted Jun. 12, 2013) (TSA-2013-0004-3599)	JA 000497
Comment of S.L. Hunt (posted Jun. 13, 2013) (TSA-2013-0004-3616)	JA 000498

Comment of Kelly McConnell (posted Jun. 17, 2013) (TSA-2013-0004-3699)	JA 000499
Comment of Tamika Harris (posted Jun. 18, 2013) (TSA-2013-0004-3742)	JA 000500
Comment of Anonymous (posted Jun. 18, 2013) (TSA-2013-0004-3769)	JA 000503
Comment of Tom Ritter (posted Jun 19, 2013) (TSA-2013-0004-3814)	JA 000512
Comment of Nick B. (posted Jun. 19, 2013) (TSA-2013-0004-3830)	JA 000513
Marc N. Evans (posted Jun. 20, 2013) (TSA-2013-0004-3980)	JA 000514
Comment of Anonymous (posted Jun. 20, 2013) (TSA-2013-0004-4025)	JA 000515
Comments of the National Center for Transgender Equality (posted Jun. 24, 2013) (page 20) (TSA-2013-0004-4070)	JA 000517
Comment of Anonymous (posted Jun. 24, 2013) (TSA-2013-0004-4086)	JA 000518
Comment of Robin Douglas Kunzler (posted Jun. 25, 2013) (TSA-2013-0004-4103).....	JA 000519
Comment of Margaret E. Hopper (posted Jun. 25, 2013) (TSA-2013-0004-4120)	JA 000520
Comment of Anonymous (posted Jun. 25, 2013) (TSA-2013-0004-4172)	JA 000521
Comments of the Transgender Law Center (posted Jun. 25, 2013) (TSA-2013-0004-4203).....	JA 000522
Comment of Michelle Patterson (posted Jun. 25, 2013) (TSA-2013-0004-4226)	JA 000528

Comments of the Competitive Enterprise Institute and Robert L. Crandall (posted Jun. 25, 2013) (TSA-2013-0004-4239)	JA 000529
Comment of Jeffrey A. Strauser (posted Jun. 25, 2013) (TSA-2013-0004-4265)	JA 000539
Comment of Anonymous (posted Jun. 26, 2013) (TSA-2013-0004-4414)	JA 000540
Comment of C.J. Lindell (posted Jun. 27, 2013) (TSA-2013-0004-4447)	JA 000541
Comment of Mark H. Lyon (posted Jun. 27, 2013) (TSA-2013-0004-4488)	JA 000542
Comments of the Pride Foundation (posted Jun. 27, 2013) (TSA-2013-0004-4519)	JA 000544
Comment of Anonymous (posted Jun. 27, 2013) (TSA-2013-0004-4553)	JA 000551
Comment of Anonymous (posted Jun. 27, 2013) (TSA-2013-0004-4562)	JA 000552
Comment of Amber Worth (posted Jun. 27, 2013) (TSA-2013-0004-4565)	JA 000553
Comment of Anonymous (posted Jun. 27, 2013) (TSA-2013-0004-4576)	JA 000555
Comments of the Sikh Coalition (posted Jun. 27, 2013) (TSA-2013-0004-4619)	JA 000556
Comments of the Human Rights Campaign (posted Jun. 27, 2013) (TSA-2013-0004-4626)	JA 000589
Comments of Sommer Gentry (posted Jun. 27, 2013) (TSA-2013-0004-4662)	JA 000597
Comments of Kathy Huff (posted Jun. 28, 2013) (TSA-2013-0004-4761)	JA 000617

Comments of the Family Equality Council (posted Jun. 28, 2013) (TSA-2013-0004-4823)	JA 000618
Comments of Anonymous (posted Jun. 28, 2013) (TSA-2013-0004-4827)	JA 000625
Comment of Kurt (posted Jun. 28, 2013) (TSA-2013-0004-4903)	JA 000627
Comments of Jim Harper, Tom Mueller and Mark Stewart of the Cato Institute (posted Jul. 1, 2013) (TSA-2013-0004-4920)	JA 000630
Comments of Freedom to Travel USA (posted Jul. 1, 2013) (TSA-2013-0004-4958)	JA 000681
Comment of Anonymous (posted Jul. 1, 2013) (TSA-2013-0004-4962)	JA 000701
Comment of John Hand (posted Jul. 2, 2013) (TSA-2013-0004-5188)	JA 000702
Comment of Anonymous (posted Jul. 2, 2013) (TSA-2013-0004-5215)	JA 000704
Comment of Jason Sonenshein (posted Jul. 3, 2013) (TSA-2013-0004-5221)	JA 000706
Comment of Gillian Conway (posted Jul. 2, 2013) (TSA-2013-0004-5270)	JA 000707
Comments of the United States Justice Foundation (posted Jul. 2, 2013) (TSA-2013-0004-5292)	JA 000708
Comment of Gayle Martin (posted Jul. 2, 2013) (TSA-2013-0004-5327)	JA 000714
Comment of Thomas A. Burns (posted Jul. 9, 2013) (TSA-2013-0004-5424)	JA 000715
Comment of Sandra Mendyk (posted Jul. 9, 2013) (TSA-2013-0004-5457)	JA 000717

Comment of Mary (posted Jul. 10, 2013) (TSA-2013-0004-5467)	JA 000718
Comment of Darian Turner (posted Jul. 10, 2013) (TSA-2013-0004-5489)	JA 000719
Comment of Jennifer More (posted Jul. 15, 2013) (TSA-2013-0004-5529)	JA 000720
Comment of Donna Ellis (posted Dec. 16, 2015) (TSA-2013-0004-5580)	JA 000721
EPIC Comment Letter on NPRM: Passenger Screening Using Advanced Imaging Technology (Oct. 10, 2013)	JA 000722
<i>TSA: Security Gaps: Hearing Before the House Committee on Oversight and Government Reform, 114th Cong. (statement of John Roth, Inspector General for the Department of Homeland Security) (Nov. 3, 2015)</i>	JA 000740
Privacy Impact Assessment Update for TSA Advanced Imaging Technology (Dec. 18, 2015)	JA 000767

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

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.

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

- I. Executive Summary
 - A. Purpose of the Regulation
 - B. Summary of Major Provisions
 - C. Costs and Benefits
- II. Background
 - A. The Evolving Threat to Aviation Security
 - B. Layers of Security
 - C. Congressional Direction To Pursue AIT
 - D. U.S. Court of Appeals Decision in *EPIC v. DHS*
- III. AIT Screening Protocols
 - A. Types of AIT Equipment
 - B. Privacy Safeguards for AIT
 - C. Safety of AIT
 - 1. Millimeter Wave Units
 - 2. Backscatter Units
 - D. AIT Procedures at the Checkpoint
- IV. Deployment of AIT
- V. Rulemaking Analyses and Notices
 - A. Regulation Evaluation Summary and Economic Impact Analyses
 - B. Executive Orders 12866 and 13563 Assessment

- C. Regulatory Flexibility Act Assessment
- D. International Trade Impact Assessment
- E. Unfunded Mandates Reform Act Assessment
- F. Paperwork Reduction Act
- G. Executive Order 13132, Federalism
- H. Environmental Analysis
- I. Energy Impact Analysis

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 anomalies⁵ 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 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.

- 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 COST⁸ 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 COST⁸ 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

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.

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

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.

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.

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

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

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.

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 Measurements⁴⁷ 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

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.

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

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 required 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

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.

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

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.

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 site⁶³ 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

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 AIT⁷⁰ and a plastic dagger concealed inside a comb was detected in a passenger's pocket.⁷¹

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>.

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>.

“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 COST⁷³ 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 utilities	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.



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 Period Closed

ID: TSA-2013-0004-0114

Tracking Number: 1jx-84h4-5tzz

Comment

I refuse to be groped by strangers 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.

Document Information

Date Posted:

Apr 1, 2013

RIN:

1652-AA67

[Show More Details](#)

Submitter Information

City:

Pickerington

Country:

United States

State or Province:

OH



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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 whatsoever, period. TSA needs to be abolished and then start over, with intelligence, in more ways than one.

ID: TSA-2013-0004-0162
Tracking Number: 1jx-84h4-kr36

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



Mary Graham

This 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

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...

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. Though 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 to 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 body, 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



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 Period Closed
Jun 24 2013, at 11:59 PM ET

Comment

Stop the screening. It should be the first thing to go in the sequester. It is unconstitutional 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.

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-0279
Tracking Number: 1jx-84k0-7gnk

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-0327
Tracking Number: 1jx-84ki-hpel

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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#) 

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.

ID: TSA-2013-0004-0342
Tracking Number: 1jx-84kv-4gsw

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



Anonymous

This 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

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.

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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-0401
Tracking Number: 1jx-84lp-s4oc

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



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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

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



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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-0596

Tracking Number: 1jx-84t4-rpp5

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



T.A.

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-0597

Tracking Number: 1jx-84t4-wlwy

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 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

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.



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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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

This 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

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

ID: TSA-2013-0004-0686

Tracking Number: 1jx-84v4-8x3c

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 perpetrators 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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-0774

Tracking Number: 1jx-84wh-biip

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.

Document Information

Date Posted:

Apr 23, 2013

RIN:

1652-AA67

[Show More Details](#)



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

This 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

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.

ID: TSA-2013-0004-1039

Tracking Number: 1jx-84wd-lpgh

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



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

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."

ID: TSA-2013-0004-1439
Tracking Number: 1jx-84wo-j3bn

Document Information

Date Posted:
May 7, 2013

RIN:
1652-AA67

[Show More Details](#)

Submitter Information

Submitter Name:
Gayle M



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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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



Anonymous

This 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

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.

Document Information

Date Posted:

May 7, 2013

RIN:

1652-AA67

[Show More Details](#)



Anonymous

This 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

Comment

I do not fly any more since these scanners have gone into effect. I'd rather drive than lose my dignity.

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

DEPARTMENT OF
TRANSPORTATION
SECRET OPERATIONS

2016 APR 23 P 1:52

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.

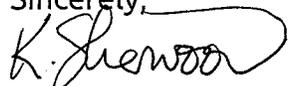
I have been boycotting the TSA for about three years now (and plan to continue) due to what I consider its government-sponsored sexual assault. I either drive, take the train, or choose airlines which make no stops in the US. Once, I took a private plane.

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 hijackers' 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,



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

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.

ID: TSA-2013-0004-1643

Tracking Number: 1jx-84x5-pwil

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



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

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."

ID: TSA-2013-0004-1737

Tracking Number: 1jx-84wm-sqi0

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



W. Hughes

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-1741
Tracking Number: 1jx-84wm-phyl

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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



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

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.

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



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

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.

ID: TSA-2013-0004-1976

Tracking Number: 1jx-84z9-gaq5

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-2074
Tracking Number: 1jx-84wq-k5hy

Document Information

Date Posted:
 May 22, 2013

RIN:
 1652-AA67

[Show More Details](#)

Submitter Information

Country:
 United States

State or Province:
 OR



Grejdi Gjura

This 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

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.

ID: TSA-2013-0004-2109

Tracking Number: 1jx-84x5-hd9a

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

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.

ID: TSA-2013-0004-2169

Tracking Number: 1jx-8551-ulf4

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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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



Vincent Wilkinson

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-2288
Tracking Number: 1jx-84wn-mcsr

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



Marianne Cherrier Burns

This 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

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.

ID: TSA-2013-0004-2397

Tracking Number: 1jx-84x4-cfb0

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



Bobbie Kent

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 dispirited 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."

ID: TSA-2013-0004-2442
Tracking Number: 1jx-85a4-rlmu

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 entire 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.

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



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

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.

ID: TSA-2013-0004-2702

Tracking Number: 1jx-84x0-bltn

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

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.

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



Kate

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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!

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



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

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 inconveniences 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 inconvenience 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.

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



E. Kelly

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-2798
Tracking Number: 1jx-85nw-r9bn

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

This 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

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.

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-3196

Tracking Number: 1jx-85kw-hr61

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



VSM

This 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

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.

ID: TSA-2013-0004-3218

Tracking Number: 1jx-84x2-3kp8

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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-3303

Tracking Number: 1jx-850g-1kwg

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.

Document Information

Date Posted:

Jun 10, 2013

RIN:

1652-AA67

[Show More Details](#)

Submitter Information

Submitter Name:

Anonymous



Joanne Frances Gladney-Naumer

This 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

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!!

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

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.

ID: TSA-2013-0004-3427

Tracking Number: 1jx-850g-z88v

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



Vicki Warthen

This 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

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.

ID: TSA-2013-0004-3465

Tracking Number: 1jx-84yd-ez21

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 Period Closed
Jun 24 2013, at 11:59 PM ET

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?

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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

ID: TSA-2013-0004-3585
Tracking Number: 1jx-8519-nfdm

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

This 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

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.

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



The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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

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.



Kelly McConnell

This 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

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.

ID: TSA-2013-0004-3699

Tracking Number: 1jx-85xx-0a31

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 no one. 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 non-ionizing) 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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#) 

ID: TSA-2013-0004-3769

Tracking Number: 1jx-85yo-rcit

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)

Document Information

Date Posted:

Jun 18, 2013

RIN:

1652-AA67

[Show More Details](#) 

Submitter Information

Submitter Name:

Anonymous

Attachments (5)



Exhibit 1

View Attachment:



Exhibit 2

View Attachment:



Exhibit 3

JA 000503



View Attachment:



Exhibit 4

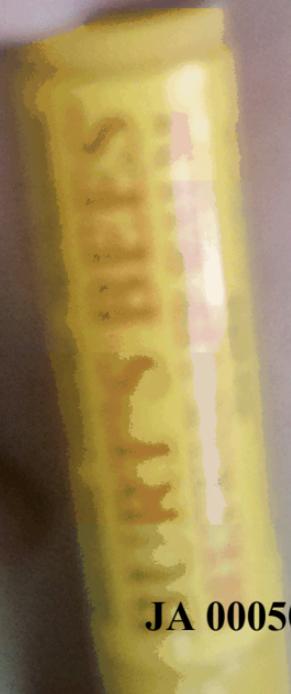
View Attachment:



Exhibit 5

View Attachment:





JA 000505

JA 000506

Page 1 of 3

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

Page 2 of 3

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.

Page 3 of 3

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.



JA 000510

JA 000511



Tom Ritter

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

Comment

I vehemently disagree 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 regularly 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 mastectomy and colonoscopy patients being embarrassed and forced to explain themselves in public, and domestic violence and harassment victims are forced to be seen naked or groped. It prompts an air of suspicion among 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.

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



Nick B.

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 profiting from their use - detailed here: <http://www.brasschecktv.com/videos/tsa-nonsense-and-abuse/investigate-michael-chertoff-for-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.

ID: TSA-2013-0004-3830
Tracking Number: 1jx-85z4-ekbd

Document Information

Date Posted:
Jun 19, 2013

RIN:
1652-AA67

[Show More Details](#)

Submitter Information

Submitter Name:
Nick B

Country:
United States



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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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.

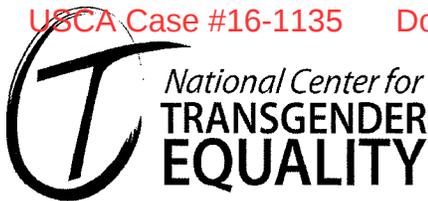
Sometimes, the TSA does not even have enough staff to operate the AIT units and reverts back to the using only the WTMDs. This results in AIT units that sit unused in checkpoints. Obviously, it is not cost effective for the AIT units to sit unused in checkpoints. In addition, if the purpose of the AIT's 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.



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 than 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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-4086

Tracking Number: 1jx-84xj-dlqh

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 arbitrary 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.

Document Information

Date Posted:

Jun 24, 2013

RIN:

1652-AA67

[Show More Details](#)



Robin Douglas Kunzler

This 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

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.

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



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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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

ID: TSA-2013-0004-4120

Tracking Number: 1jx-85z9-uj4y

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)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-4172

Tracking Number: 1jx-8637-xy4t

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.

Document Information

Date Posted:

Jun 25, 2013

RIN:

1652-AA67

[Show More Details](#)

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 areas 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 than 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 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. 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 in 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>.



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

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.

ID: TSA-2013-0004-4226

Tracking Number: 1jx-8638-4lmy

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%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](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 scanners²²—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

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



Why isn’t this “pat down” option mentioned in the Code of Federal Regulations?

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/optiming-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:

$$(1) \quad \frac{\textit{Cost}}{(\textit{Damage})(\textit{Risk Reduction})}$$

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:

$$(2) \quad \frac{1.2}{(26)(0.086)}$$

$$(3) \quad \frac{1.2}{2.236} = 0.537 = 53.7\%^{38}$$

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



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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 Napalitano) 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

ID: TSA-2013-0004-4265
Tracking Number: 1jx-860e-u7in

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

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.

ID: TSA-2013-0004-4414
Tracking Number: 1jx-8613-h7ay

Document Information

Date Posted:
Jun 26, 2013

RIN:
1652-AA67

[Show More Details](#)

Submitter Information

Submitter Name:
Anonymous



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

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.

ID: TSA-2013-0004-4447
Tracking Number: 1jx-862g-kmc2

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 through 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 confidentiality 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 than 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 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. 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 in 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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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

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.

ID: TSA-2013-0004-4562

Tracking Number: 1jx-863e-3wru

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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 than 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.

JA 000553

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

Sincerely,
Amber Worth

USCA Case #16-1135

Document #1651335

Filed: 12/15/2016

Page 151 of 370

JA 000554



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](#)



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>.

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.

Exemption (b)(3)

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

From:



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)



TSA Passenger Screening Program
Strategic Options to Consider
Racial Profiling Concerns

Submitted By:

(b) (6)

Senior Leadership Development Program – 3

June 16, 2009

Table of Contents

IntroductionPage 1

Strategic Option 1Pages 2-4

Strategic Option 2Pages 4-5

Strategic Option 3Pages 5-6

Strategic Option 4Pages 6-7

Strategic Option 5Pages 7-8

Strategic Option 6Page 8

Strategic Option 7Page 9

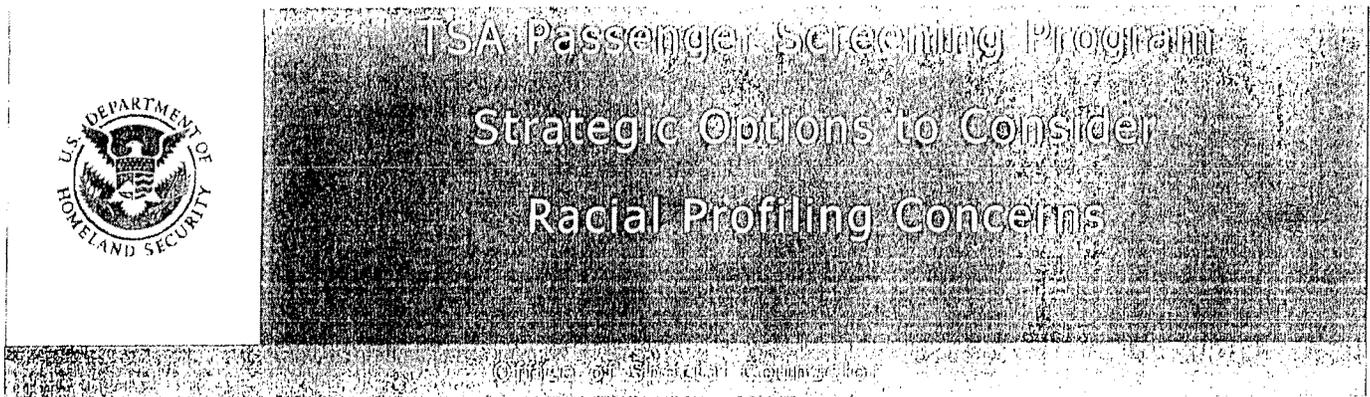
Strategic Option 8Pages 9-10

Conclusion Page 10

Attachment 1

Attachments 2, 2A & 2B

Attachment 3

**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 one of three screening options that includes passing through either a Trace Portal (Puffer) or Whole Body Imaging (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 Programs
Strategic Options to Consider
Racial Profiling Concerns

Office of Special Inspection

(b) (5)

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)

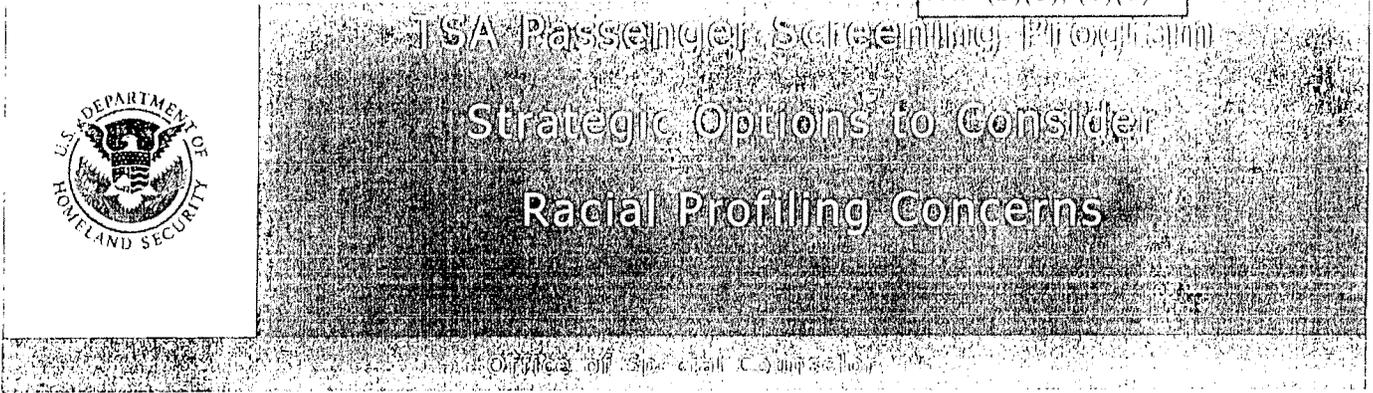
(b) (4)

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)

WIF (b)(3), (b)(5)



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.

Strategic Option Recommendation #2 to SLT:

Perform a CLIA on the Passenger Screening Checkpoint SOP then publically announce the effort and results.

(b)(3) 49 USC 114(r)

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 (b)(3) 49 USC 114(r)

(b)(3) 49 USC 114(r)

(b)(3) 49 USC 114(r) Such data could be delivered to Congress during

WIF (b)(3), (b)(5)



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:

(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.

WIF (b)(3), (b)(5)



U.S.A. Passenger Screening Program
 Strategic Options to Consider
 Racial Profiling Concerns

Office of Special Counsel

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) reveals that CCTV technology is lacking. Conversely, airports such as (b)(3) 49 USC 114(r) 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 injuries 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).

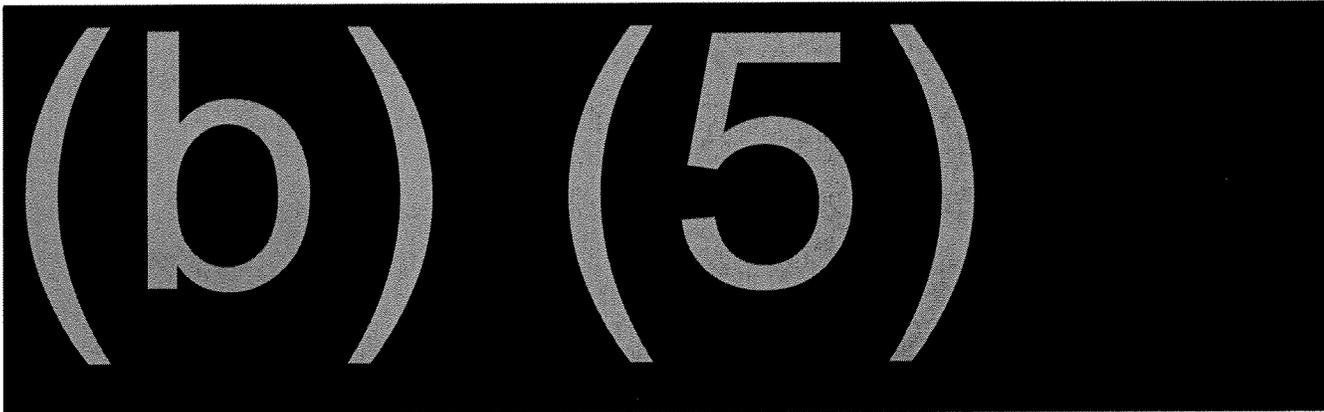
Strategic Option Recommendation #6 to SLT:

Accelerate and improve CCTV systems at airports that lack such technology today.



TSA Passenger Screening Program
 Strategic Options to Consider
 Racial Profiling Concerns

Office of the Chief Counsel



Conclusion:

The 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



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%	23%
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

**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 Turbanned 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.

Ethnic Profiling in Airport Security Screening

Page 2 of 3

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).

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

² 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.

Ethnic Profiling in Airport Security Screening
Page 3 of 3

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

11

Washington DC Office
1330 Connecticut Ave NW, Suite B
Washington, DC 20036

Tel: (202) 347-6776
Fax: (202) 347-6047
www.vera.org



To: (b) (6) Transportation Security Administration
From: (b) (6) 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.

**VERA INSTITUTE OF JUSTICE
TSA preliminary proposal**

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 INSTITUTE OF JUSTICE
TSA preliminary proposal**

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.

**VERA INSTITUTE OF JUSTICE
TSA preliminary proposal***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

VERA INSTITUTE OF JUSTICE
TSA preliminary proposal

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

**VERA INSTITUTE OF JUSTICE
TSA preliminary proposal**

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

26

Attachment 3



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)

SENSITIVE SECURITY INFORMATION - WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in C.F.R. parts 15 and 1520, except with the written permission of the administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 & 1520.

WARNING: These documents contain information subject to the Privacy Act of 1974, as amended. Please ensure appropriate measures are taken to safeguard these records.

36



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

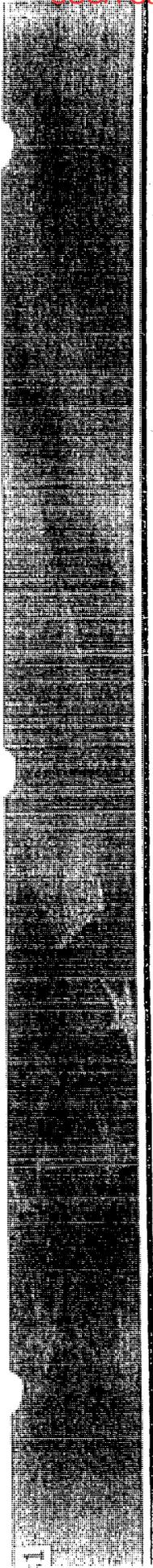
Comments:

Large empty rectangular box for handwritten comments.

SENSITIVE SECURITY INFORMATION - WARNING: This record contains Sensitive Security Information that is controlled under 49 C.F.R. parts 15 and 1520. No part of this record may be disclosed to persons without a "need to know," as defined in C.F.R. parts 15 and 1520, except with the written permission of the administrator of the Transportation Security Administration or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For U.S. government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 C.F.R. parts 15 & 1520.

WARNING: These documents contain information subject to the Privacy Act of 1974, as amended. Please ensure appropriate measures are taken to safeguard these records.

31



**TSA Strategic Options to Consider
Secondary Screening – Bulky Clothing & Headwear
Community Perceptions of Racial or Religious Profiling**

June 11, 2009

(b) (6)

Senior Leadership Development Program - 3
Office of the Special Counselor (OSC)
Transportation Security Administration (TSA)



Transportation
Security
Administration

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 or 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*

WIF (b)(3), (b)(5)

Proposed Strategic Options for TSA

- Data collection efforts on secondary screening
- Civil Liberties Impact Assessment
- (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



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 than 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 in 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 on a 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 vaginal 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 of Kafka-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 completely assured that no TSA person will put their hands on my body? I can not stress enough to you how outraged and upset 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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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

ID: TSA-2013-0004-4761
Tracking Number: 1jx-8618-ckn4

Document Information

Date Posted:
 Jun 28, 2013

RIN:
 1652-AA67

[Show More Details](#)

Submitter Information

Submitter Name:
 Kathy Huff

ZIP/Postal Code:
 78412



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 than 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 than 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
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 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 Niassé, a Muslim.

Let’s all just be glad that Niassé 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:)	TSA-2013-0004
Passenger Screening Using)	(RIN 1652-AA67)
Advanced Imaging Technology)	
)	Comments of Jim Harper, John Mueller,
)	and Mark Stewart of the Cato Institute
)	

Table of Contents

- I. Introduction and summary
- II. The NPRM and proposed rule fail to account for privacy
 - a. The NPRM does not exhibit an understanding of privacy
 - b. Body scans undercut privacy
 - c. The NPRM takes body scanners as a given to deny their privacy effects
- III. The proposed rule fails to articulate sufficiently clear standards
- IV. Unjustified secret classification of the “risk-reduction analysis” undercuts the rulemaking
 - a. An understanding of risk management is essential
 - b. Classification of the risk management document is unwarranted
- V. Risk management and cost-benefit analysis show that the policy supported by the proposed rule is not cost-effective
 - a. Nothing excuses TSA from using risk management and cost-benefit analysis
 - b. Amidst talk of risk management, DHA and TSA have long failed to implement risk-based decision-making, and they fail to do so here
 - c. TSA’s body scanners fail to be cost-effective
 - d. Non-monetary costs, the mortal danger produced by increased automobile travel, and opportunity costs further undercut the policy
 - e. The risk of being killed by terrorists during an airline flight is already acceptably low by standards TSA uses for other dangers
 - f. It is not clear that the machines actually secure against attacks
- VI. The body scanning policy should be reversed pending a new, sufficient rulemaking

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 risks²⁴ 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:

$$\text{Likelihood} \times \text{Consequence} = \text{Risk}$$

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 tradeoffs 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:

$$\text{Risk} = (\text{Probability of a Successful Attack}) \times (\text{Losses Sustained in an Attack})$$

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:

$$\text{Benefit} = (\text{Probability of a Successful Attack}) \times (\text{Losses Sustained in an Attack}) \times (\text{Reduction in Risk Generated by the Security Measure})$$

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 resistance, 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 Conflict & 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>

©2011 Berkeley Electronic Press. All rights reserved.

JA 000661

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:

$$\text{Net Benefit} = \underbrace{p_{\text{attack}} \times C_{\text{loss}} \times \Delta R}_{\text{benefit}} - \underbrace{C_{\text{security}}}_{\text{cost}} \quad (1)$$

- 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 $C_{\text{security}} = \$1.2$ 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 $C_{\text{loss}} = \$2$ 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 $C_{\text{loss}} = \$50$ 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.

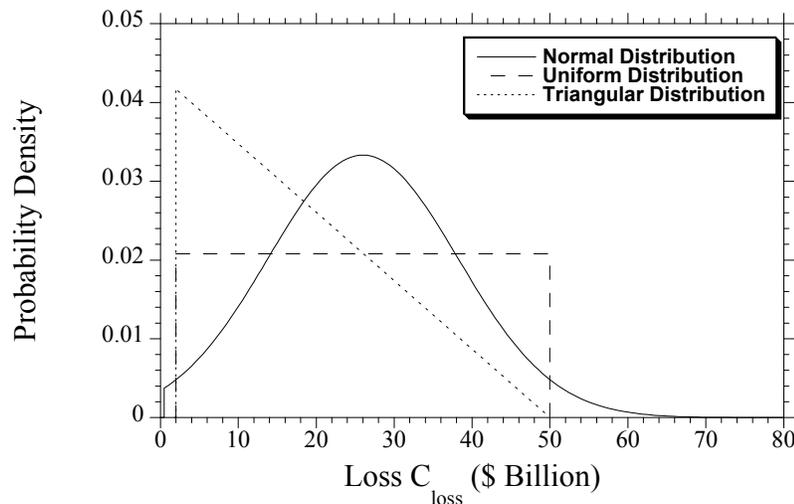


Figure 1. Alternative Loss Uncertainty Models.

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

$$\begin{aligned} \Pr(\text{airliner loss}) &= \prod_{i=1}^{10} \Pr(\text{non-detection for preboarding security measure } i) \\ &\times \Pr(\text{Passengers/Crew non-detection}) \times \Pr(\text{IED detonates successfully}) \quad (2) \\ &\times \Pr(\text{aircraft downed by IED detonation}) = (0.9)^{10} \times 0.5 \times 0.75 \times 0.75 = 9.8\% \end{aligned}$$

The probability then that the plot is foiled, deterred or disrupted is $1 - \Pr(\text{airline loss}) = 90.2\%$ 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%.

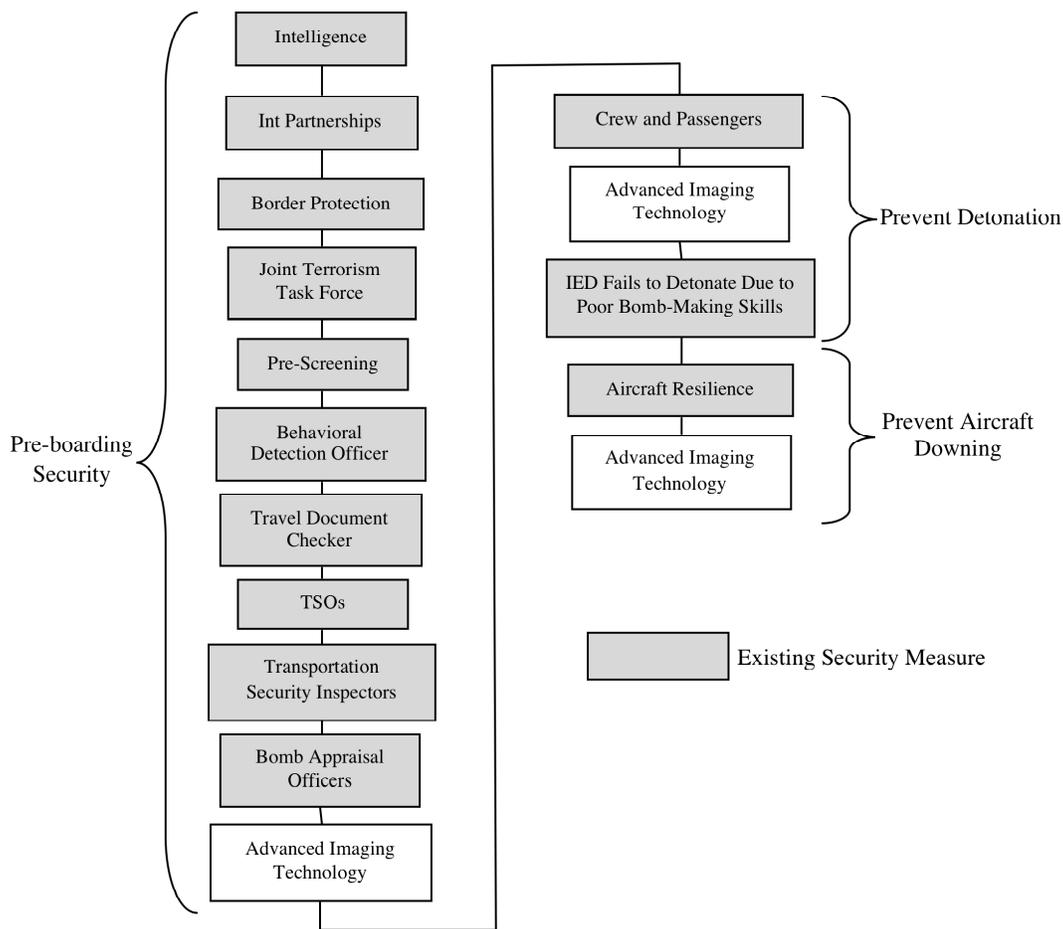


Figure 2. Reliability Block Diagram of Existing (shaded) and Enhanced Aviation Security Measures With Advanced Imaging Technology (AIT).

Again assuming a series system, and since $\text{Pr}(\text{AIT effectiveness})$ is 50%, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is $[1-\text{Pr}(\text{AIT effectiveness})]^3=(1-0.5)^3=12.5\%$ and so probability of airliner loss is now calculated as $9.8\% \times 12.5\% = 1.2\%$. 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 $\Delta R = 98.8 - 90.2 = 8.6\%$. 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 $\Delta R = 9.8\%$. If AITs are less effective than assumed above, but still twice as effective than any existing layer of TSA pre-boarding security [$\text{Pr}(\text{AIT effectiveness}) = 20\%$], 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%.

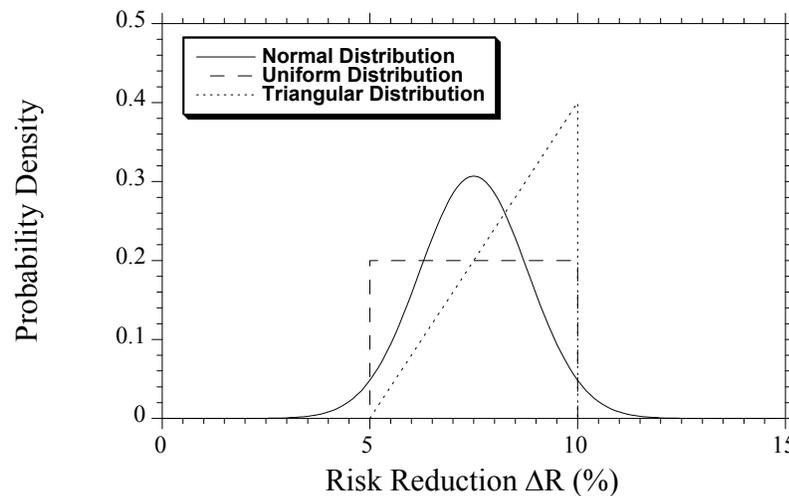


Figure 3. Alternative Risk Reduction Uncertainty Models.

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, $\Pr(\text{cost-effectiveness})$, 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. $\Pr(\text{cost-effective})=100\%$). 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.

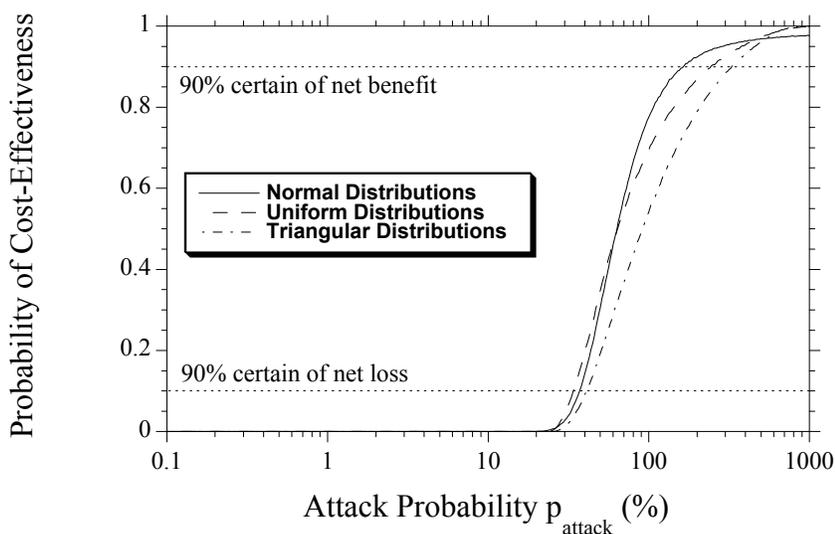


Figure 4. Probability of Cost-Effectiveness (Net Benefit Exceeds Zero).

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 $\Delta R=16.5\%$. If AITs are 100% effective then they reduce existing risk to zero and so $\Delta R=16.8\%$. 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 $\Delta R=11.5\%$. 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 $C_{\text{loss}}=\$100$ 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 Cavities*, 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.

Stewart and Mueller: Cost-Benefit Analysis of Full Body Scanners

17

- 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 to 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 Imaging 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	4
<i>Conclusions</i>	4
<i>Freedom To Travel USA –Reasons For Changes To The Proposed Rule</i>	7
<i>POST-NPRM Request for Legal Action To Restore America’s Freedoms</i>	11
ADDENDUM: Comments From FTTUSA Media Kit	13
<i>4th Amendment</i>	13
<i>History of Administrative Searches</i>	14
<i>History of Airport Screenings</i>	14
<i>United States vs Davis</i>	14
<i>Discussion of United States vs Davis</i>	16
<i>NPRM Ignores Body Images, Yet TSA Scanners Are “Strip Searches”</i>	18
<i>Sexual Assault Pat Downs</i>	20

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](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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-4962

Tracking Number: 1jx-862q-cb44

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.

Document Information

Date Posted:

Jul 1, 2013

RIN:

1652-AA67

[Show More Details](#)



John Hand

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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!!!
JA 000702

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



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 weaponds, especially when compared to alternative technology



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 weaponds, 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

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.

ID: TSA-2013-0004-5221
Tracking Number: 1jx-8632-v2p1

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



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

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.

ID: TSA-2013-0004-5270
Tracking Number: 1jx-8632-qvpm

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

Board of Directors
Norman Olney
San Diego, California
Floyd Brown
Phoenix, Arizona
Randy Goodwin
Santa Ana, California



Executive Director
Michael Connelly

Of Counsel
James F. Altham, Jr.
New Haven, Connecticut
G. Darlene Anderson
San Diego, California
Russell A. Austin, Jr.
Seattle, Washington

Roy L. Brun
Shreveport, Louisiana
Kenneth G. Burke
Memphis, Tennessee
James L. Byrnes
Pittsburgh, Pennsylvania
William M. Crosby
Orange, California
Scott E. Darling
Riverside, California

Richmond T.P. Davis
Silver Spring, Maryland
William G. Davis
Baton Rouge, Louisiana
Frank Donatelli
Alexandria, Virginia
James E. Edwards
Coral Springs, Florida
William E. Evans
Annandale, Virginia

Fred Friedman, P.C.
Akron, New York
Malcolm N. Fleming
Manlius, New York
Richard G. Handler
Bellerose, New York
John J. Jawor
Chicago, Illinois

J. Kent Jarrell
Washington, D.C.
Karl Keating
San Diego, California
James V. Lacy
Laguna Niguel, California
Robert M. Levy
Woodland Hills, California
W. Andrew McCullough
Orem, Utah

John C. Meyer
Washington, D.C.
David B. Nolan
Alexandria, Virginia
Taylor O'Hearn
Shreveport, Louisiana
Alfred S. Regnery
Washington, D.C.

John L. Roche
San Diego, California
Duane Root, P.C.
Akron, New York
Richard B. Sanders
Seattle, Washington
Leonard J. Snow
Ithaca, New York

David J. Strachman
Providence, Rhode Island
Elroy Strickland
Murrysville, Pennsylvania
Roscoe Stovall, Jr.
Indianapolis, Indiana
John P. Taylor
Cupertino, California

John H. Tovey
Allendale, New Jersey
Neil T. Wallace
Ithaca, New York
(Partial Listing)

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>

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=main-grid7|main5|dl12|sec1_inlk3%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#.UcjbsZzNIPc>

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
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.



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 Period Closed
Jun 24 2013, at 11:59 PM ET

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.

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-scanners-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)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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

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



Mary

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

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.

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

This 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



Jennifer Moore

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

ID: TSA-2013-0004-5529

Tracking Number: 1jx-85cg-j2mn

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.

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



Donna Ellis

The is a Comment on the **Transportation Security Administration (TSA) Proposed Rule: NPRM: Passenger Screening Using Advanced Imaging Technology (Federal Register Publication)**

Comment Period Closed
 Jun 24 2013, at 11:59 PM ET

For related information, [Open Docket Folder](#)

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 than 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

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



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 55,275.

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 Alarming, 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*, TECHNEWSAILY (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 identity 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.



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.

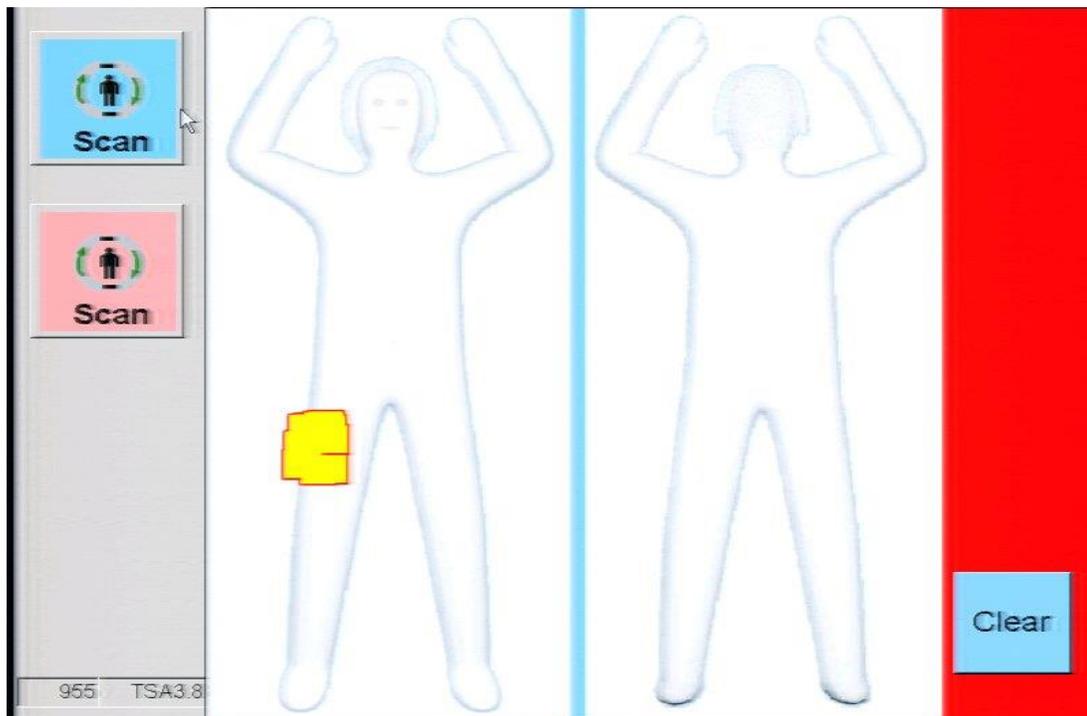
¹ Pub. L. 107-71

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 underlying 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