Before the
TRANSPORTATION SECURITY ADMINISTRATION
DEPARTMENT OF HOMELAND SECURITY
Washington, DC 20590

Notice of Proposed Rulemaking: Passenger Screening Using Advanced Imaging Technology	)	TSA-2013-0004 (RIN 1652-AA67)
	)	Comments of Jim Harper, John Mueller, and Mark Stewart of the Cato Institute

Table of Contents

I. Introduction and summary

Submitting these comments in response to the Notice of Proposed (NPRM), "Passenger Screening Using Advanced Imaging Technology,"[1] are Jim Harper, John Mueller, and Mark Stewart of the Cato Institute.

The Cato Institute is a public policy research organization dedicated to the principles of individual liberty, limited government, free markets and peace. Its scholars and analysts conduct independent, nonpartisan research on a wide range of policy issues. Founded in 1977, Cato owes its name to Cato's Letters, a series of essays published in 18th-century England that presented a vision of society free from excessive government power.

[1] 78 Fed. Reg. 18287-18302 (Mar. 26, 2013), docket number TSA-2013-0004, RIN 1652-AA67.

Jim Harper is director of information policy studies at the Cato Institute, in which role he works to adapt law and policy to the unique problems of the information age. He deals with areas such as privacy, telecommunications, intellectual property, and security. Harper was a founding member of the Department of Homeland Security's Data Privacy and Integrity Advisory Committee and he recently co-edited the book *Terrorizing Ourselves: How U.S. Counterterrorism Policy Is Failing and How to Fix It*.

John Mueller is a senior fellow at the Cato Institute. He is also a member of the political science department and Senior Research Scientist with the Mershon Center for International Security Studies at Ohio State University. He is a leading expert on terrorism and particularly on the reactions (or over-reactions) it often inspires. His most recent book on the subject, *Terror, Security and Money: Balancing the Risks, Benefits and Costs of Homeland Security* (co-authored with Mark Stewart) was published in September 2011 by Oxford University Press. Other books on the subject include *Overblown: How Politicians and the Terrorism Industry Inflate National Security Threats, and Why We Believe Them* (Free Press, 2006) and *Atomic Obsession: Nuclear Alarmism from Hiroshima to Al-Qaeda* (Oxford, 2010).

Mark G. Stewart, recently a visiting fellow at the Cato Institute, is Professor of Civil Engineering and Director of the Centre for Infrastructure Performance and Reliability at The University of Newcastle in Australia. He is also currently an Australian Research Council Professorial Fellow. He is the author, with R.E. Melchers, of Probabilistic Risk Assessment of Engineering Systems (Chapman & Hall, 1997), as well as more than 300 technical papers and reports. He has more than 25 years of experience in probabilistic risk and vulnerability assessment of infrastructure and security systems that are subject to man-made and natural hazards.

The euphemism "Advanced Imaging Technology" fails to describe the technology at issue in the instant rulemaking. It would be more accurate to call them "nude body scanners." The machines look under the clothes of travelers, as a traditional strip-search does, without actually stripping the person. Obscuring language like "AIT" is just one dimension of the indifference to privacy shown in the preamble and the proposed rule, which does not account for the privacy concerns that prompted the court to order this rulemaking.

As to the substance of the rulemaking, the proposed rule fails fully to articulate the TSA's policies, existing or proposed, with respect to the use of body scanners at the nation's airports. It thus fails to fulfill the order of the D.C. Circuit Court of Appeals in *EPIC v. TSA.*

Secret classification of the agency's "risk-reduction analysis" is not warranted by law or policy, and it fatally undercuts the requirements in administrative law and related executive orders that require the agency to perform and publish various analyses. Risk management and cost-benefit analysis can easily be conducted without revealing

technical details or threat information that may legitimately be kept confidential. The agency must conduct risk management and cost-benefit analyses of its policies so that its policies can be examined for rationality and sufficiency under the law.

Independent, scholarly, and unchallenged risk management and cost-benefit analyses of the use of body scanners in U.S. airports have been made. They find that the machines fail overwhelmingly to reduce risk enough to justify their costs—even assuming they work effectively. Among the costs produced by TSA policies is this area is disinclination to travel by air, which is quite safe relative to automobile travel. Thus, TSA policies may result in increased mortality among travelers.

Having taken twenty months to issue a deficient proposed rule and utterly lacking analysis, the TSA has abused the rulemaking process to the detriment of the public, some of whom may needlessly be killed due to current TSA policy. The only appropriate remedy is for TSA to suspend its body scanning policy and commence a new rulemaking, adopting whatever policy emerges from that rulemaking. Otherwise, some Americans may die awaiting the resolution of this rulemaking, the appeals that follow it, and the new rulemaking that those appeals will inevitably produce.

II. The NPRM and proposed rule fail to account for privacy

Though the TSA is obliged to produce privacy impact assessments under the E-Government Act of 2002, and though the Department of Homeland Security has had a privacy advisory committee since 2005, the NPRM does not exhibit an understanding of privacy. It uses language that obscures the privacy interests of travelers, and betrays no recognition that privacy is lost to the TSA's policies.

In this comment, we decline, as noted earlier, to adopt the obscuring euphemism "advanced imaging technology" or "AIT" because it inappropriately draws attention away from the interest that sparked the *EPIC v. TSA* lawsuit and this court-ordered rulemaking. Instead, we will use a term we believe to be accurately descriptive: nude body scanner. This terminology acknowledges the privacy interests of travelers, to which we now turn.

a. The NPRM does not exhibit an understanding of privacy

Privacy's legal roots go back as far as 1890 and the publication by Samuel D. Warren and Louis D. Brandeis of "The Right to Privacy" in the Harvard Law Review.[2] Since the late 1960s, scholars, advocates, and government agencies have been grappling articulately with privacy and its protection. The late 1960s and early 1970s were an era of privacy foment not unlike today, with books written on the subject and state constitutions amended to protect privacy explicitly. In 1967, the year that the Supreme Court decided

[2] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193 (1890).

Katz v. United States,[3] scholar Alan Westin characterized privacy in his seminal book as "the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[4]

This is the strongest sense of the word "privacy": the enjoyment of control over personal information. A tighter, more legalistic definition of privacy is: "the subjective condition that people experience when they have power to control information about themselves and when they exercise that power consistent with their interests and values."[5] Given control over information about themselves, people will define and protect their privacy as they see fit.

Among other techniques, such as contractual agreements, people control information about themselves by arranging physical things with reference to themselves and by changing their behavior. Retreating into one's home and drawing the blinds, for example, causes what happens inside to be "private." Lowering one's voice to a level others cannot hear make a conversation "private." Draping the body with clothing makes the details of its shapes, textures, and colors "private." These arrangements and behaviors literally prevent others from perceiving things, maintaining the privacy of those things. Body scanners defeat this privacy protection for everyone passing through them.

b. Body scans undercut privacy

So-called "Advanced Imaging Technology" examines what is underneath the clothes of travelers. It does this using machines rather than human vision, but it is no less a scan of the body. The scanners evade rather than remove the coverings of the body.

Millimeter wave technology directs radio waves through the clothes and captures their reflection. Recording the reflected radio waves that have passed through clothing allows software to produce a visual image of the naked body similar to what reflected photons would produce. The court in *EPIC v. TSA* characterized the situation this way: "Despite the precautions taken by the TSA, it is clear that by producing an image of the unclothed passenger, an AIT scanner intrudes upon his or her personal privacy in a way a magnetometer does not."[6] It is the functional equivalent of recording photon patterns that have reflected off a nude body. This defeats the privacy-protecting function of clothing and allows an image of the unclothed person to be created.

It is true that, along some dimensions, the use of millimeter wave scanning to produce an image of the nude body offers greater privacy protection than an actual, physical strip-search. For example, in millimeter wave, the object of the search does not

[3] 389 U.S. 347 (1967).
[4] Alan Westin, Privacy and Freedom 7 (1967).
[5] See Jim Harper, Understanding Privacy—and the Real Threats to It, Cato Institute, Policy Analysis No. 520 (2004).
[6] U.S. Ct. App. D.C. Cir. No. 10-1157, slip op. at 8 [hereinafter "EPIC v. TSA"].

experience the physical sensation of having her clothes removed and her body exposed to the cool surrounding air. This reduces the sense of mortification most travelers would experience if undergoing a physical strip-search. If recent modifications to body scanning software are reliable, no human sees an image of the nude body. The knowledge that a human has seen one's body contrary to one's wishes is a common, strongly held privacy concern.

Along other dimensions, though, nude body scans are worse for privacy than a physical strip-search because they produce a *digital* image of the unclothed body. This is an image that computers can store indefinitely, transfer around the globe in seconds, and copy an infinite number of times without the copies degrading. The scanners take the control travelers have exercised over the appearance of their bodies by putting on clothes—their privacy—and makes it contingent on the TSA maintaining body scanners and their software as advertised. If the TSA does not enforce its policies—a prospect that is within the realm of possibility given hundreds of machines around the country and the possibility of official dereliction—travelers may learn that nude digital images of themselves flow across the Internet.

So, where a physical strip-search produces the sensation of bodily exposure and the embarrassment of having one or two other people (typically) view areas of the body that one intended to keep private, body scanners reduce the perception of bodily exposure, but replace it with the risk of massive online exposure of one's nude image worldwide. The trade-off is not subject to cold calculation, but it is roughly a wash. Either treatment is a loss for privacy.

Millimeter wave machines are certainly imaging technology, but the anodyne term "advanced" is not justified. It provides no relevant meaning, obscures what the machines do, and leaves their functionality inappropriately nondescript.

People put on clothes in the morning in order to conceal the appearance of their bodies. This is not only for practical purposes—because revealing their bodies can cause embarrassment, for example—but because one has a right over one's body, including a right to control what parts of it one reveals. Indeed, it is a specifically itemized constitutional right, the right to be secure in one's person against unreasonable searches.

c. The NPRM takes body scanners as a given to deny their privacy effects

To read the NPRM, one might think that the proposed rule improves privacy over the status quo ante. It says, "The use of ATR software enhances passenger privacy by eliminating images of individual passengers…" But the policy of subjecting American travelers to either a nude body scan or an intimate pat-down incontrovertibly reduces the privacy of travelers. The proposed rule, such as it is, codifies TSA's discretion to maintain this policy.

The use of "Automated Targeting Recognition" software, which shows on an outline where suspect articles may be found, undoubtedly mitigates the privacy lost to the use of body scanners in the first place. But the NPRM fails to acknowledge or address that original, significant loss to travelers' bodily privacy in the use of nude body scanners at all. This is a basic insufficiency of the NPRM caused in part by failing to apprehend what privacy is.

III. The proposed rule fails to articulate sufficiently clear standards

The proposed rule is insufficient to apprise members of the public of their rights and responsibilities at the airport. It does not articulate, even in a general way, what people can expect at the airport, what they must do at the airport, what they may not do at the airport, or what they can do to appeal any adverse action. Neither does the proposed rule articulate what TSA agents must do, what they may do, what they may not do, or any other dimension of their rights and responsibilities. The vague policy statement, proposed as if it were a rule, flies in the face of the D.C. Circuit Court of Appeals ruling requiring the instant rulemaking. It should be revised to clearly articulate the rights and responsibilities of both travelers and TSA agents with respect to body scanning.

The Administrative Procedure Act (APA) generally requires that a notice of proposed rulemaking be published in the Federal Register, unless the rule fits into one of a few exceptions.[7] In *EPIC v. TSA*, the court rejected arguments that the TSA's policy on the use of strip-search machines fit into one of these exceptions: It was not a "procedural rule," an "interpretive rule," or a "general statement of policy."[8] In order to resolve the deficiencies in its procedure, the court remanded to the TSA "to conduct a notice-and-comment rulemaking."[9] Throughout its opinion, the court relied on the premise that this rulemaking would pertain to a legislative rule: a rule adding to or amending the body of rules that dictate action or conduct.

The APA requires that such a rulemaking show the terms or substance of the proposed rule, or at least a description of the subjects and issues involved.[10] In its opinion requiring notice and comment proceedings, the court repeatedly emphasized the importance of issues surrounding body scanners. The court ordered a rulemaking that reflects the TSA's policies' "'substantial impact' upon the persons subject to it."[11] The court thought few rules "impose [as] directly and significantly upon so many members of the public" as the use of body scanning machines.[12] The court said that "the TSA's use of

[7] 5 USCS § 553(b)(3)(A).
[8] EPIC v. TSA at 7-11.
[9] EPIC v. TSA at 12.
[10] 5 USCS § 553(b)(3).
[11] EPIC v. TSA at 7.
[12] EPIC v. TSA at 9.

AIT for primary screening has the hallmark of a substantive rule…."[13] Finally, the court held that the TSA's policy "substantially changes the experience of airline passengers."[14]

Despite the repeated emphasis the D.C. Circuit Court's opinion puts on the significance of this rulemaking for exploring the TSA's policies and rationale, the court's opinion is more informative about TSA policies than the proposed rule laid out in the NPRM. The decision in *EPIC v. TSA* says, for example:

> No passenger is ever required to submit to an AIT scan. Signs at the security checkpoint notify passengers they may opt instead for a pat down, which the TSA claims is the only effective alternative method of screening passengers. A passenger who does not want to pass through an AIT scanner may ask that the pat down be performed by an officer of the same sex and in private.[15]

This is more informative than the NPRM or proposed rule.

Describing the regulations in place at the time of the decision, now changed in fact if not by the proposed rule, the court wrote:

> Each image produced by a scanner passes through a filter to obscure facial features and is viewable on a computer screen only by an officer sitting in a remote and secure room. As soon as the passenger has been cleared, moreover, the image is deleted; the officer cannot retain the image on his computer, nor is he permitted to bring a cell phone or camera into the secure room.[16]

This is more informative than the NPRM or proposed rule.

The court was able to describe the rules as they affected both travelers and the TSA at the time of its decision. These were the rules it expected the TSA to articulate in the rulemaking it ordered. When an agency statement is of "'present binding effect,'" the court wrote, "then the APA calls for notice and comment."[17] The court called for notice and comment because the TSA was to produce a legislative rule.

The government, too, took as a premise that it would produce a legislative rule. When EPIC filed a motion seeking enforcement of the court's mandate, the government filed a declaration averring the difficulty of producing a regulation in the challenging area of airline security.

[13] EPIC v. TSA at 9.
[14] EPIC v. TSA at 10.
[15] EPIC v. TSA at 3-4.
[16] EPIC v. TSA at 4.
[17] EPIC v. TSA at 10-11.

"The rulemaking of the type contemplated by the Opinion requires extensive preparation" declared James Clarkson, Acting General Manager of the Intermodal Security Support Division at TSA, "including in-depth economic analysis, that is generally measured in months."[18] The court of appeals, expecting a legislative rule, evidently accepted the gist of the declaration, as it declined the motion.

This "extensive preparation" did not amount to much. The proposed rule is a thin scrap of language, especially given the twenty months it took to produce. A regulatory agency like the TSA "has an obligation to make its views known to the public in a concrete and focused form so as to make criticism or formulation of alternatives possible."[19] Instead, it provided the public with two vague sentences containing fewer than fifty words:

> (d) The screening and inspection described in (a) may include the use of advanced imaging technology. For purposes of this section, advanced imaging technology is defined as screening technology used to detect concealed anomalies without requiring physical contact with the individual being screened.

This language delineates no obligations, either on the part of travelers or the TSA. It provides no notice to the public of what they can expect at the airport. It fails to signal in any way the rules that might pertain to the machines and their use. The language does nothing to bind the agency to a course of conduct or to cabin its exercise of discretion in any way.

Issuing such a general statement of policy a full twenty months after a court order requiring a legislative rule is totally insufficient. The statement hardly provides the "sufficient factual detail and rationale for the rule to permit interested parties to comment meaningfully" that the D.C. Court of Appeals requires.[20] The TSA's proposed rule does not even address most of the issues that the *EPIC* court found substantive enough to require notice and comment rulemaking in the first place. The NPRM is therefore non-responsive to the order of the court, as it fails to meet the basic notice requirements of administrative law and regulatory policy.

As the *EPIC v. TSA* court said, "the purpose of the APA would be disserved if an agency with a broad statutory command (here, to detect weapons) could avoid notice-and-comment rulemaking simply by promulgating a comparably broad regulation (here, requiring passengers to clear a checkpoint) and then invoking its power to interpret that statute and regulation in binding the public to a strict and specific set of obligations."[21] Yet that is what the TSA has done here. The NPRM has the form of notice-and-comment

[18] Declaration of James S. Clarkson in Support of Respondents' Opposition to Petitioners' Motion to Enforce the Court's Mandate, ¶ 4 (filed Nov. 10, 2011).
[19] Home Box Office, Inc. v. FCC, 567 F.2d 9, 36 (D.C. Cir. 1977).
[20] Florida Power & Light Co. v. United States, 846 F.2d 765, 771 (D.C. Cir. 1988).
[21] EPIC v. TSA at 10.

rulemaking, but it is just as broad as the agency's statutory command, preserving for later the specific set of obligations to which the public will be subjected. The APA does not require the TSA to provide precise notice of every aspect of the regulation, but in order for notice to be sufficient it must at the very least offer a rule that is "sufficiently descriptive of the subjects and issues involved so that interested parties may offer informed criticism and comments."[22] The NPRM flies in the face of the court's ruling and the direct language of the court rejecting overly broad regulatory language.

Given the purposes of APA rulemaking, adding requisite detail to the final rule would be insufficient. "[N]otice is inadequate if the interested parties could not reasonably have anticipated the final rulemaking from the draft rule."[23] The NPRM as it exists now gives no means of anticipating any aspect of the body scanning policy, other than an ambivalent statement that body scans might be used. Without a more descriptive rule, criticism of, and comment on, the TSA's body scanning machine is impossible, making the notice-and-comment process purposeless and defeating the court's order.

As we discuss at the end of this comment, the appropriate remedy, given the threat to human life produced by current policy, is to suspend the use of the body scanning machines for primary screening and commence a new rulemaking aimed at discovering the policy that most effectively secures the nation's travelers. The new rulemaking should be on the record and it should not use vagueness to insulate TSA policy from public review.

IV. Unjustified secret classification of the "risk-reduction analysis" undercuts the rulemaking

Classification of the "risk-reduction analysis" noted in the NPRM deprives the public of the benefits that notice-and-comment rulemaking is intended to provide, it deprives the agency of information and data that could improve the rule, and its likely result is more American highway deaths because of a poorly tuned rule. If the TSA cannot declassify the results of the risk-reduction analysis entirely, it should declassify the bulk of the analysis itself, redacting only specific threat and vulnerability information, and, if it issues a new proposed rule as called for below, it should create a new analysis of that rule, leaving it declassified in its entirety.

The NPRM claims the existence of a "risk-reduction analysis" that validates the proposed rule, such as it is. But the NPRM says that "the results of TSA's risk-reduction analysis are classified."

There is no possible way that the *results* of a risk-reduction analysis could possibly justify classification. It is possible that some parts of an entire risk-reduction

[22] Ethyl Corp. v. EPA, 541 F.2d 1, 48 (D.C. Cir. 1976) (quotation marks omitted).
[23] Am. Iron & Steel Inst. v. OSHA, 182 F.3d 1261, 1276 (11th Cir. 1999) (quotation marks omitted).

analysis could be subject to classification, but inappropriate use of classification authority that undercuts notice-and-comment rulemaking.

To arrive at these conclusions, we begin with a précis on risk management.

a. An understanding of risk management is essential

Risk management is the identification, assessment, and prioritization of risks[24] followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events. Everyone manages risk every day, in nearly every decision, substantial or insubstantial. But with the growth of large organizations and complex processes, risk management is a distinct planning and organizing tool. When a lot is on the line, it is worth taking time to manage risks articulately. And a lot is on the line with passenger air travel.

A formal risk management effort will generally begin with an examination of the thing or process being protected. This is often called "asset characterization."[25] Studying whatever infrastructure, business, or process one wants to protect will reveal what particular things are important about it, what weaknesses it might have, what things might threaten it, what would happen if it was damaged or destroyed, and so on. Asset characterization is the survey that begins the risk management process.

The next step in risk management is to identify and assess risks, often called "risk characterization" or "risk assessment." There are a few key concepts that go into it:

- *Vulnerability* is weakness or exposure that could prevent an objective from being reached. Vulnerabilities are common, and having a vulnerability does not damn an enterprise. The importance of vulnerabilities depend on other factors.

- *Threat* is some kind of actor or entity that might prevent an objective from being reached. When the threat is a conscious actor, we say that it "exploits" a vulnerability. When the threat is some environmental or physical force, it is often called a "hazard." As with vulnerability, the existence of a threat is not significant in and of itself. A threat's importance and contribution to risk turns on a number of factors.

With vulnerabilities and threats in hand, risk managers then make rough calculations about likelihood and consequence:

---

[24] Risk is defined in ISO 31000 as "the effect of uncertainty on objectives," whether positive or negative. *See* Wikipedia, "Risk Management" page, visited July 13, 2010, http://en.wikipedia.org/wiki/Risk_Management

[25] *See* Thomas L. Norman, Risk Analysis and Security Countermeasure Selection (Boca Raton: CRC Press, 2010), pp. 85-99.

- *Likelihood* is the chance that a vulnerability left open to a threat will materialize as an unwanted event or development that frustrates the objective. Knowing the likelihood that a threat will materialize is part of what allows risk managers to apportion their responses.

- *Consequence* is the significance of the loss or the impediment to objectives that would result should the threat materialize. Consequences can range from very low to very high. As with likelihood, gauging consequence allows risk managers to focus on the most significant risks.

Though these factors are often difficult to measure, a simple formula guides risk assessment:

Likelihood x Consequence = Risk

The matrix in Figure 1 illustrates which risks deserve little or no attention (green), which deserve some priority (yellow), which deserve prompt attention (orange), and which deserve immediate attention (red). Obviously, threats that are rare and inconsequential deserve no attention at all. Threats that are common and existential should be addressed first.

	Consequence				
Likelihood	Insignificant	Minor	Moderate	Major	Extreme
Rare	Low	Low	Low	Low	Low
Unlikely	Low	Low	Low	Medium	Medium
Possible	Low	Low	Medium	Medium	Medium
Likely	Low	Medium	Medium	High	High
Almost Certain	Low	Medium	Medium	High	Extreme

Figure 1. Risk Matrix, Combining Likelihood and Consequence

After risk assessment, the next step in risk management is choosing responses.

There are four general ways to respond to risk:

- *Acceptance* – Acceptance of a threat is a rational alternative that is often chosen when the threat has low probability, low consequence, or both.

- *Prevention* – Prevention is the alteration of the target or its circumstances to diminish the likelihood of the bad thing happening.

- *Interdiction* – Interdiction is any confrontation with, or influence exerted on, a threat to eliminate or limit its movement toward causing harm.

- *Mitigation* – Mitigation is preparation so that, in the event of the bad thing happening, its consequences are reduced.

An important consideration when choosing a response is whether or not the response creates new risks to the asset or to others. This is known as "risk transfer." Airport body scans, intended to interdict the smuggling of dangerous articles aboard planes, transfer risk to travelers who, averse to being scanned, choose to drive instead of fly. These travelers suffer injuries and die in greater numbers, as automobile travel is more dangerous than air travel.

The DHS Privacy Committee recommended use of a risk management model like this in 2006. [26] The NPRM exhibits no discernable methodology, and the resulting "rule" is arbitrary as a result.

To reach that conclusion, we had to guess at the agency's thinking. The inappropriate use of classification shields the documents that purportedly justify the rule and existing policy.

b. Classification of the risk management document is unwarranted

Under Executive Order 135256, classification is permitted if "disclosure of the information reasonably could be expected to result in damage to the national security, which includes defense against transnational terrorism." The order continues: "If there is significant doubt about the need to classify information, it shall not be classified." The need to classify the risk management work underlying the proposed rule is indeed doubtful, and its classification undercuts the purpose of notice-and-comment rulemaking.

Because risk analysis by its nature requires analysts to make assumptions and to work with data that are often far from precise, it is crucial that the full analysis be open and transparent. This allows other analysts to evaluate not only the results, but also the components from which they derive. As a RAND report puts it:

> [B]est practices for analytic products generally, and policy analysis modeling specifically, emphasize the importance of transparency and comprehensibility of the model; clear and candid accounting of its caveats, assumptions, and hypotheses; and a thorough assessment of how uncertainties in the model's logic, underlying theory or input data could affect its

[26] *See* Department of Homeland Security, Data Privacy and Integrity Advisory Committee, "Framework for Privacy Analysis of Programs, Technologies, and Applications," Report No. 2006-01 (Mar. 7, 2006) http://www.dhs.gov/xlibrary/assets/privacy/privacy_advcom_03-2006_framework.pdf.

findings.[27]

Obviously, risk analyses that have been classified do not conform to this important—indeed vital—characteristic.

There may be justifications for keeping from the public (and, by inference, attackers) details about body scanning—about its mechanical workings, for example, its error rate, or methods by which it might be defeated. However, analysis designed to assess the overall cost-effectiveness of a security measure does not need to delve into such issues. One might simply assume that the measure is technically effective and then seek to determine whether, given that assumption, it is cost-effective. Obviously, if it fails to be so, the measure should not be deployed no matter how technically effective it might be. On the other hand, if analysis conducted under that assumption deems the measure to be cost-effective, further analysis (which might then run into the classification issue) should be done to see if altering the assumption importantly changes the result about the measure's cost-effectiveness.

A second sort of detail that might be kept confidential is threat information that reveals sources and methods by which the information was gathered or that signals to threats that their existence or plans are known. (The latter could deter threats, which would be fine, but if it inspires threats to evade detection or capture, that would be a setback for security.) If a risk analysis reaches a level of detail that could compromise national security in these ways, the solution is simple: Dial back to a level of generality that is not so revealing.

As noted earlier, publishing the *results* of a risk-reduction analysis cannot possibly damage national security. Depending on how it was produced, there may be elements of TSA's "risk-reduction analysis" that merit redaction. But classification of the document as a whole is excessive and it undercuts the rulemaking disproportionately to the negligible risk that its release would create.

Credible and complete risk management analysis of TSA's airport body scanning policy has been done, publicly, by co-authors of this comment Mark G. Stewart of the University of Newcastle, Australia, and John Mueller of Ohio State University. Their analysis was published in 2011 in an important, peer-reviewed journal, *The Journal of*

[27] A. R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System*, pg. 98 RAND Corporation (2012), citing James H. Bigelow and Paul K. Davis, *Implications for Model Validation of Multi-Resolution Multiperspective Modeling (MRMPM) and Exploratory Analysis*, Santa Monica, Calif.: RAND Corporation, MR-1750-AF, 2003; Office of the Director of National Intelligence, Intelligence Community Directive, Number 203, Analytic Standards, Effective June 21, 2007; National Research Council, *Department of Homeland Security Bioterrorism Risk Assessment: A Call for Change*, Washington, D.C.: National Academies Press, 2008; and National Research Council of the National Academies, *Review of the Department of Homeland Security's Approach to Risk Analysis*, Washington, DC: National Academies Press, 2010 [hereinafter "NRC 2010"].

Homeland Security and Emergency Management, and it was included later in the year in their Oxford University Press book, *Terror, Security, and Money*. No one has ever asked Mueller and Stewart not to discuss their research, and they have been invited to present their findings at national security conferences open to the public.

Their study did not reveal unknown information or break any new analytical ground. Rather, they systematically and transparently applied standard risk-analytic and cost-effective procedures that have been codified and are routinely applied throughout the world when determining the desirability of measures and procedures intended to enhance security and welfare. Neither author of the study has heard objection from any quarter that their analysis exposes information that terrorists or other attackers could exploit.

Stewart and Mueller would, of course, be delighted to bring this experience to bear in evaluating any TSA studies that arrive at different conclusions, but they are prevented from doing so by the fact that such studies have been classified.

Walking through how well policies and technologies produce security can be done without revealing any intelligence about threats, and it can be done without revealing vulnerabilities in the policy and technology. The TSA's use of secrecy is inappropriate, and it should be reversed.

V. Risk management and cost-benefit analysis show that the policy supported by the proposed rule is not cost-effective

Nothing excuses the TSA from performing risk management and cost-benefit analyses that validate the proposed regulation, such as it is, and validate actual TSA practice at airports. Though it says that one exists and is classified, the language of the NPRM suggests either that the risk management and cost-benefit work underlying the proposed rule are invalid, or, as will be discussed more fully below, that the authors of the NPRM do not understand risk management.

Full-fledged, articulate risk management studies show that the policies in place under the proposed rule are not justified. Indeed, by shifting travelers to more dangerous automobiles, the policies currently in place may cause more travelers to die than it saves.

a. Nothing excuses TSA from using risk management and cost-benefit analysis

There is no argument that current policies are dictated by statute. The court said so in *EPIC v. TSA*: "Although the statute, 49 U.S.C. § 44925, does require the TSA to develop and test advanced screening technology, it does not specifically require the TSA to deploy AIT scanners let alone use them for primary screening."[28] The authorities cited

[28] EPIC v. TSA at 10.

in the preamble to the proposed rule do not exempt the TSA from rational cogitation about its policies in the course of the instant rulemaking.

Indeed, listing a variety of possible technologies, 49 U.S.C. § 44925 calls for "*optimal* utilization and deployment of explosive detection equipment…." (emphasis added). None of the hortatory language in appropriations conference reports and other legislative history since then overcomes the statutory requirement of "optimal" use of technology. Optimization requires risk management and balancing of costs and benefits. The agency must flesh out its policies through the rational processes required in administrative law.

Among the things the agency must take into account, which it does not in the preamble, is "the public right of freedom of transit through the navigable airspace" referred to in 49 USC § 40101 and 49 USC § 40103. These two statutory provisions do not establish a statutory right for purposes of administering that title of the U.S. Code. They acknowledge a preexisting right. The TSA must minimize its interference with the right of travel in the course of optimizing its policies and the rule.

The agency must also take into account the Fourth Amendment to the U.S. Constitution, which bars unreasonable searches and seizures. Though the court in *EPIC v. TSA* summarily concluded that the use of body scanners fell within the "administrative search" exception to Fourth Amendment protection,[29] the issue was not ripe for decision, as the court did not have a rulemaking record before it. This rulemaking may invalidate the *EPIC v. TSA* decision as to the Fourth Amendment merits, and other courts will reconsider the issues in light of the record in this rulemaking.

b. Amidst talk of risk management, DHS and TSA have long failed to implement risk-based decision-making, and they fail to do so here

Homeland security is concerned with public safety—or domestic tranquility—the central, foundational reason for government. It is imperative, therefore, that decisions and expenditures be made sensibly and responsibly in this area because human lives are at stake.

To do so requires applying the kind of analytic risk management approaches that are routinely required of other governmental agencies and that have been standard coin for policy decision making for decades throughout the world. These approaches seek to balance the competing demands of safety and cost even in such highly charged and politicized decisions as where to situate nuclear power plants, how to dispose of toxic waste, and how to control pollution—decisions that engage the interests and passions of multiple groups.

[29] EPIC v. TSA at 16-18.

Most policies aimed at security will improve security. The important question is not whether a given policy improves security. It is whether the improvement in security justifies its costs. Nothing in the preamble to the proposed rule overcomes the evidence that the current body scanning policy does not provide cost-effective security. Indeed, it could produce greater death among American travelers than it averts.

Risk reduction measures that produce little or no net benefit to society or produce it at very high cost are not only irresponsible but also, essentially, immoral. When we spend resources to save lives at a high cost, we forgo the opportunity to spend those same resources on regulations and measures that can save more lives at the same cost or even at a lower one. Bad risk management kills.

Upon taking office in 2005, Department of Homeland Security (DHS) Secretary Michael Chertoff strongly advocated that the department "must base its work on priorities driven by risk."[30] Yet, a year later, when DHS expenditures had increased by some $135 billion beyond those already in place in 2001, and when the department had become the government's largest nonmilitary bureaucracy, one of its senior economists wistfully noted, "We really don't know a whole lot about the overall costs and benefits of homeland security."[31] By 2007, RAND President James Thomson was contending that DHS leaders "manage by inbox," that the "dominant mode of DHS behavior" was not risk management, but "crisis management."[32] In the same year, the Congressional Research Service after an exhaustive assessment, concluded that DHS simply could not answer the "central question" about the "rate of return, as defined by quantifiable and empirical risk reductions" on its expenditure.[33]

The emphasis on risk-informed decision making continued with the change of administrations after the 2008 elections, as Secretary Janet Napolitano insisted, "Development and implementation of a process and methodology to assess national risk is a fundamental and critical element of an overall risk management process, with the ultimate goal of improving the ability of decision makers to make rational judgments about tradeoff s between courses of action to manage homeland security risk."[34]

Yet a 2010 report of the National Research Council of the National Academies of Sciences, Engineering, and Medicine ("NRC") suggests that little progress had been

---

[30] Mayer, Matt A. 2009. *Homeland Security and Federalism: Protecting America from Outside the Beltway*, p. 62 (Santa Barbara, CA: ABC-CLIO).
[31] Troy Anderson, "Terror May Be at Bay at Port; Shipping Hubs Too Vulnerable," *Daily News of Los Angeles* , May 18, 2006.
[32] James A. Thomson, "DHS AWOL? Tough Questions about Homeland Security Have Gone Missing," *RAND Review* , Spring 2007.
[33] Todd Masse, Siobhan O'Neil, and John Rollins. *The Department of Homeland Security's Risk Assessment Methodology: Evolution, Issues, and Options for Congress*, pg. 14, Washington, DC: Congressional Research Service, February 2, 2007.
[34] NRC 2010, pg. 108.

made by that time. Requested by Congress to assess the activities of the Department of Homeland Security, a committee worked for nearly two years and came up with some striking conclusions. Except for the analysis of natural disasters, the committee "did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making," and therefore "only low confidence should be placed in most of the risk analyses conducted by DHS." Indeed, "little effective attention was paid to the features of the risk problem that are fundamental."[35]

The committee also found an "absence of documentation of methods and processes," with the result that the committee sometimes had to *infer* details about DHS risk modeling. In fact, "in a number of cases examined by the committee, it is not clear what problem is being addressed." It also found "a pattern" of "trusting numbers that are highly uncertain." Concluded the committee: "It is not yet clear that DHS is on a trajectory for development of methods and capability that is sufficient to ensure reliable risk analyses": although it found that "there are people at DHS who are aware of these current limitations," it "did not hear of efforts to remedy them."[36]

This situation is particularly strange because, as the committee also noted, the risk models used in the department for *natural* hazards are "near state of the art" and "are based on extensive data, have been validated empirically, and appear well suited to near-term decision needs."[37]

At times DHS has ignored specific calls by other government agencies to conduct risk assessments. For example, GAO requested that DHS conduct a full cost-benefit analysis of the extremely costly process of scanning 100 percent of U.S.-bound containers. To do so would require the dedicated work of a few skilled analysts for a few months or possibly a year. Yet, DHS replied that, although it agreed that such a study would help to "frame the discussion and better inform Congress," to actually carry it out "would place significant burdens on agency resources."[38]

The DHS appears to focus all or almost all of its analyses on the contemplation of the consequences of a terrorist attack while substantially ignoring the equally important "likelihood" component of risk assessment—whether the attack will happen or not—as well as the key issue of risk reduction. DHS risk assessment seems to simply identify a potential source of harm and then try to do something about it without evaluating whether the new measures reduce risk sufficiently to justify their costs. Kip Hawley, head of the TSA when the NRC report came out, responded, unconvincingly and contrary to the

[35] NRC 2010, pg. 11.
[36] NRC 2010, pg. 65.
[37] NRC 2010, pg. 57
[38] United States Government Accountability Office, "Report to Congressional Requesters: Supply Chain Security: Feasibility and Cost-Benefit Analysis Would Assist DHS and Congress in Assessing and Implementing the Requirement to Scan 100 Percent of U.S.-Bound Containers," GAO-10-12, October 2009.

conclusions of the report, that risk analytic work is done by TSA. "It's just not done the way they are defining it."[39]

In 2007, TSA, under Hawley, commissioned Boeing to develop and operate a Risk Management Analysis Tool ("RMAT"). In 2010 the agency asked RAND to evaluate the tool—"before relying on RMAT results for high-stakes resource management and policy decisions," according to the RAND report which came out late last year. RMAT is a "suite of tools and processes for conducting risk assessments" designed "to model and explain the complex interactions between security providers and systems and adversaries."

It is not clear how it is put together because the tool remains proprietary, but the RAND report is quite critical. The tool has "thousands of input variables," many of which cannot be estimated with much precision, and it could generate results that are "completely wrong." Moreover, it takes so long to run that "neither RAND nor Boeing have been able to conduct even a superficial sensitivity analysis" of its "many thousands of assumptions and parameter estimates." Moreover, it only deals with relative risk, not absolute risk (a key criticism as well in the 2010 NRC study), and its estimates of these "are subject to strong, probably untenable, assumptions." RMAT is also insensitive to changes in the magnitude of risk and "assumes no attack can be deterred."[40]

Little appears to have changed, as the NPRM devotes only one sentence to the cost-effectiveness of this security measure, and that sentence is problematic: "Risk reduction analysis shows that the chance of a successful terrorist attack on aviation targets generally decreases as TSA deploys AIT." This is a statement of the obvious. Virtually any new security measure—adding one bomb-sniffing dog at one airport, for example—will in some sense decrease the risk of a successful terrorist attack, however microscopically. The question risk analysis seeks to answer is not simply, "Will the added security measure reduce risk?" (or "generally decrease[]" it), but rather, "Will it reduce the risk enough to justify its cost?"

In 2010, the Government Accountability Office considered body scanning technology then being deployed by TSA. It noted pointedly that "cost-benefit analyses are important because they help decision makers determine which…investments in technologies or in other security programs, will provide the greatest mitigation of risk for the resources that are available," and it specifically declared that conducting a cost-benefit analysis of the new, expensive technology was "important."[41]

---

[39] Steven Cherry, Airport Security: Everything You Know Is Wrong, Techwise Conversations (podcast), May 2, 2012.

[40] A.R. Morral et al., *Modeling Terrorism Risk to the Air Transportation System*, p. 98 RAND Corporation, 2012.

[41] Lord, Steve. *Aviation Security: TSA Is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to This Effort and Areas of Aviation Security Remain.* United States Government Accountability Office, GAO-10–484T, March 17, 2010.

By simply stating that body scanners reduce risk—not that they reduce risk enough to justify their cost—the one sentence in the NPRM devoted to this key issue hints that risk analysis sufficient to validate the rule may not have been conducted.

c. TSA's body scanners fail to be cost-effective

Co-authors of this comment John Mueller and Mark Stewart have conducted exactly the sort of analysis that is required by this rulemaking. At several points, their study biased the analysis in favor of finding body scanning technology to be cost-effective security, and they assumed that it is technically effective at detecting body-borne explosives. Even under these generous assumptions, they found body scanners to be cost-ineffective.

The Mueller/Stewart analysis was published in 2011 in the peer-reviewed *Journal of Homeland Security and Emergency Management*, and it was included later in the year in their Oxford University Press book, *Terror, Security, and Money*. The version published in the *Journal of Homeland Security and Emergency Management* is attached to this comment as Appendix I.

The discussion below is a development of material presented in the 2011 article. It takes a complementary approach, but, while the input data and conclusions are the same, numerical results differ slightly from those in the 2011 analysis because of a change in the definition of what constitutes a successful attack.

The standard definition of risk adopted by the DHS is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequences})$$

where:

- *Threat* = annual probability a successful terrorist attack will take place if the security measure were not in place.
- *Vulnerability* = probability of loss (*i.e.*, that an explosive will be successfully detonated leading to damage and loss of life) given the attempt.
- *Consequences* = loss or consequence (economic costs, number of people harmed) if the attack is successful in causing damage.

Assuming 100% vulnerability, the above equation simplifies to:

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

Reduction in risk is the degree to which a security measure foils, deters, disrupts,

or protects against a terrorist attack.

The *benefit* of a security measure is the sum of the losses averted due to the security measure and any expected co-benefit from the security measure not directly related to mitigating vulnerability or hazard (such as reduction in crime, improved passenger experience, etc.). This benefit is then compared to the cost of the security measure, which should include opportunity costs, to determine cost-effectiveness. A security measure is cost-effective if the benefit exceeds the cost. The benefit of a security measure, then, is calculated:

Benefit = (Probability of a Successful Attack) x (Losses Sustained in an Attack) x (Reduction in Risk Generated by the Security Measure)

One can apply a common, government-approved approach called break-even analysis to these problems. In break-even analysis, one calculates what the likelihood of an otherwise successful attack would have to be to justify a security measure's cost. There are three key considerations in applying this approach.

Reduction in risk generated by the security measure

The threat that body scanners are primarily dedicated to is preventing the downing of a commercial airliner by an improvised explosive device (IED) smuggled on board by a passenger. The present analysis assumes that the terrorist successfully arrives at an airport undetected and proceeds to airline passenger screening bearing a concealed IED.

The analysis then assumes that the terrorist's luck substantially continues to hold through the next barriers:

- the likelihood of successfully avoiding detection by the metal detector and checkpoint transportation security officers is 90%,
- the likelihood of avoiding successful crew and passenger resistance on board the airliner when attempting to set off the bomb is 50%,
- the likelihood of successfully detonating the explosive is 75%, and
- the likelihood the explosion will actually down the airliner is 75%.

Under these conditions, there is a 75% chance the attack will fail due to one or another of these measures: existing checkpoint security measures, crew and passenger resitance, terrorist incompetence and amateurishness, and the technical difficulties in setting off a bomb sufficiently destructive to down an airliner.

The analysis now adds the body scanner/pat-down to this mix of security measures and assumes that the measure reduces the likelihood of a successful attack almost completely—by 85-90%.

The chance the terrorist will fail due to one of another of the existing measures or due to the body scanner now approaches an impressive 97%.

The cost of the security measure

Using TSA figures, it can be determined that the cost of purchasing, installing, maintaining, and staffing 1,800 body scanners will be $1.2 billion per year after it is fully deployed. A 2012 Congressional Research Service (CRS) comes to the same conclusion.[42] It also finds: "Even at full operating capacity, not all airports and not all screening lanes will be equipped with AIT under TSA's plan." Body scanners would clearly need to be fully deployed to be truly effective because, if some airport security lines do not use the technology, it would obviously be a matter of only minor inconvenience for terrorists to determine where the gaps are simply by visiting airports and taking a look—assuming they couldn't get the information on the web.

The NPRM arrives at a significantly lower cost estimate of roughly $400 million per year. However, the NPRM does not say how many scanners it assumes will be deployed, and personnel and operating costs decrease by 20% in 2014 and 2015 while scanner equipment costs increase by over 20% in the same period. This is a clear inconsistency, as more scanners should mean higher staff and operating costs. The NPRM also gives 'net costs' as these deduct the cost of not using metal detectors, yet a walk-through metal detector costs less than $2,000 compared to over $150,000 for a full-body scanner, and staffing will be significantly higher to operate and maintain the new scanners. TSA cost summaries are anything but transparent.

The consequences of a successful terrorist attack

The consequences of a successful terrorist attack where an IED detonates and downs in an airliner would be quite high: somewhere between $2-50 billion, which can be averaged to $25 billion including property loss, loss of lives, and the impact on the economy and on air travel. There have been many studies of such costs inflicted by the 9/11 disaster, and these generally run from around $100 billion to $200 billion. The cost consequences of the successful terrorist downing of a single commercial airliner that does not crash into a significant building on the ground would clearly be less—though they would still be quite substantial.

[42] Bart Elias, *Airport Body Scanners: The Role of Advanced Imaging Technology in Airline Passenger Screening*, Congressional Research Service, September 20, 2012.

Results

Applying these assumptions and estimates, body scanners only become cost-effective when the likelihood that there will be a successful attack if the body scanners were not included in the array of security measures is 22%—or one every five years.

TSA body scanning policy seems, then, rather impressively to fail a cost-effectiveness test, even one that very considerably biases the discussion in favor of coming to the opposite conclusion.

In the nine years after 9/11—before body scanners began to be deployed—there were only four instances in which a terrorist boarded (or, it seems, even attempted to board) an aircraft with body-borne explosives. Two of these failed (the 2001 shoe and 2009 underwear bombers), and two were carried out by Chechen women in Russia. None of these boarded their aircraft in the United States where the TSA's body scanners are deployed.

There is a very high likelihood that terrorists would be foiled, deterred or disrupted by police and security services, tip-offs from the public, and other pre-screening security measures at the airport, including no-fly lists, travel document checkers, behavioral detection officers, bomb appraisal officers, and other TSA and policing layers of security. But the analysis essentially assumed these had no effect.

It should also be noted that, since 9/11, only one attack consisting of two explosions has occurred in the United States, and this was on terra firma in Boston in 2013, using devices that could not pass through the magnetometers or x-ray machines that preceded body scanning in American airports. Similarly, there has been one case in which terrorists have been able to detonate bombs in the UK, producing four explosions, also on the ground, on the London transit system in 2005. This experience suggests that, for the most part, the terrorist adversary is not a terribly capable one.[43] Accordingly, the study was very generous in assuming that, if a terrorist were able to get his bomb on board and if he remained un-harassed by crew and passengers, he would still be 75% likely to successfully to detonate his bomb.

PETN seems to be the preferred explosive, and it has a long history of use in terrorist attacks. However, like most stable explosives, it is not easy to ignite. The best detonators are metallic but these are detectable by the airline security measures that were already in place before 9/11. Thus, the underwear bomber of 2009 used a syringe filled with a liquid explosive like nitroglycerin to detonate the PETN. However, this is by no

[43] Michael Kenney, "'Dumb' Yet Deadly: Local Knowledge and Poor Tradecraft among Islamist Militants in Britain and Spain," *Studies in Conºict & 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 × 0.001 × 0.004% = one in 60 million.

Howard Kunreuther, "How much should we be willing to pay for a small reduction in probabilities that are already extremely low?"[62]

f. It is not clear that the machines actually secure against attacks

Under highly favorable assumptions that only consider dollar expenditures, body scanners are not cost-effective security. When the privacy consequences of rendering nude images of American travelers are added in along with other costs, the evidence that body scanners fail cost-benefit analysis rises to overwhelming.

This analysis assumes that the machines work perfectly to discover explosives and similar threats. Whether this is a valid assumption, however, appears questionable. Certainly TSA officials' public pronouncements on this issue are less than fully reassuring.

When TSA Administrator John Pistole appeared on the PBS NewsHour on November 16, 2010, he was specifically asked: "A lot of passengers are wondering whether these procedures are proportionate to the threat. And I'm just wondering, would, for instance, these more extensive pat-downs and the full-body scans, would they have caught the Christmas Day bomber with the explosives in his underwear?"

Interestingly Pistole did not answer or comment on that question directly. To the key issue about whether the procedures are proportionate to the threat, he simply said, "I know the threats are real." This observation is relevant, but scarcely responsive. His response to the question about whether the measures would have caught the underwear bomber was equally evasive: "I believe that the techniques and the technology we're using today are the best possible that we have. And it gives us the best opportunity for detecting a Christmas Day-type bomber."

To her credit, the interviewer, Margaret Warner, persisted for one more round: "Are there any other examples of people who have gotten through with explosive material that weren't caught that would have been caught with these new methods?"

This generated a response that can charitably be characterized as irrelevant: "We know that the General Accounting Office and the Homeland Security inspector general and even our own TSA Office of Inspection does what we refer to as covert testing. Now, I can't go into the details of those, but some of the results of those are that we could and should improve the techniques that we use to do the security screening."

The TSA's NPRM is distinctly less than clear on this issue, offering ambiguous assertions like:

---

[62] Howard Kunreuther, "Risk Analysis and Risk Management in an Uncertain World," *Risk Analysis* , 22(4) 2002, pg. 662–663.

> "AIT currently provides the best available opportunity to detect non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security layers."
>
> "The best defense against these and other terrorist threats remains a risk-based, layered security approach that uses a range of screening measures, both seen and unseen. This includes the use of AIT, which is proven technology for identifying non-metallic explosives during passenger screening, such as the device Umar Farouk Abdulmutallab attempted to detonate on Christmas Day 2009."
>
> "Advanced Imaging Technology is proven technology which provides the best opportunity to detect metallic and non-metallic anomalies concealed under clothing without touching the passenger and is an essential component of TSA's security. Since it began using AIT, TSA has been able to detect many kinds of non-metallic items, small items, and items concealed on parts of the body that would not have been detected using metal detectors."

Language arguing that body scans are the "best available opportunity" or provide the "best defense" or have detected items missed by other technologies does not make the case that it really works to detect body-borne bombs or bomb material. And it is certainly not the same as saying that the measure is cost-effective.

VI. The body scanning policy should be reversed pending a new, sufficient rulemaking

Due to TSA policies that the proposed rule would ratify, many Americans avoid air travel altogether, preferring to drive long distances instead. This may result in as many as 500 deaths per year, deaths that are attributable to these policies.

The benefits of notice-and-comment rulemaking accrue when the public is allowed to comment on a rule that has contours. In the ideal rulemaking—not even ideal: in the usual rulemaking—a proposed rule delineates much of what may appear in the final rule. This allows affected parties to comment intelligently on manifold nuances of the proposed rule. The agency can then consider the wisdom offered by interested parties with perspective and experience that the agency lacks. The result is often a rule that is improved.

By proposing a rule without contours, and by hiding the analysis that might support even the general policy statement proposed, the TSA has denied the public the ability to meaningfully comment. TSA has also denied itself the ability to learn how its practices (and analyses) could be improved. In an important sense, the rulemaking has already failed.

By proposing a policy statement as if it were a legislative rule, the agency may have irreparably biased the process against the public participation required by notice-and-comment rulemaking. It is unacceptable that the agency's failure in the present notice-and-comment rulemaking should aid the agency in maintaining its disputed policy.

None of the remedies for this are attractive, but given our conclusion that the TSA's current policies cause more death than they avert, the TSA should voluntarily adopt the presumption that its current practices are not justified. TSA should suspend the use of body scanners for primary screening, initiate a rulemaking around a true legislative rule, and await the results of that rulemaking and subsequent litigation before it proceeds with the policy of using body scanners for primary screening.

Reversing the present policy would likely save American lives, reduce taxpayer expenditures, and relieve an impediment to economic growth in the travel industry.

Journal of Homeland Security and Emergency Management

Volume 8, *Issue* 1 2011 *Article* 30

Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening

Mark G. Stewart, *The University of Newcastle, Australia*
John Mueller, *Ohio State University*

Recommended Citation:
Stewart, Mark G. and Mueller, John (2011) "Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening," *Journal of Homeland Security and Emergency Management*: Vol. 8: Iss. 1, Article 30.
DOI: 10.2202/1547-7355.1837
Available at: http://www.bepress.com/jhsem/vol8/iss1/30

Cost-Benefit Analysis of Advanced Imaging Technology Full Body Scanners for Airline Passenger Security Screening

Mark G. Stewart and John Mueller

Abstract

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AITs) that are full-body scanners to inspect a passenger's body for concealed weapons, explosives, and other prohibited items. The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. The cost of this technology will reach $1.2 billion per year by 2014. The paper develops a preliminary cost-benefit analysis of AITs for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and costs of security measures in the estimation of costs and benefits. Since there is uncertainty and variability of these parameters, three alternate probability (uncertainty) models were used to characterise risk reduction and losses. Economic losses were assumed to vary from $2-$50 billion, and risk reduction from 5-10 percent. Monte-Carlo simulation methods were used to propagate these uncertainties in the calculation of benefits, and the minimum attack probability necessary for full body scanners to be cost-effective were calculated. It was found that, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. However, the attack probability needs to exceed 160-330 percent per year to be 90 percent certain that full body scanners are cost-effective.

KEYWORDS: terrorism, security, cost-benefit analysis, aviation security, passenger screening

Author Notes: Mark G. Stewart, Australian Research Council Professorial Fellow; Professor and Director, Centre for Infrastructure Performance and Reliability, The University of Newcastle, New South Wales, 2308, Australia; phone: +61 2 49216027; email: mark.stewart@newcastle.edu.au. John Mueller, Professor of Political Science and Woody Hayes Chair of National Security Studies, Mershon Center for International Security Studies and Department of Political Science, Ohio State University, Columbus, Ohio 43201, United States; phone: +1 614 2476007; email: bbbb@osu.edu. Part of this work was undertaken while the first author was a Visiting Professor in the Department of Civil, Structural and Environmental Engineering at Trinity College Dublin. He greatly appreciates the assistance provided by Trinity College. The first author also appreciates the financial support of the Australian Research Council.

INTRODUCTION

The Transportation Security Administration (TSA) has been deploying Advanced Imaging Technologies (AIT) that are full-body scanners to inspect a passenger's body for concealed weapons and explosives. The cost of this technology will reach $1.2 billion per year by 2014. The U.S. Government Accountability Office (GAO) remarked in 2010 that "conducting a cost-benefit analysis of TSA's AIT deployment is important.", and "would help inform TSA's judgment about the optimal deployment strategy for the AITs" (Lord 2010). Yet, before deciding to install AITs at considerable cost the TSA has not conducted a cost-benefit analysis. This absence of a cost-benefit analysis for AITs is the motivation for the present study.

Since the events of 9/11 there has been much focus on preventing or mitigating damage and casualties caused by terrorist activity. A key issue is whether counter-terrorism expenditure has been invested in a manner that optimizes public safety in a cost-effective manner. This is why the 9/11 Commission report, amongst others, called on the U.S. government to implement security measures that reflect assessment of risks and cost-effectiveness. However, while the U.S. requires a cost-benefit analysis for government regulations (OMB 1992), this does not appear to have happened for most homeland security expenditure.

The need for risk and cost-benefit assessment for homeland security programs, and those supported by the Department of Homeland Security (DHS) in particular, is forcefully made by many in government, industry and academe (e.g., Friedman 2010, Poole 2008). The U.S. National Research Council (NRC 2010), after a 15 month study period, made critical recommendations about the DHS, and their primary conclusion was: "the committee did not find any DHS risk analysis capabilities and methods that are yet adequate for supporting DHS decision making, because their validity and reliability are untested" and "only low confidence should be placed in most of the risk analyses conducted by DHS".

To compare costs and benefits requires the quantification of threat probability, risk reduction, losses, and security costs. This is a challenging task, but necessary for any risk assessment, and the quantification of security risks is recently being addressed (e.g., Stewart et al. 2006, Stewart and Netherton 2008, Dillon et al. 2009, Cox 2009), as well as recent life-cycle and cost-benefit analyses for infrastructure protective measures (Willis and LaTourette 2008, von Winterfeldt and O'Sullivan 2006, Stewart 2008, 2010, 2011). Much of this work can be categorized as 'probabilistic terrorism risk assessment'.

Stewart (2010) has shown that, based on expected values, the threat probability has to be very high for typical counter-terrorism measures for buildings and bridges to be cost-effective. Similar cost-benefit analyses have

shown that the U.S. Federal Air Marshal Service which costs over $1 billion per year fails to be cost-effective, but that hardening cockpit doors is very cost-effective (Stewart and Mueller 2008). It therefore appears that many homeland security measures would fail a cost-benefit analysis using standard expected value methods of analysis as recommended by the U.S. Office of Management and Budget (OMB); a detailed assessment of threats and vulnerabilities leads to similar conclusions (Mueller 2010, Mueller and Stewart 2011). This suggests that policy makers within the U.S. government and DHS are risk-averse.

Terrorism is a frightening threat that influences our willingness to accept risk, a willingness that is influenced by psychological, social, cultural, and institutional processes. Moreover, events involving high consequences can cause losses to an individual that they cannot bear, such as bankruptcy or the loss of life. On the other hand, governments, large corporations, and other self-insured institutions can absorb such losses more readily and so governments and their regulatory agencies normally exhibit risk-neutral attitudes in their decision-making (e.g., Sunstein 2002, Ellingwood 2006). This is confirmed by the OMB which requires cost-benefit analyses to use expected values (an unbiased estimate), and where possible, to use probability distributions of benefits, costs, and net benefits (OMB 1992).

For many engineering systems the threat rate is known, but for terrorism the threat is from an intelligent adversary who will adapt to changing circumstances. For this reason, a practical approach is a 'break even' cost-benefit analysis that finds the minimum probability of a successful attack required for the benefit of security measures to equal their cost. While this approach is not without challenges (Farrow and Shapiro 2009), 'break-even' cost-benefit analyses are increasingly being used for homeland security applications (e.g., Ellig 2006, Willis and LaTourette 2008, Winterfeldt and O'Sullivan 2006). Hence, we will undertake a 'break even' cost-benefit analysis in this paper.

The terrorist threat that AITs are primarily dedicated to is preventing the downing of a commercial airliner by an IED (Improvised Explosive Device) smuggled on board by a passenger. Since AITs operated by the TSA are effective only for passengers leaving the U.S., the present paper considers the threat probability, risk reduction and losses for a suicide bomber who attempts to board an aircraft at a U.S. airport. This preliminary study will also include uncertainty analysis in the cost-benefit calculations to reflect the uncertainty in underlying data and modeling assumptions, and will allow the probability of cost-effectiveness to be calculated. AITs are being trialed or deployed in the U.K., France, Netherlands, Italy, Canada, Australia and elsewhere which will cost billions of dollars if they are also used for primary screening in those countries. Hence, the present paper will provide useful guidance to U.S. and international aviation security regulators.

RISK AND COST-BENEFIT METHODOLOGY

A security measure is cost-effective when the benefit of the measure outweighs the costs of the security measure. The *net benefit of a security measure* is:

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

- 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 $C_{security}$=$1.2 billion per year and will ignore opportunity costs - although these have the potential to be very substantial. We also ignore any possible security theatre benefits - likely, however, to be small as there is little evidence that AITs by themselves will make travelers feel much safer, and could well have the opposite effect.

Economic Loss (C_{loss})

The loss of an aircraft and follow-on economic costs and social disruption might be considerable. A 2007 RAND study reported that the loss of an airliner with 300 passengers by a shoulder fired missile, a shutdown of U.S. airspace for a week, and 15% drop in air travel in the 6 months following the attack would cause an economic loss of more than $15 billion (Chow et al. 2005). Another study, again assuming an attack using shoulder fired missiles also assumed a seven day shutdown, but a two-year period of recovery (Gordon et al. 2007). Losses were summed across airline, ground transportation, accommodation, food, gifts/shopping and amusement sectors to derive loss estimates of $214-$420 billion. This seems overly conservative as adding up individual sectoral losses can lead to double counting and "that large scale terrorist attacks cause reallocations

of people and resources across sectors" and "it is relatively easy to measure the heavy losses experienced by some areas but very difficult to measure the small indirect gains experienced by thousands of areas." (Enders and Olsen 2011).

The downing of an airliner due to an passenger-borne IED is likely not to trigger the same response as a downing caused by a shoulder fired missile as no counter-measures exist for a missile attack that could be implemented quickly. On the other hand, a series of screening measures were implemented quickly following the 9/11 and subsequent attacks that provides assurance to the public that it is safe to fly. This all suggests that the losses forecast above for a shoulder-fired missile attack will over-estimate losses for our threat scenario.

A report for the DHS concludes that the best estimate for value of a statistical life (VSL) for homeland security analysis is $6.5 million in 2010 dollars (Robinson et al. 2010). If we take 300 lives at VSL of $6.5 million then the economic loss caused by 300 fatalities is approximately $2 billion. If we add the cost of a large commercial airliner of $200-$250 million then direct economic loss is approximately $2.5 billion if we also include forensic and air transport crash investigations. Passenger numbers less than 300 will reduce direct losses considerably, for example, 150 passenger will reduce direct losses to $1.5 billion. However, we will select C_{loss}=$2 billion as a reasonable lower bound.

To establish something of an upper bound for the losses inflicted by conventional terrorist attacks, it may be best to begin with the losses inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. A study by the National Center for Risk and Economic Analysis of Terrorist Events found that the impact on the U.S. economy of the 9/11 attacks range from 0.3 to 1.0 percent of GDP (Blomberg and Rose 2009). While the $15 billion proposed by the RAND study would be a plausible upper value of economic loss, it may fail to consider full losses to the economy. The economic consequences of a suicide bomber would likely be less than the shocking events of 9/11, so we will assume that a reasonable upper bound of losses is 0.3% of GDP ($42 billion based on 2010 GDP figures) which we will round up to C_{loss}=$50 billion.

Results from uncertainty and probabilistic modeling may be sensitive to the shape of the probability distribution. In this case, we will assume three alternate probability distributions of loss (see Figure 1):

1. Normal Distribution - loss is normally distributed with 95% confidence interval between $2 billion and $50 billion, then mean loss is $26 billion and standard deviation is $12.2 billion. Loss is truncated at $500 million to represent loss of a single aircraft with few passengers and no indirect losses.
2. Uniform Distribution - equal likelihood of any loss between $2 billion and $50 billion, with mean loss of $26 billion.

3. Triangular Distribution - higher likelihood of smaller losses bounded by $2 billion and $50 billion, with mean loss of $18 billion.

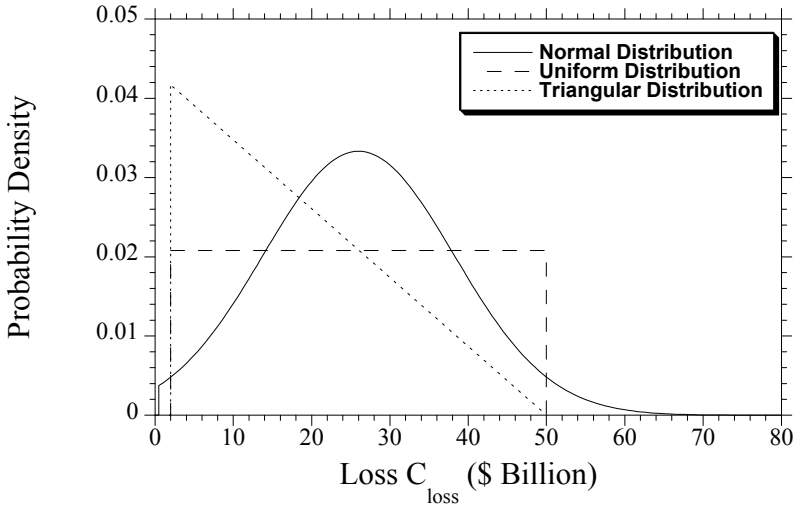

Figure 1. Alternative Loss Uncertainty Models.

Risk Reduction (ΔR)

A key motivation for the rapid deployment of AITs was the foiled 2009 Christmas Day plot by Umar Farouk Abdulmutallab to hide liquid explosives in his underwear to blow-up Northwest Airlines Flight 253. There is little doubt that that full-body scanners improve the ability to detect weapons and explosives, however, there is doubt about their ability to detect *all* explosives that may be hidden on a person. The GAO follows this line of reasoning by casting doubt on the ability of AITs to detect the weapon Abdulmutallab used in his attempted attack (Lord 2010). It is also suggested that existing screening methods, such as detectors that test swabs wiped on passengers and luggage for traces of explosives, would have detected the explosives used in the 2009 Christmas Day attack. Moreover, the search for a detonator is equally important and easier to detect since most detonators contain metal.

Also relevant is the fact that it is not necessarily easy to blow up an airliner even if a bomb detonates. Airplanes are designed to be resilient to shock, and attentive passengers and airline personnel complicate the terrorists' task further. Apparently, the explosion over Lockerbie was successful only because the suitcase bomb just happened to have been placed at the one place in the luggage compartment where it could do fatal damage (Bayles 1996). Logically, then, a terrorist will not leave such matters to luck, which may be why the shoe and

underwear bombers both carried their bombs onto the planes and selected window seats that are, of course, right next to the fuselage. Yet even if their bombs had exploded, the airliner might not have been downed. The underwear bomber was reported to be carrying 80 grams of the explosive PETN (PETN or Pentaerythritol tetranitrate) and when his effort was duplicated on a decommissioned plane in a test set up by the BBC, the blast did not breach the fuselage (BBC 2010), although the explosive test was conducted while the aircraft was on the ground. Moreover, an aircraft may not be doomed even if the fuselage is ruptured. In 2008 an oxygen cylinder exploded on a Qantas flight blasting a two meter hole in the fuselage. In 1989, a cargo door opened on a United Airlines flight heading across the Pacific extensively damaging the fuselage and cabin structure adjacent to the door. In both instances the aircraft landed safely. Aircraft, like many types of infrastructure are more robust and resilient than we often give them credit for.

PETN has a long history of use in terrorist attacks but, like most stable explosives, it's not easy to ignite. Presumably because airport screening makes smuggling a metal detonator a risky proposition, the underwear bomber used a syringe filled with a liquid explosive like nitroglycerin. However, this adds to the difficulty of a successful detonation.

Since two Russian airliners were blown up by terrorists in 2004, the terrorist's task is obviously not impossible. However, it is a difficult one, and terrorists trying to detonate explosives in flight are likely to end up with more duds than successes. Moreover, although their explosion may cause real damage and loss of life, this result is by no means guaranteed: aircraft have shown themselves to be resilient to accidental explosions or other mid-air mishaps, and so 'blowing up' an airliner is more challenging than we imagine.

Although some terrorists are skilled and well trained, many terrorist attacks in the U.K, U.S. and Afghanistan were averted by the 'ineptitude' of the terrorists themselves. Moreover, many, but not all, terrorists lack bomb-making skills such as those behind the failed car bombings in London and Glasgow in 2007, and Times Square in 2010 (Kenney 2010). Assembling and detonating a small or miniaturized IED needed to minimize the chances of passenger screening detection is even more challenging than their larger compatriots. This all suggests that even if a terrorist can board an aircraft and attempt to detonate the device undetected, there is no 100% surety that the bomb will successfully detonate - poor training, lack of hands-on experience and poor tradecraft means there is a good chance that the IED will be a 'dud'.

Suicide bombers, like drug couriers, can go to inordinate lengths to conceal weapons or contraband - including body cavities. In August 2009 Abdullah Hassan al-Asiri attempted to assassinate a Saudi prince by detonating 100 grams of PETN, which according to some reports was concealed in his underwear, and other reports, his rectum. A Europol (2009) study confirmed that

concealment of IEDs in rectal cavities was possible but that the body would absorb much of the blast. This explains why Asiri succeeded in only killing himself, while the Saudi prince who stood close by escaped unharmed. It would seem that a terrorist would need to remove explosives from their underwear for it to be fully effective against a target - an act which increases the odds of detection.

The TSA has arrayed '21 Layers of Security' to 'strengthen security through a layered approach'. This is designed to provide defense-in-depth protection of the travelling public and of the United States transportation system. Of these 21 layers, 15 are 'pre-boarding security' (i.e., deterrence and apprehension of terrorists prior to boarding aircraft): Intelligence, International Partnerships, Customs and border protection, Joint terrorism task force, No-fly list and passenger pre-screening, Crew vetting, Visible Intermodal Protection Response (VIPR) Teams, Canines, Behavioral detection officers, Travel document checker, Checkpoint/transportation security officers, Checked baggage, Transportation security inspectors, Random employee screening, and Bomb appraisal officers. The remaining six layers of security provide 'in-flight security': Federal Air Marshal Service, Federal Flight Deck Officers, Trained flight crew, Law enforcement officers, Hardened cockpit door, and Passengers.

The risk reduction (ΔR) is the additional risk reduction achieved by the presence of AITs when compared to the overall risk reductions achieved by the presence, absence and/or effectiveness of all other security measures. If a combination of security measures will foil every threat then the sum of risk reductions is 100%. This soon becomes a multidimensional decision problem with many possible interactions between security measures, threat scenarios, threat probabilities, risk reduction and losses. Fault and event trees and logic diagrams, together with systems engineering and reliability approaches, will aid in assessing these and other complex interactions. This is the approach used herein.

We start assessing risk reduction by developing a simple systems model of new (AITs) and existing aviation security measures. For a suicide bomber to succeed in downing a commercial airliner requires that all stages of the planning, recruiting and implementation of the plot go undetected. We will focus on three steps linked to aviation security:

1. success in boarding aircraft undetected
2. success in detonating IED
3. location and size of IED is sufficiently powerful to down the aircraft

The security measures in-place to foil, deter or disrupt these three steps are:

1. success in boarding aircraft undetected - 10 layers of security: intelligence, international partnerships, customs and border protection, joint terrorism

task force, no-fly list and passenger pre-screening, behavioral detection officer, travel document checker, checkpoint/transportation security officers (TSO), transportation security inspectors, bomb appraisal officers
2. success in detonating IED - trained flight crew and passengers
3. location and size of IED is sufficiently powerful to down the aircraft - aircraft resilience

If any one of these security measures are effective, or the capabilities of the terrorist are lacking, then the terrorist will not be successful. We do not include all 'layers' of TSA security such as checked baggage or canines, only those likely to stop a suicide bomber. Note that air marshals, hardened cockpit door, armed flight crew, and on-board law enforcement officers are designed to protect against hijackings or replication of a 9/11 style attack. Moreover, air marshals are on less than 10% of aircraft and so are unlikely to be deter, foil or disrupt a suicide bomber (Stewart and Mueller 2008).

Figure 2 shows a reliability block diagram used to represent the system of foiling, deterring or disrupting an IED terrorist attack on a commercial airplane. If a terrorist attack is foiled by any one of these layers of security, then this is viewed as a series system. Assume:

- Probability that a terrorist is successful in avoiding detection by any one of the 10 layers of pre-boarding TSA security is a high 90%.
- Passengers and trained flight crew have a low 50/50 chance of foiling a terrorist attempting to assemble or detonate an IED.
- Imperfect bomb-making training results in high 75% chance of IED detonating successfully.
- Aircraft resilience - a 75% chance of an airliner crashing if a bomb is successfully detonated.

Since there are uncertainties with quantifying these probabilities a sensitivity analysis is conducted later in the paper to assess robustness of results. For a series system where each event probability is statistically independent the probability of airliner loss is

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

The probability then that the plot is foiled, deterred or disrupted is 1-Pr(airline loss)=90.2% assuming existing security measures. Now, if the additional security measure is AITs, then we assume:

- The probability of this technology in preventing a suicide bomber boarding an aircraft is five times higher than any existing layer of TSA pre-boarding security - i.e., 50%.
- The probability of this technology in preventing a suicide bomber from successfully detonating an IED is 50% because AITs may deter a terrorist from using more reliable, but more detectable, detonator.
- The probability of this technology in preventing an IED from being sufficiently large to down the aircraft is 50%.

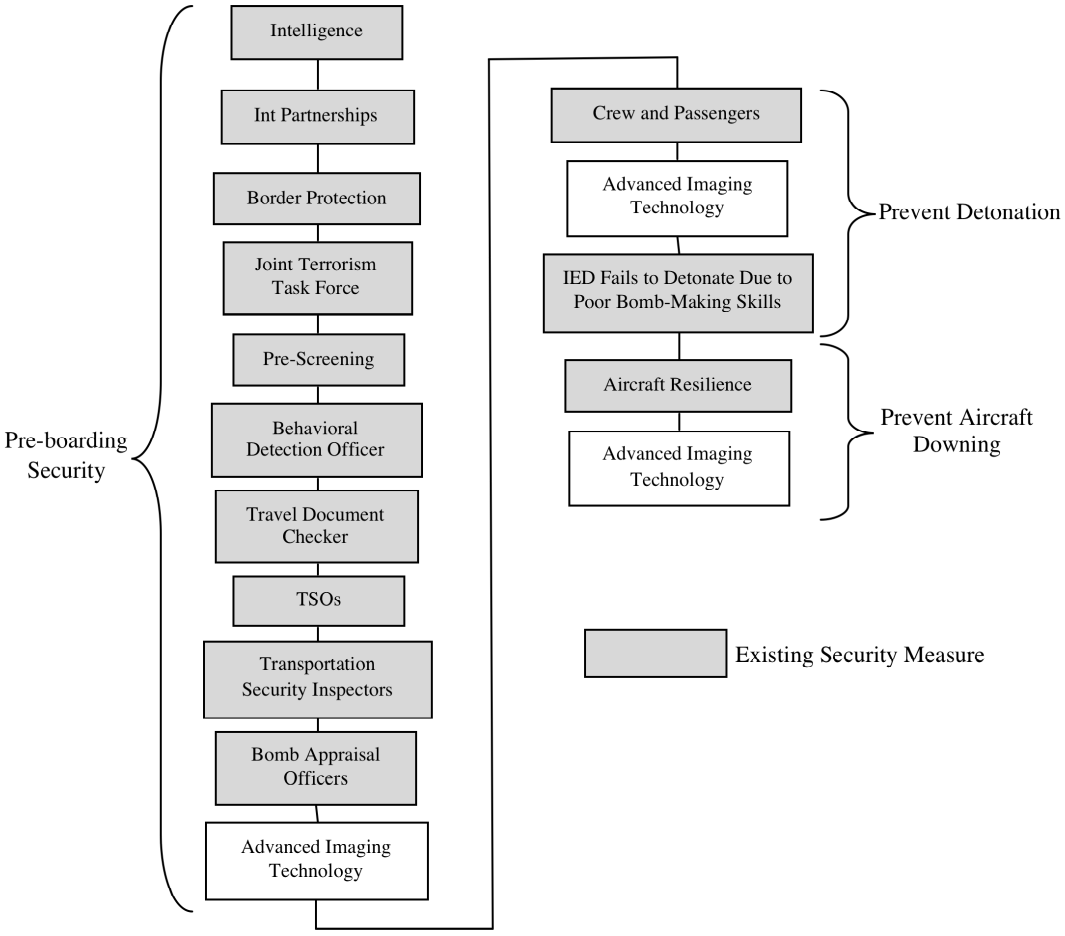

Figure 2. Reliability Block Diagram of Existing (shaded) and Enhanced Aviation Security Measures With Advanced Imaging Technology (AIT).

Again assuming a series system, and since Pr(AIT effectiveness) is 50%, the probability that a terrorist plot will not be foiled, disrupted or deterred by AITs is $[1\text{-Pr(AIT effectiveness)}]^3=(1-0.5)^3=12.5\%$ and so probability of airliner loss is now calculated as $9.8\%\times12.5\%=1.2\%$. 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 [Pr(AIT effectiveness)=20%], then risk reduction is reduced to 4.8%. Lower and upper bound risk reductions is thus taken as 5% and 10%, respectively. We will also assume three alternate probability distributions of risk reduction (see Figure 3):

1. Normal Distribution - risk reduction is normally distributed with 95% confidence interval between 5% and 10%, then mean risk reduction is 7.5% and standard deviation is 1.3%.
2. Uniform Distribution - equal likelihood of any risk reduction between 5% and 10%, with mean risk reduction of 7.5%.
3. Triangular Distribution - higher likelihood of higher risk reduction bounded by 5% and 10%, with mean risk reduction of 8.3%.

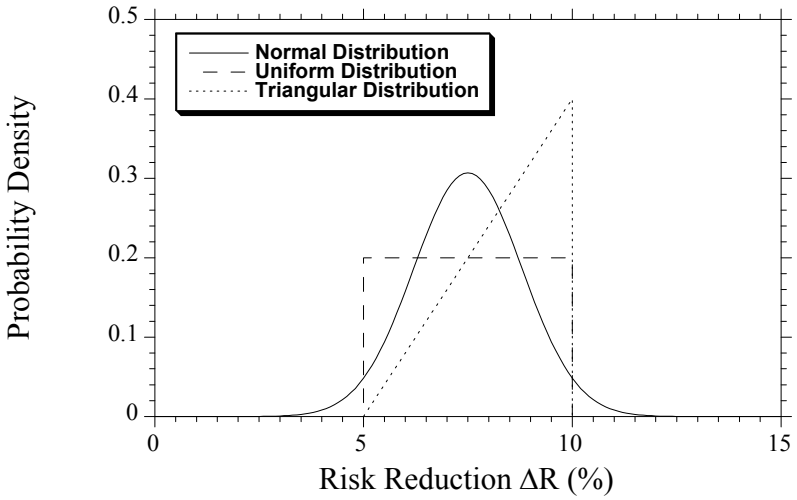

Figure 3. Alternative Risk Reduction Uncertainty Models.

Results

An expected value cost-benefit analysis is one that uses mean values. In this case, the minimum attack probability for full body scanners to be cost-effective is 61.5% per year calculated as $1.2 billion divided by $26 billion in losses divided by 7.5% risk reduction. Thus, full body scanners must deter or foil more than one otherwise successful attack every two years for the security measure to be deemed cost-effective. However, this type of cost-benefit analysis fails to consider the uncertainty of losses and risk reduction - this is now described in the following section. Note that the attack probability is the probability of an attack that originates in the U.S. and the bomber boards an aircraft in the U.S. and not elsewhere. This is an important distinction as the shoe and underwear bombers boarded their aircraft at international locations and not in the U.S.

Uncertainty Analysis

Monte-Carlo simulation analysis is used as the computational tool to propagate uncertainties through the cost-benefit analysis. The analysis assumes that losses and risk reductions are either normally, uniformly or triangularly distributed. If inputs are random variables then the output of the analysis (net benefit) will also be variable and so the probability that net benefit exceeds zero, Pr(cost-effectiveness), can be calculated for any attack probability. Figure 4 shows the probability of cost-effectiveness for attack probabilities from 0.1% to 1,000%. If attack probability is less than 20% per year then there is zero likelihood that AITs are cost-effective and so 100% likelihood of a net loss. On the other hand, if

attack probabilities exceed 1,000% or ten attacks per year then AITs are certain to be cost-effective (i.e. Pr(cost-effective)=100%). Clearly, as attack probability decreases then benefit reduces thus reducing net benefit.

The decision problem can be recast another way. In a break-even analysis, the minimum attack probability for AITs to be cost effective is selected such that there is 50% probability that benefits equal cost (see Table 1). However, a decision-maker may wish the likelihood of cost-effectiveness to be higher before investing billions of dollars in a security measure - to say 90% so there is more certainty about a net benefit and small likelihood of a net loss. Table 1 shows the minimum attack probabilities needed for there to be a 90% chance that AITs are cost-effective. For all three uncertainty models, the attack probability needs to exceed 160-330% per year to be near certain that AITs are cost-effective. This means that there is 90% confidence that AITs will pass a cost-benefit analysis if the mean rate of attack is two to three attacks per year originating from U.S. airports. Conversely, Table 1 shows that if attack probability is less than 34-41% per year then there is only a 10% chance of a net benefit, and a 90% likelihood of a net loss. The results are not overly sensitive to the probabilistic models used.

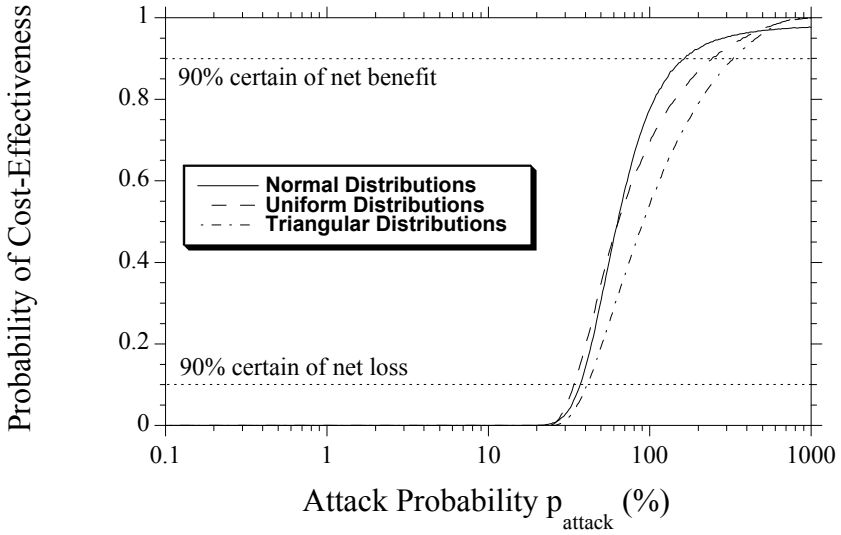

Figure 4. Probability of Cost-Effectiveness (Net Benefit Exceeds Zero).

Table 1. Minimum Attack Probability for AITs to be Cost-Effective.

Loss and Risk Reduction Distributions	Pr(cost-effective)=10%	Pr(cost-effective)=50%	Pr(cost-effective)=90%
Normal	37.2%	63.2%	161.8%[1]
Uniform	34.0%	63.9%	247.7%
Triangular	41.0%	91.2%	330.4%

[1] 1.62 attacks per year

Sensitivity Analysis

While we have tried to err on the generous side - i.e. towards improving the cost-effectiveness of full-body scanners - we recognize that the probability estimates for effectiveness of security measures are uncertain. If the effectiveness of pre-boarding security is reduced, then the additional risk reduction of AITs increases. Hence, assume that effectiveness of pre-boarding security measures is half of those used above (i.e. probability of avoiding detection increases from 90% to 95%), and (ii) effectiveness of AITs increases from 50% to 75% due to, for example, a higher deterrent capability. Then Pr(airliner loss) is 16.8% and 0.3% for existing and enhanced security measures, respectively. The risk reduction is ΔR=16.5%. If AITs are 100% effective then they reduce existing risk to zero and so ΔR=16.8%. Or if we assume that Pr(successful IED detonation) increases from 75% to 100% due to highly skilled and experienced terrorists, then risk reduction is ΔR=11.5%. If we modify the three alternative uncertainty models of risk reduction so that their range is 5-20%, then the attack probability needs to exceed 115-192% for there to be 90% confidence that AITs are cost-effective. A break-even analysis shows that the attack probability needs to exceed 39-53% for AITs to be cost-effective. However, if opportunity costs are considered then this would increase the threshold attack probabilities.

If the lower bound of loss is increased to $5 billion, then the attack probability needs to exceed 131-201% for there to be 90% confidence that AITs are cost-effective. If the upper bound of loss is doubled to C_{loss}=$100 billion, then the attack probability needs to exceed 89-209% for there to be 90% confidence that AITs are cost-effective. While doubling risk reduction or losses reduces threshold attack probabilities, they still remain at relatively high levels.

Discussion

The present paper has shown the utility of systems and uncertainty modeling for cost-benefit analysis for homeland security expenditure. The preliminary results suggest that the threat probability - the likelihood an attack will be otherwise successful - needs to be high for AITs to be cost-effective. But we recognize that

the preliminary cost-benefit analysis conducted herein will not give a definitive answer to whether AITs are cost-effective. A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in aviation security. This paper provides a starting point for this type of analysis. The assumptions and quantifications made here can be queried, and alternate hypotheses can be tested in a manner which over time will minimize subjectivity and parameter uncertainty inherent in an analysis for which there are little accurate data. This should lead to more widespread understanding and agreement about the relative cost-effectiveness of aviation security measures.

CONCLUSIONS

The paper has developed a preliminary cost-benefit analysis of Advanced Imaging Technologies (AITs) using full-body scanners for passenger screening at U.S. airports. The analysis considered threat probability, risk reduction, losses, and security costs. Monte-Carlo simulation methods were used to propagate risk reduction and loss uncertainties in the calculation of net benefits, and the minimum attack probability necessary for full-body scanners to be cost-effective were inferred. It was found that, based on mean results, more than one attack every two years would need to originate from U.S. airports for AITs to pass a cost-benefit analysis. The uncertainty modeling also allowed the probability of cost-effectiveness to be calculated. It was found that the attack probability needs to exceed 160-330% per year to be 90% certain that AITs are cost-effective.

REFERENCES

Bayles, F. (1996), 'Planes Don't Blow Up' Aviation Experts Assert, *International Herald Tribune*, July 24, 1996.

BBC News (2010), Boeing 747 Survives Simulated 'Flight 253' Bomb Blast, 5 March 2010.

Blalock, G., Kadiyali, V. and Simon, D.H. (2007), The Impact of Post-9/11 Airport Security Measures on the Demand for Air Travel, *Journal of Law and Economics*, 50(4): 731-55.

Blomberg, S.B. and Rose, A.Z. (2009), Editor's Introduction to the Economic Impacts of the September 11, 2001, Terrorist Attacks, *Peace Economics, Peace Science, and Public Policy*, May 2009, 15(2):1-14.

Chow, J, Chiesa, J., Dreyer, P., Eisman, M., Karasik, T.W., Kvitky, J., Lingel, S., Ochmanek, D. and Shirley, C. (2005), *Protecting Commercial Aviation Against the Shoulder-Fired Missile Threat*, RAND, Santa Barbara, 2005.

Cox, L.A. (2009), Improving Risk-Based Decision-Making for Terrorism Applications, *Risk Analysis*, 29(3): 336-341.

Dillon, R.L., Liebe, R. and Bestafka, T. (2009), Risk-based Decision Making for Terrorism Applications, *Risk Analysis*, 29(3): 321-335.

Ellig, J., Guiora, A, and McKenzie, K. (2006), *A Framework for Evaluating Counterterrorism Regulations*, Policy Resource No. 3, Mercatus Center, George Mason University, September 2006.

Ellingwood, B.R. (2006), Mitigating Risk from Abnormal Loads and Progressive Collapse, *Journal of Performance of Constructed Facilities*, 20(4), 315-323.

Enders, W. and Olsen, E. (2011), Measuring the Economic Costs of Terrorism, In M. Garfinkel and S. Skaperdas eds. *Oxford Handbook of the Economics of Peace and Conflict,* Forthcoming.

Europol (2009), *The Concealment of Improvised Explosive Devices (IEDs) in Rectal Cavaties*, Europol, The Hague, 18 September 2009, p.8

Farrow, S. and Shapiro, S. (2009), The Benefit-Cost Analysis of Security Focused Regulations, *Journal of Homeland Security and Emergency Management*, 6(1):Article 25.

Freidman, B.H. (2010), Managing Fear: the Politics of Homeland Security, in *Terrorizing ourselves: why U.S. counterterrorism policy is failing and how to fix it*, B.H. Friedman, J. Harper, and C.A. Preble (Eds.), Cato Institute, p. 211.

Gordon, P., Moore II J.E., Pak, J.Y. and Richardson, H.W. (2007), The Economic Impacts of a Terrorist Attack on the U.S. Commercial Aviation System, *Risk Analysis*, 27(3): 505-512.

Halsey, A. (2010), All check-points wont get body scanners, *The Washington Post*, December 2, 2010.

Kenney, M. (2010), "Dumb" yet Deadly: Local Knowledge and Poor Tradecraft among Islamist Militants in Britain and Spain, *Studies in Conflict and Terrorism*, 31:1-22.

Lord, S. (2010), *Aviation Security: TSA is Increasing Procurement and Deployment of the Advanced Imaging Technology, but Challenges to this Effort and Areas of Aviation Security Remain*, United States Government Accountability Office, GAO-10-484T, March 17 2010, p.5

Mueller, J. (2010), Assessing Measures Designed o Protect the Homeland, *Policy Studies Journal*, 38(1), 1-21, February.

Mueller, J. and Stewart, M.G. (2011), *Terror, Security and Money: Balancing the Risks, Benefits and Costs of Homeland Security*, Oxford University Press, October 2011.

NRC (2010), *Review of the Department of Homeland Security's Approach to Risk Analysis*, National Research Council, National Academic Press, Washington.

OMB (1992), *Guidelines and Discount Rates for Benefit-Cost Analysis of Federal Programs (Revised)*, Circular No. A-94, October 29, 1992, Office of Management and Budget, Washington, DC.

Poole, R.W. (2008), *Towards Risk-Based Aviation Security Policy*, Discussion Paper No. 2008-23, OECD/ITF Round Table on Security, Risk Perception and Cost-Benefit Analysis, International Transport Forum, December 2008.

Robinson, L.A., Hammitt, J.K., Aldy, J.E., Krupnick, A. and Baxter, J. (2010), Valuing the Risk of Death from Terrorist Attacks, *Journal of Homeland Security and Emergency Management,* 7(1).

Rossides G. (2010), Advanced Imagining Technology - Yes, It's Worth It, *The Blog@Homeland Security*, April 1 2010.

Stewart, M.G., Netherton, M.D. and Rosowsky, D.V. (2006), Terrorism Risks and Blast Damage to Built Infrastructure, *Natural Hazards Review* 7(3):114-122.

Stewart, M.G. and Netherton, M.D. (2008), Security Risks and Probabilistic Risk Assessment of Glazing Subject to Explosive Blast Loading, *Reliability Engineering and System Safety*, 93(4): 627-638.

Stewart, M.G. (2008), Cost-Effectiveness of Risk Mitigation Strategies For Protection of Buildings Against Terrorist Attack, *Journal of Performance of Constructed Facilities*, ASCE, 22(2):115-120.

Stewart, M.G. and Mueller, J. (2008), A Risk and Cost-Benefit Assessment of U.S. Aviation Security Measures, *J. of Transportation Security*, 1(3):143-159.

Stewart, M.G. (2010), Risk-Informed Decision Support for Assessing the Costs and Benefits of Counter-Terrorism Protective Measures for Infrastructure, *International Journal of Critical Infrastructure Protection*, 3(1): 29-40.

Stewart, M.G. (2011), Life Safety Risks and Optimisation of Protective Measures Against Terrorist Threats to Infrastructure, *Structure and Infrastructure Engineering,* 7(6): 431-440.

Sunstein. C.R. (2002), *The Cost-Benefit State: The Future of Regulatory Protection*, ABA Publishing, American Bar Association, Chicago.

TSA (2010), Passenger Screening Program: Program Specific Recovery Act Plan May 24 2010, Department of Homeland Security, Washington, DC, p.3

Willis, H. and LaTourette, T. (2008), Using Probabilistic Terrorism Risk-Modeling for Regulatory Benefit-Cost Analysis: Application to the Western Hemisphere Travel Initiative in the Land Environment*, Risk Analysis* 28:325.

von Winterfeldt, D. and O'Sullivan, T.M. (2006), Should WE Protect Commercial Airplanes Against Surface-to-Air Missile Attacks by Terrorists?, *Decision Analysis*, 3(2): 63-75.