J Transp Secur
DOI 10.1007/s12198-016-0175-0

Risk and economic assessment of expedited passenger screening and TSA PreCheck

Mark G. Stewart[1] **· John Mueller**[2,3]

Received: 25 August 2016 / Accepted: 14 November 2016

Abstract The Transportation Security Administration's PreCheck program allows airline passengers assessed as low risk to be directed to faster screening lanes. The paper assesses the scenario of a terrorist plot to down an airliner with a passenger-borne bomb. There are four main conclusions. First, we find that the layered system currently in place reduces the risk of such an attack by 98% - and probably by quite a bit more. Second, this level of risk reduction is very robust: security remains high even when the parameters that make it up are varied considerably. In particular, because of the large array of other security layers, overall risk reduction is relatively insensitive to how effective checkpoint screening is. Third, under most realistic combinations of parameter values PreCheck actually *increases* risk reduction, perhaps up to 1%, while under the worst assumptions, it lowers risk reduction by some 0.3%. Fourth, the co-benefits of the PreCheck program are very substantial: by greatly reducing checkpoint costs and by improving the passenger experience, this benefit can exceed several billion dollars per year. We also find that adding random exclusion and managed inclusion to the PreCheck program has little effect on the program's risk reducing capability one way or the other. TSA PreCheck thus seems likely to bring efficiencies to the screening process and great benefits to passengers, airports, and airlines while actually enhancing security.

Keywords Aviation security · Terrorism · PreCheck · Risk · Cost-benefit analysis · Passenger screening · Airports

✉ Mark G. Stewart
mark.stewart@newcastle.edu.au

John Mueller
bbbb@osu.edu

1 Centre for Infrastructure Performance and Reliability, The University of Newcastle, Callaghan, New South Wales 2308, Australia

2 Mershon Center for International Security Studies, Department of Political Science, Ohio State University, 1501 Neil Avenue, Columbus, OH 43201, USA

3 Cato Institute, 1000 Massachusetts Avenue, NW, Washington, DC 20001, USA

Introduction

In 2011 the Transportation Security Administration began its PreCheck program (or TSA Pre ✓®) that allows expedited screening for passengers deemed to be of low risk. Such passengers are selected from passenger information assessed through the TSA Secure Flight program. They may also qualify either directly through the TSA's PreCheck application program, or through the Global Entry or trusted traveller programs of the U.S. Customs and Border Protection (Fletcher 2015). Selected passengers do not need to take off belts, shoes, or jackets, nor do they need to remove liquids and laptops from their carry-on luggage. In addition, they are not required to undergo full-body screening.

Each PreCheck lane provides "the capability for doubling hourly throughput" (TSA 2014). Owing to this impressive efficiency gain, TSA expected the number of screeners to decline by nearly 1700 and screening costs to be reduced by $110 million in FY2016 (DHS 2016). PreCheck seems to be one of the few TSA programs that is risk-based - or at least it is one that is determined by screening passengers on the basis of risk. The goal of PreCheck is to allow screeners to concentrate more effort on passengers who might present a higher risk.

This is a worthy initiative. It recognises that aviation security can be improved by focussing on high-risk passengers (Price and Forrest 2013; Wong and Brooks 2015; Gillen and Morrison 2015), and it does not treat all passengers as if each poses an equal threat. This allows for more efficient and faster screening thus reducing opportunity costs that deters travellers from flying, causes them to miss flights, or induces them to take a more dangerous means, the automobile, to get to their destination.

The potential problem for PreCheck, however, is that, because it applies screening measures that are, or appear to be, more lax to a substantial portion of passengers, it might increase the likelihood that a terrorist plotting to bring down an airliner would pass through screening undetected. However, even though this program might, in some sense, be seen to make us less safe, it appears to have generated no opposition, and it is often viewed as a "significant success story for TSA" (Beckner 2015). Indeed, if it has generated any clamour among the public, it has come from those who are anxious to sign up.

In 2015, 45% of all passengers went through the PreCheck lines (TSA 2016). This was achieved not only by including those who had signed up for the program, but also by sending all members of the military there and by using "managed inclusions" in which people in regular screening lines are sent to join the PreCheck lanes by Behavioral Detection Officers (BDOs) or after undergoing explosive testing. However, a 2014 report noted that managed inclusion had not been tested by the TSA for overall security effectiveness and that the program was often used simply to speed up security lines (GAO 2014, 2015). Accordingly, in September 2015, the TSA discontinued managed inclusion based on BDO or explosive trace detector sampling, allowing managed inclusion only for passengers who are pre-screened by TSA canines (Aratani 2015). TSA recognises that "random and unpredictable security measures are needed to prevent terrorists from 'gaming the system'" (Price and Forrest 2013). To mitigate these risks, TSA uses a random exclusion process that routes a certain percentage of PreCheck passengers into regular lines (GAO 2014). For more details on TSA PreCheck see GAO (2014, 2015).

In our first studies, we assessed various security layers designed to prevent another airliner hijacking, finding that the U.S. Federal Air Marshal Service (FAMS) fails to be cost-effective, but that hardening cockpit doors does prove to be cost-effective (Stewart and Mueller 2008; Mueller and Stewart 2011). We have also conducted a systems reliability analysis and a detailed cost-benefit assessment of Advanced Imaging Technologies (AIT) - full-body scanners that inspect a passenger's body for concealed weapons, explosives, and other prohibited items – finding the technology to be a questionable expense (Stewart and Mueller 2011). We then developed a systems reliability model for aviation security using single point estimates of risk reduction and losses, and applying a risk-neutral decision analysis, finding Installed Physical Secondary Barriers (IPSB) and the Federal Flight Deck Officer (FFDO) program to be highly cost-effective (Stewart and Mueller 2013a). This work was then considerably extended by applying utility theory to quantify levels of risk aversion finding that FAMS would need to foil 2.6 otherwise successful attacks per year to be 90% sure that the program is cost-effective and that a very risk averse decision-maker is 48% likely to prefer to retain the expensive FAMS program even if the attack probability is as low as 1% per year - a very high level of risk aversion that is exhibited by few, if any, other government agencies (Stewart and Mueller 2013b; see also Stewart et al. 2011). We have also assessed the risks and cost-effectiveness of airport policing, measures to protect airport terminals, and the counter-terrorism efforts of the Federal Bureau of Investigation (Stewart and Mueller 2014a, 2014b; Mueller and Stewart 2014, 2016a).

There is other research that looks at the risks and efficiencies of aviation security, such as Jackson and LaTourette (2015), Sewell et al. 2013, Jackson et al. (2012a, b), Lee and Jacobson (2011), McLay et al. (2010), Jacobson et al. (2006), Morral et al. (2012), Martonosi and Barnett (2006), von Winterfeldt and O'Sullivan (2006), Willis and LaTourette (2008), and Poole (2008). Few of these studies, however, take our approach of estimating absolute risk and risk reduction. A key component of assessing absolute risk is to include the probability of an attack in the calculations. A relative risk assessment, in contrast, is often conducted conditional on an attack occurring and then ranking risks based on the relative likelihood of threats.

We have also undertaken a preliminary risk assessment of the PreCheck program (Stewart and Mueller 2015). It uses results from an earlier study (Stewart and Mueller 2013a) to estimate risk reduction from existing security measures to deter or disrupt a 9/11 type hijacking.[1] This paper is more comprehensive in that it models all layers of existing security that might deter or disrupt a terrorist plot (including policing), in that it assumes that the accuracy of TSA's Secure Flight program may be less than 100% when identifying low and high risk passengers, in that it assesses the effect of enhanced and expedited (or regular and PreCheck) screening on deterrence and disruption rates, and in that it evaluates random exclusion and managed inclusion programs. Instead of dealing with hijacking, we assess the more likely threat presented by terrorists who seek to detonate a passenger borne IED (Improvised Explosive Device) to bring down an

[1] It assumed that the deterrence and disruption rates for PreCheck screening would be reduced by half and that the effectiveness of enhanced screening would be increased by 50%. It found that under these conditions there is an overall decrease in risk reduction of 0.1% when PreCheck passengers are selected randomly and an overall benefit (increase of risk reduction) of 0.5% if PreCheck makes no mistakes in selecting the risk profile of passengers. These results are similar to another study (Jackson et al. 2012), in which it was found that the Trusted Traveller program seemed to be cost-effective.

airliner (Price and Forrest 2013). Finally, we expand and update earlier work (Stewart and Mueller 2015) to better estimate the economic benefits (or co-benefits) that PreCheck may engender in passenger satisfaction and increased airline revenues. Our risk analysis assumes that the bomber boards in the United States unlike the shoe and underwear bombers who boarded their U.S.-bound aircraft abroad. The methodology and findings of this paper are also relevant to risk-based passenger screening programs that are currently being developed by other countries - such as the International Air Transport Association and Airports Council International "Smart Security" initiative (IATA 2013).

The risk framework

The standard definition of risk used by the Department of Homeland Security is:

$$(\text{Risk}) = (\text{Threat}) \times (\text{Vulnerability}) \times (\text{Consequence}) \tag{1}$$

where

- Threat is the annual probability of a terrorist attempt
- Vulnerability is the probability of loss given the attempt
- Consequence is the loss if the attack is successful.

Equation (1) can be simplified to deal with successful attacks - ones that actually do damage:

$$\text{Risk} = p_{\text{attack}} \times \text{Loss} \tag{2}$$

where p_{attack} is the yearly average probability that a terrorist attack would successfully down the airliner if there are no security measures in place at all and that the attack originates at a U.S. airport. Loss is the consequences of that successful attack.

The benefit of TSA PreCheck is

$$\text{PreCheck Benefit} = p_{\text{attack}} \times \text{Loss} \times \Delta R \tag{3}$$

where ΔR is the additional risk reduction generated by PreCheck. Like almost all airline security measures, PreCheck reduces risk by lowering the likelihood of a successful attack (p_{attack}). It does not reduce the consequences (Loss) of a successful attack.

A security measure may not only reduce the terrorism risk but also supply a "co-benefit." In the case of PreCheck, this could come from improving the passenger experience or from reducing screening costs. The full benefit, then, would include any co-benefits as well as any achieved by risk reduction.

We favour a risk-neutral approach to decision-making as strongly recommended by the U.S. Office of Management and Budget and other regulatory agencies (OMB 1992; see also Sunstein 2002). This entails using mean or average estimates for risk and cost-benefit calculations, and not worst-case or pessimistic estimates. However, we recognise that public policy decision-making for low probability - high consequence events is often characterised by risk-aversion (e.g., Cha and Ellingwood 2012). Utility theory can be used to factor risk aversion into the decision process (e.g., Stewart et al. 2011; Stewart and Mueller 2013b).

Risk reduction of existing aviation security without PreCheck

Layers of aviation security

TSA has arrayed 21 "Layers of Security" to "strengthen security through a layered approach" (TSA 2012). This is designed to provide defence-in-depth protection to the travelling public and to the American transportation system.

Of these 21 layers, 15 involve pre-boarding security - layers that seek to deter terrorists from attempting attacks on aircraft or to disrupt them before they board the aircraft. One of these, inspection of checked baggage, is irrelevant to the threat presented by passenger-borne bombs. The remaining 14 are:

1. Intelligence
2. International Partnerships
3. Customs and Border Protection
4. Joint terrorism task force (JTTF)
5. No-fly list and passenger pre-screening
6. Crew vetting
7. Visible Intermodal Protection Response (VIPR) Teams
8. Canines
9. Behavioral detection officers (BDOs)
10. Travel document checker
11. Checkpoint/transportation security officers
12. Transportation security inspectors
13. Random employee screening
14. Bomb appraisal officers

TSA's remaining six layers provide security designed to deter or disrupt a terrorist attempt after boarding. Two of these, the training of the flight crew in the Federal Flight Deck Officers (FFDO) program and the hardened cockpit door are irrelevant to the threat presented by passenger-borne bombs. The remaining four are:

15. Federal Air Marshal Service (FAMS)
16. Trained flight crew
17. Law enforcement officers
18. Passengers

We also add two other layers that may deter or disrupt the success of an effort to down an airliner with a passenger-borne bomb:

19. IED is defective
20. The aircraft may survive even if the bomb is successfully detonated

We separate these 20 layers of aviation security into three stages (see also Fig. 1). However, although we have a full model of the process, we do not directly include one other impediment to a successful attack: the general incompetence and poor tradecraft of most terrorists, particularly in complicated plots (Kenney 2010, Mueller and Stewart 2012, Mueller 2016, Aaronson 2013, Mueller and Stewart 2016a).

Stage 1. Terrorists are deterred from attempting an attack

There are many reasons a terrorist contemplating an IED attack on an airliner will be deterred. In addition to concerns about specific security measures in the array above which we will use in this analysis, the terrorist might be deterred by other concerns: for example, by an unwillingness to commit suicide. In addition, the belief that a terrorist attack, particularly one on civilians, will be counterproductive to the cause is likely a major deterrent and helps to explain why terrorism is generally such a rare phenomenon (Abrahms 2006, 2011; Mueller and Stewart 2011, 2016a, b).

Stage 2. Terrorists attempt an attack, but are prevented from boarding

There is a considerably array of security measures that are specifically designed to prevent a terrorist from boarding. These include all those numbered 1 to 14 in the list above.

Stage 3. Terrorists succeed in boarding, but fail to bring down the airliner

One reason for the extent of the losses on 9/11 was the lack of *passenger resistance* and of a *trained flight crew* (16 and 18 in the list) to deal with terrorist attacks. However, that policy was obviously shattered by the experience as demonstrated on the fourth plane in which passengers and crew, having learned of what had happened on the earlier flights, fought to overcome the hijackers (Mueller and Stewart 2016a). Beyond hijacking, passenger and crew reactions were also effective in subduing the shoe bomber of 2001 and the underwear bomber of 2009. However, two Russian airliners were blown up by suicidal Chechen female terrorists in

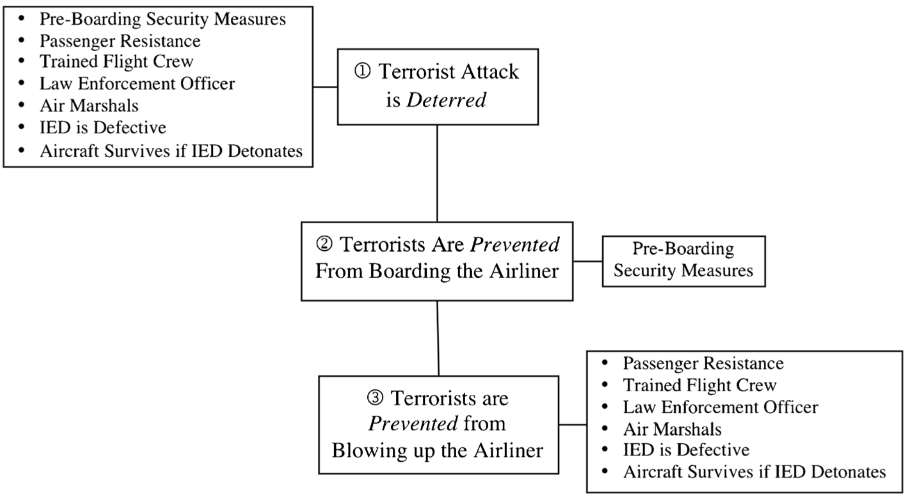

Fig. 1 Overall system model of aviation security measures

> 2004, and in 2016 an IED hidden in a laptop blew a hole in a Somali airliner (although the plane was not downed). Thus, passengers and crew may not always be able to prevent an IED from detonating successfully.

Law enforcement officers (17 on the list) are on some flights for reasons other than countering terrorism, such as escorting prisoners or protecting VIPs. However, their numbers are small and their impact on security is also likely to be low.

There are now some 2500 to 4000 *air marshals*, 15 in the list above (Elias 2009).[2] It has been estimated that air marshals ride on less than 5% of flights in the United States (Elias 2009). Although these are deemed to be high-risk flights based on intelligence reports, it is unclear exactly how that risk has been determined – after all, since 9/11 no airline flight in the U.S. has had an active terrorist on board. The potential presence of air marshals may well have a deterrent effect (Poole 2015). And, although the original intent of the program was to protect the cockpit from forced intrusions, an air marshal may be able to help defuse an IED or relocate it to a section of the aircraft where it is less likely to cause terminal damage. However, the air marshals' added value over crew and passenger resistance is likely to be rather small because they are present on only a rather small number of flights and because they are likely to be seated far from any potential bomber.

It may also prove to be the case that the *IED is defective* (19 on the list). In principle, an improvised explosive device, or IED, is relatively simple to design and manufacture if done by well-trained personnel resulting in reliabilities in excess of 90% (Grant and Stewart 2012). However, analysis of the Global Terrorism Database shows that the probability that a terrorist IED used in a Western country will prove defective and will fail to inflict damage is 81% because there is less opportunity for IED operational skills to be acquired. The general figure across all IED attacks (of all sizes) for the U.S. is even higher: 85%. By contrast, the probability that a terrorist or insurgent IED attack will be successful is more than three times higher in the Middle East (Grant and Stewart 2015). Kip Hawley, a former director of TSA, notes that even world-class laboratories are able to get the explosive mixture right only one time in three when making hydrogen peroxide bombs (Hawley and Means 2012). PETN does have a long history of use in terrorist attacks. However, 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 to detonate the PETN. However, this adds to the difficulty (Walsh 2009), and may help explain why no terrorist has been able successfully to detonate a bomb of that sort in the United States since 2001, and why, except for the four bombs set off in London in 2005, neither has any in the United Kingdom. The challenges faced in crafting an IED that is small enough to evade detection at airport checkpoints, but large enough to severely damage an airliner, are daunting indeed.

Also relevant is the fact that *the aircraft may survive even if the bomb is successfully detonated* (20 on the list). As it happens, it is not necessarily easy to blow up an airliner. Airplanes are designed to be resilient to shock, and attentive passengers and airline personnel complicate the terrorists' task further. Apparently, the explosion over

[2] This is an especially expensive security layer. The FY2015 the budget for the Federal Air Marshal Service (FAMS) is approximately $790 million (GAO 2016). In addition, airlines are expected to provide free seats for air marshals and this costs them more than $200 million per year.

Lockerbie in 1988 was successful only because the suitcase bomb just happened to have been put in a 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 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. In 2008, an oxygen cylinder exploded on a Qantas flight from Hong Kong, blasting a six-foot hole in the fuselage. The plane suddenly depressurised, but the aircraft returned safely to Hong Kong. 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, but the plane was able to make an emergency landing in Honolulu (Mueller and Stewart 2011, 2016a). And in 2016 a suicide bomber sitting at a window seat detonated his IED on a Somali airliner, resulting in a 3 to 5 ft hole in the fuselage, and to the death of the perpetrator. According to one expert "The bomber knew precisely where to sit and how to place the device to maximize damage" (Kriel and Cruickshank 2016). However, the damage was not catastrophic apparently because the detonation occurred before the plane reached its cruising altitude - otherwise a more hazardous depressurisation might have occurred – and the plane landed safely. Aircraft, like other types of infrastructure, are more robust and resilient than we often give them credit for.

Calculation of risk reduction

We apply a reliability analysis to the overall system (e.g., Stewart and Melchers 1997). In this, the probability that an attempt to blow up an aircraft with an IED is deterred or disrupted will be equal to:

$$R = 1 - \left\{ \begin{array}{l} [1-\Pr(\text{deterred by pre-boarding measures})] \\ \times[1-\Pr(\text{deterred by in-flight measures})] \\ \times[1-\Pr(\text{disrupted by pre-boarding measures})] \\ \times[1-\Pr(\text{disrupted by in-flight measures})] \\ \times[1-Pr(\text{IED is defective and does not detonate})] \\ \times[1-\Pr(\text{aircraft survives if IED detonates})] \end{array} \right\} \quad (4)$$

For example, if each of the six probabilities in Eq. (4) is set at 50%, the overall risk reduction would a high $R = 98.4\%$. If other layers of security are added to the array, this risk reduction will be pushed even higher, but the additional risk reduction of each layer (ΔR) will become progressively smaller.

Equation (4) is based on one threat scenario, whereas security measures are often designed to deal with a range of threats. A more detailed and comprehensive study is required to properly model the complex interactions and interdependencies in aviation security. For example, security measures may not be perfectly substitutional (i.e. independent of each other) – thus, removing one layer may alter the deterrence or detection rates of other layers (e.g., Stewart and Mueller 2013b). Nonetheless, Eq. (4) provides a basis for assessing the influence and sensitivity of policy options on risk reduction.

Estimating risk reductions

We use words of estimative probability, adapted from Fletcher (2011) as in Table 1. These are applied to single-point (mean) estimates of deterrence and disruption rates in Table 2. Since there is little quantitative data on these rates, it is more tractable to assign words such as "probably not" and "chances about even" when assessing the effectiveness of security measures and then translated them into probabilities following the designations in Table 1. Nearly all measures have some chance of being effective at least in extreme cases or in an unlikely combination of circumstances. We allocate deterrence or disruption rates at 1% for those measures we deem to make a negligible contribution to risk reduction. Others might be inclined to put these higher. A sensitivity analysis is conducted later to assess changes in risk reduction when these estimates of deterrence and disruption rates are changed. For the most part, these changes don't make much difference in the outcome.

We assess two scenarios: an effort by a lone wolf terrorist to bring down an airliner with an IED, and an effort by a terrorist organisation to do so.

Deterrence and disruption rates for pre-boarding security measures

In Table 2 we estimate separately the effectiveness of all 14 of the TSA's pre-boarding security layers as arrayed in the list above. Deterrence rates we think, are likely to be low for most of these layers with the exception of passenger checkpoint screening. Disruption rates for the pre-boarding layers are also modest, with the most effective being intelligence, the JTTF, FBI, police, and tip-offs which have been responsible for most foiled terrorist plots in the U.S. (Mueller and Stewart 2016a), and passenger screening at the TSA checkpoints. Although it has been contended that "canine programs have been one of the most consistently successful explosive detection programs in the history of aviation security" and that they constitute the "gold standard" in bomb detection (Price and Forrest 2013), they probably have a very modest effect on deterrence and disruption rates because of their relatively low numbers, and the same is likely to hold for bomb appraisal officers.

Table 1 Words of estimative probability (Fletcher 2011)

Certain	100%
Almost certain	95%
Highly probable	85%
Probable	75%
Chances about even	50%
Less likely than not	40%
Probably not	25%
Highly improbable	15%
Almost certainly not	5%
Impossible	0%

Table 2 Deterrence and disruption rates for existing aviation security measures

	Deterrence rate	Disruption rate	Notes
Pre-boarding:			
Intelligence	15%	15%	Insider threats beyond scope of paper
International partnerships	1%	5%	
Customs and border protection	1%	5%	
JTTF (including FBI and police)	15%	25%	
No-fly list & passenger pre-screening	5%	5%	
Crew vetting	0%	0%	
VIPR teams	1%	5%	
Canines	5%	5%	
Behavioral detection officers	1%	1%	
Travel document checkers	5%	5%	
Checkpoint/TSOs before PreCheck	50% Lone Wolf 25% Terrorist Organisation	50% Lone Wolf 25% Terrorist Organisation	Based on pre-2011 screening before TSA PreCheck. Metal detectors, X-ray machines and AITs will have high disruption rates for IED threats. Martonosi and Barnett (2006) suggest that pre-boarding security screening has a 50% detection rate. Fletcher (2011) suggests detection rate for explosives is 60–85%
Transportation security inspectors	1%	1%	
Random employee screening	0%	0%	Insider threats beyond scope of paper
Bomb appraisal officers	5%	5%	
In-flight:			
Passenger and crew resistance	15%	30%	May not be able to react in time
Law enforcement officer	1%	1%	Very low probability of being on a fligh
Air marshals	5%	-	Air marshals on a very low number of flights. May not be able to react in time
IED detonation prevented by air marshals if air marshals on board	5%		
Probability that air marshals are on-board	20%		FAMS are on no more than 5% of flights, but are placed on 'high risk' flights so assume 20% coverage
IED is defective and does not detonate	40%[a]	80%[b]	Lone Wolf or Self-Starter
	15%	35%[c]	Terrorist Organisation
Aircraft survives if IED detonates	0%	50%	Aircraft are resilient to small IEDs

[a] Likely to be deterred by the challenging task of acquiring bomb making materials, making the IED, testing the IED, and concerns that the IED will be defective

[b] Based on database of IED successes in Western countries

[c] Based on database of IED successes in Middle East and North Africa

Deterrence and disruption rates for In-flight security measures

As discussed above, passengers and flight crew may well be unable to prevent an IED from detonating successfully. An IED disruption rate of 30% is assigned for passengers and flight crew in total. Passengers in close proximity to a suicide bomber will be more effective in foiling a bombing event than an air marshal who would most likely be seated at some distance from the bomber. However, a low but non-negligible rate of deterrence (5%) is assumed for air marshals. The impact of law enforcement officers is likely to be negligible.

Deterrence and disruption rates for other post-boarding measures

We assume in Table 2 that the probability that an IED is defective and fails to detonate is 80%. This estimate is based on an analysis of the Global Terrorism Database (Grant and Stewart 2012, 2015). This is unlikely to be an over-estimate because, as noted, the likelihood that an IED of any size will fail to detonate in the U.S. is even higher: 85%. That might be even higher for a small IED fabricated in order to avoid detection by airport checkpoint screening technologies. This defect rate represents the average across Western countries where many terrorists are lone wolves or self-starters with little training or operational experience in explosives. A possible, albeit less likely, scenario concerns a perpetrator affiliated with a terrorist cell or network like ISIS or al-Qaeda, one who has access to bomb making materials and has had some substantial training. In this case, the probability of a failed detonation declines to 35% as is suggested by experience in the Middle East and North Africa (Grant and Stewart 2012). We use this figure in Table 2. This higher threat assumes, of course, that such terrorists are able to infiltrate themselves into the United States to board their flight. We also assume that a terrorist organisation is less likely to be deterred or disrupted by checkpoint security, leading to a lower deterrence and disruption rates of 25%. The analysis to follow considers both IED threat scenarios – attempts by lone wolves and by terrorist organisations.

Because of the daunting nature of the task and of the abysmal success rate, terrorists are also likely to be deterred from even attempting to acquire bomb making materials and to manufacture an IED. The rate of deterrence is assumed to be 40% for lone wolves and 15% for terrorist organisations.

Based on descriptions of aircraft bombings since 1960 (Baum 2016), there is approximately a 50–50 chance of an airliner surviving and landing safely in the event of a successful IED detonation in the cabin. We do not include the effect that aircraft resilience may have on deterrence because this is difficult to quantify and, in particular, because the attacker may well (mistakenly) believe aircraft to be highly vulnerable to a bombing.

Risk reduction for existing aviation security measures without PreCheck

Table 3 shows the results when a systems reliability analysis is applied in Eq. (4) to existing measures as outlined in Table 2 and as discussed in the previous section. Deterrence and disruption risk reductions separately supplied by pre- and post-boarding security measures are shown, as are those supplied by the entire array of security

Table 3 Risk reductions for existing security measures without PreCheck

	Lone wolf	Terrorist organisation
Deterrence by		
Pre-boarding security measures	72.0%	58.0%
Post-boarding measures	52.0%	32.0%
Total	86.6%	71.5%
Disruption by		
Pre-boarding security measures	78.2%	67.3%
Post-boarding measures	93.1%	77.7%
Total	98.5%	92.7%
Deterrence and disruption by		
Pre-boarding security measures	93.9%	86.3%
Post-boarding measures	96.7%	84.8%
Total risk reduction (R)	99.8%	97.9%

measures.[3] There is a total risk reduction of 99.8% for IED lone wolf attempts and 97.9% for IED attempts by terrorist organisations. This high number makes sense since there have been no successful terrorist attacks, or even attempts, on US airliners since 2001.

This result, which assumes that deterrence and disruption are statistically independent events that can be modelled as a series system, suggests that, because of existing security measures, even a well planned and executed terrorist attack has only about one chance in 50 of being successful. Any opportunity for risk reduction by additional measures (including PreCheck), then, is rather low.

We recognise that some terrorists may exhibit adaptive behaviour. Jackson and LaTourette (2015) have developed a set of adaptation strategies: substitute target or location, substitute tactic or attack mode, hide from or deceive defence, avoid defence at the target, attack defence directly, and absorb defence effects. Although our results suggest that airliners departing from U.S. airports are not very feasible targets for terrorists, they may have sought out other targets. However, the number of terrorist attempts of all kinds in the United States has been very low (Mueller 2016). We consider adaptive behaviour later in our analysis by considering changes in rates of deterrence and disruption. Due to the many layers of passenger and baggage screening, attackers could attempt to smuggle an IED on an aircraft through a baggage handler, catering employee, or other airport worker - although there hasn't been any evidence of that in the United States either. This consideration, however, is beyond the scope of the present paper.

Overall, the results of this model seem to be extremely robust: changing the deterrence or disruption rates in Table 2, often very substantially, scarcely alters the outcome. For example, if we assume that the only effective pre-boarding security measures are passenger checkpoint screening and the JTTF, total risk reduction goes

[3] The high level of risk reduction concurs with Fletcher (2011) who finds a high level of deterrence (92.5%) and slightly lower rate in the probability of detecting terrorists (85%).

down, but by less than 3%. If the probability that air marshals are on board is reduced from 20% to 5% (which is considerably more realistic), total risk reduction is essentially unchanged and is thus insensitive to the probability that an air marshal is on board. The rate of disruption by air marshals would need to increase four-fold to 20% before there is a noticeable increase in total risk reduction. If all the rates of deterrence as shown in Table 2 are halved, the total risk reduction goes down by less than 2%. In nearly all cases, and even when we reduce the effectiveness of deterrence or disruption of one or more layers by 50%, the total risk reduction ranges from 96% to 99% - that is, at worst, there remains less than one chance in 25 that a terrorist plot to down an airliner will be successful.

In additions, it should be pointed out that some, or even many, of the deterrence and disruption rates estimated in Table 2 might be too low. For example, passenger and crew reactions were effective in subduing the shoe bomber of 2001 and the underwear bomber of 2009, whereas our analysis estimates a disruption rate of only 30% If that rate is increased to 50%, total risk reduction increases to 99.9% and 98.5% for IED lone wolf and terrorist organisation attacks, respectively. Or if the disruption rate of the JTTF, FBI, police and tip-offs from the public is doubled to 50%, total risk reduction increases to 99.9% and 98.6% for IED lone wolf and terrorist organisation attacks, respectively Thus, our general conclusion that a terrorist's chance of success in attempting to blow one up with a bomb carried aboard is one in 50 may be quite generous. In line with such thinking, it might be pointed out that a statistical analysis of the Global Terrorism Database (2016) finds that the worldwide probability that an airline passenger will be killed on an individual flight by a terrorist is a miniscule 1 in 100 million for the years from 2002 through 2015.

Clearly, the level of risk reduction is very robust: security remains high even when the parameters that make it up are varied considerably. As a final example, if the effectiveness of checkpoint screening is reduced to only 5%, overall risk increases by less then 0.5%. Hence, because of the large array of other security layers, overall risk reduction is relatively insensitive to how effective checkpoint screening is, or to how effective any other security layer is. However, the presence of checkpoint screening may still be important given that it is the most visible security measure with an important deterrence function.

The risk reduction effects of adding TSA PreCheck

Risk reduction due to PreCheck

The risk reduction effects of adding PreCheck (ΔR) is

$$\Delta R = R_{\text{PreCheck}} - R \tag{5}$$

where R_{PreCheck} is the risk reduction from security measures with PreCheck and R is risk reduction from existing security measures without PreCheck given by Eq. (4).

The systems reliability analysis for the total risk reduction effects of aviation security measures that includes the deterrence and disruption features of TSA PreCheck is described in full by Stewart and Mueller (2016). A large number of input variables are required to model the effectiveness of PreCheck. Many of these will only be known to the TSA, so the following analysis is based on our best-estimates and is illustrative only. The variables known to be most sensitive to risk reduction will be identified later in a sensitivity analysis.

For our analysis, we make four assumptions.

1. To begin with, we assume that one out of every 100 million passengers is highly likely to be a terrorist. To arrive at that number, we assume that one out of every 100 million passengers has a threat likelihood one trillion times higher than the remaining 99,999,999 passengers. In practical terms, if 99,999,999 out of every 100 million passengers have a likelihood of being a terrorist that is close to zero, and if one attack is expected each year, the likelihood that a high risk passenger would be responsible for the attack is 99.99% (Stewart and Mueller 2016). Low risk passengers are defined as those who are in TSA PreCheck or those who, although not formally assessed, will pose a low risk. Our assumption that one passenger in 100 million is likely to be a terrorist is an exaggeration of the threat that terrorism presents to airliners under current conditions. After all, nearly 2 million passengers pass through checkpoints in the United States every day, or over 700 million per year (TSA 2016). Yet, no passenger has tried to smuggle an IED onto an airliner in the U.S. in more than 30 years.[4]
2. We further assume that 50% of all air travellers go through the PreCheck line.
3. We also assume that TSA's Secure Flight program is 99% accurate in correctly identifying low risk passengers, but is less accurate (90%) in correctly identifying high risk passengers.
4. Finally, we assume the deterrence and disruptive effects for PreCheck that are summarised in Table 4. The table also shows how we arrived at these numbers by taking the weighted average of predictions. Essentially, we conducted a sort of mock meeting of a panel of experts in which various views about how the deterrence and disruption numbers might change, and we then aggregated the imagined preferences. We assume that checkpoint deterrence will decrease when compared to the baseline case (without PreCheck), and that disruption rates in the PreCheck line will also be lower than the baseline rate, while those in the regular lines will be higher. Specifically, because there is a chance that a crafty terrorist may be able to be go through the PreCheck lane rather than the regular one, we assume that deterrence rates decrease, in relative terms, by 19% (e.g., from 50% as in Table 2 to 41% for a lone wolf attack). Similarly, we assume that disruption rates in the PreCheck (expedited) lines will be 38% lower, in relative terms, than baseline (without PreCheck) screening. At the same time, detection rates in the regular (enhanced) lines will be 29% higher, in relative terms, because, with half the work load, checkpoint security in these lines is more likely to be successful. Our assumed values are similar to those applied by Jackson et al. (2012a, b) who assumed, in their illustrative example, that enhanced screening increases detection rates by 25%, and expedited screening will reduce the detection rate by 38%.

[4] A device suspected of being a bomb was discovered in a suitcase of a man who boarded a Haiti Air flight at Kennedy International Airport on 26 September 1985 (GTD 2016).

Table 4 Estimated effect of PreCheck on checkpoint deterrence and detection rates

		Relative change in deterrence or disruption rate	Likelihood
PreCheck deterrence	Decrease in rate of deterrence	-20%	95%
	Increase in rate of deterrence	10%	5%
	Relative change in checkpoint deterrence rate:	-19%	
Enhanced	Decrease in rate of detection	0%	5%
Screening	Increase in rate of detection	30%	95%
Detection	Relative change in checkpoint detection rate:	29%	
Expedited	Decrease in rate of detection	-40%	95%
Screening	Increase in rate of detection	5%	5%
Detection	Relative change in checkpoint detection rate:	-38%	

To be sure, the deterrent effects of PreCheck could be described by other algorithms. However, rates of deterrence are more difficult to quantify than disruption rates as the former depends more on the motivation and on the adaptive capability of the terrorist. For example, deterrence rates for PreCheck depend on the ability of terrorists to game the system, to weigh their odds of being selected for inclusion in the PreCheck line or for random exclusion from it. Moreover, the security protocols when enrolling in PreCheck may reveal the applicant to be high risk and bring them to the attention of the authorities. This is an area for further study.

Under these four assumptions, and with managed inclusion and random exclusion omitted from the analysis, the total risk reduction for the full array of security measures is increased, albeit slightly, when PreCheck is added. The total risk reduction rises from 99.799% to 99.822% for lone wolf attacks and from 97.919% to 97.976% for terrorist organisation attacks. That is, the additional risk reduction (benefit) due to PreCheck is $\Delta R = 0.023\%$ for lone wolf attacks, and $\Delta R = 0.057\%$ for terrorist organisation attacks.

Risk reduction effects: sensitivity analysis

This conclusion proves to be very robust. The results of our model are in the top line of Table 5, and the rest of the table supplies a summary of what happens to these total risk reduction numbers when we change the assumptions in the model. As can be seen, any changes in risk reduction are very modest.

For example, there is still a risk-reducing benefit when three-quarters of passengers, rather than half of them, are directed to PreCheck.

The worst-case for Secure Flight is to assume that it is no better than random (50/50) when determining which line a passenger should go through. In this extreme case, the risk reduction benefit of PreCheck goes negative, but only slightly to: −0.01% for lone wolf IED attacks and −0.04% for terrorist organisation IED attacks.

Table 5 Sensitivity analysis of risk reductions for PreCheck without random exclusion or managed inclusion

	PreCheck risk reduction (ΔR)	
	Lone wolf	Terrorist organisation
50% PreCheck	0.02%	0.06%
Increase in Benefit (ΔR > 0%):		
Rates of deterrence and disruption of existing measures (without PreCheck) increased by 50%	0.01%	0.02%
Rate of disruption for expedited screening is reduced to 0%	0.01%	0.03%
75% of passengers go through PreCheck	0.02%	0.04%
25% of passengers go through PreCheck	0.03%	0.07%
One out of a million passengers is high risk	0.02%	0.06%
One out of a billion passengers is high risk	0.02%	0.06%
Relative decrease in the rate of disruption for expedited screening reduced by 50%	0.02%	0.05%
Secure Flight is 100% accurate in selecting passengers	0.03%	0.08%
Probability that aircraft survives if IED detonates reduced by 50%	0.03%	0.08%
Rates of disruption for all layers increased by 50%	0.03%	0.08%
Probability that IED is defective reduced by 50%	0.06%	0.07%
Rates of deterrence of existing measures (without PreCheck) are reduced by 50%	0.12%	0.24%
Existing measures (without PreCheck) have no deterrence	0.38%	0.62%
The terrorist arrives at the airport undeterred and undetected	0.66%	1.1%
Reduction in Benefit (ΔR < 0%):		
Reduction in PreCheck deterrence is doubled	-0.01%	-0.06%
Secure Flight selects passengers at random	-0.01%	-0.04%
Relative increase in the rate of disruption for enhanced screening reduced to 10%	-0.02%	-0.07%
Relative increase in the rate of disruption for enhanced screening reduced to 10%, and disruption rate for expedited screening reduced by 75%	-0.02%	-0.08%
No increase in the rate of disruption for enhanced screening	-0.04%	-0.13%
Rate of disruption for checkpoint screening (without PreCheck) reduced to 5%	-0.06%	-0.12%
No increase in the rate of disruption for enhanced screening, relative decrease in PreCheck deterrence is doubled from 20% to 40%, and relative decrease in expedited screening effectiveness increased from 40% to 60%.	-0.08%	-0.27%

A 2015 report from the Department of Homeland Security (DHS) Office of the Inspector General found that U.S. airport screening failed to detect mock weapons in 95% of tests (Reuters 2015). Our analysis assumes a disruption (or detection) rate of 25–50% for screening without PreCheck (Table 2). If we instead assume a lower disruption rate of only 5%, which is perhaps more in line with those findings, the benefit of PreCheck becomes modestly negative: −0.06% to −0.12% for the two IED threats.

A worse-case scenario may assume that there is (i) no increase in the rate of disruption for enhanced screening, (ii) the relative decrease in PreCheck deterrence is doubled from 20% to 40%, and (iii) the relative decrease in expedited screening effectiveness is increased from 40% to 60%. Under these circumstances, PreCheck increases risk (or provides a negative risk reduction) by 0.08% to 0.27% for the two IED threats. Finally, if the terrorist arrives at the airport undeterred and undetected (i.e. rates of deterrence are 0% for all security measures, and disruption rates are 0% for those measures that apply before the terrorist arrives at the airport), the risk reduction from existing security measures at the airport and on-board the aircraft remains a high 97.4% and 87.2% for IED lone wolf and terrorist organisation attacks, respectively. Because there is more remaining risk to reduce, the risk reduction from PreCheck is a high 0.66% and 1.1%.

With the exception of checkpoint deterrence and disruption rates, the influence of PreCheck on risk is not dependent on the deterrence and disruption rates of each of the remaining security layers, but of their rates in combination. For example, for a terrorist organisation IED attack in which checkpoint deterrence and disruption rates are each 25%, the deterrence and disruption rates for all other layers combined must be equal to 96.5% in order for the risk reduction from PreCheck to be 0.054%. If it is believed that these layers of security have an increased combined risk reducing potential of, say, 99%, risk reduction from PreCheck is lowered three-fold to only 0.015%. On the other hand, if the remaining layers of security are judged to be only 80% effective in total, the risk reduction from PreCheck increases to 0.31%. Clearly, most realistic combinations of parameter values suggest that, at worst, PreCheck lowers the benefit (or risk reduction) by 0.3%, while in other cases the benefit can exceed 1.0%. That is, any lowering of risk reduction is small while at least some increases in risk reduction are more pronounced. All changes in the risk reducing benefit from PreCheck essentially lie within the margin of error of the analysis – that is, they would not be considered to be particularly significant. This attests to the robustness of our results, while suggesting that PreCheck would most likely modestly increase the overall risk-reducing benefit.

PreCheck with random exclusion or managed inclusion

Overall, the results suggest that when random exclusion and managed inclusion are added to the PreCheck program, they have little effect one way or the other on the risk reducing capability of PreCheck.

The random exclusion program does increase the benefit of PreCheck by directing more passengers to enhanced screening, but it does so only modestly. For example, if 5% of PreCheck passengers are diverted to the regular screening lines, the benefit of PreCheck increases only slightly, by less than 0.001%.

If we assume that 10% of passengers in the regular lines are diverted to the PreCheck ones as part of the managed inclusion program and that canines have a 99% probability of identifying low risk passengers but only a 80% probability of detecting high risk ones, the benefit of PreCheck in producing risk reduction remains positive but is lowered slightly from 0.023% to 0.020% for lone wolf attacks and from 0.057% to 0.048% for terrorist organisation attacks. Increasing the number of passengers diverted to 40% reduces the benefit of PreCheck from 0.023% to 0.011% for the lone wolf and from 0.057% to 0.020% for the terrorist organisation. If canines are only 50% accurate in detecting high risk passengers then, under the 40% condition, the risk reduction benefit of PreCheck declines to 0.01% for both threats.

Finally, if 10% of passengers in the regular lanes are randomly sent to the PreCheck ones by managed inclusion, the benefit of PreCheck is lowered to 0.01% for both IED threats. Allocating 10% of enhanced screening passengers to expedited lanes increases the proportion of travellers who "qualify" for PreCheck from 50% to 55%. If 50% PreCheck results in $110 million of savings to TSA each year, managed inclusion under these circumstances will result in additional TSA savings of $11 million per year while at the same time reducing checkpoint queuing times and improving security outcomes.

The economic benefits of TSA PreCheck

The risk reducing benefit of PreCheck can be expressed in economic terms and can be obtained from Eq. (3). For the condition under which 50% of passengers go through PreCheck, if we estimate that a successful IED attack will inflict a loss of $25 billion while assuming a high attack likelihood of 20% per year, the yearly risk reduction benefit in economic terms comes to $1 million and $3 million for lone wolf and terrorist organisation attacks, respectively. If we posit that each threat would occur each year or that an attack will cause $100 billion in losses, the yearly benefit increases to $5–$14 million per year. Under a worst-case scenario in which passengers are selected at random for which line to go through, or there is no increase in the rate of disruption for enhanced screening, PreCheck deterrence rates are halved, and disruption rates for expedited screening reduced by 50% (see Table 5), the yearly "benefit" becomes a loss of $2–$13 million. If we posit that each threat would occur each year or that an attack will cause $100 billion in losses, the yearly expected loss increases to $10–$65 million per year.

However, it is important to stress that PreCheck generates a number of co-benefits, and these should be added into the consideration. Expanding and updating an earlier discussion (Stewart and Mueller 2015), it seems clear that these co-benefits are orders of magnitude greater than those supplied by PreCheck's risk-reducing benefit (or its risk-increasing loss).

As noted, PreCheck reduces overall screening costs by over $110 million per year (DHS 2016). In addition, however, it provides a very substantial additional co-benefit by improving the passenger experience. It increases the numbers of satisfied business passengers by 12%, and for many it "makes for a better business travel experience" (GBTA 2016). Mathew et al. (2016) found that the median wait time for enhanced screening was 8.9 min but only 2.4 min in the PreCheck lanes at Cincinnati/Northern Kentucky airport. Stone and Zissu (2007) observed that expedited screening reduced wait times by an average 4 minutes at Orlando International Airport. There is, of course, great financial benefit to airlines if more efficient and faster screening reduces wait times because this leads to high passenger satisfaction (Gkritza et al. 2006). Holguin-Veras et al. (2012) find that reducing waiting times from 10 to 5 min increased airline market share by 1% for a large airport in the U.S., which comes to $2 billion in additional U.S. airline revenues based on total annual U.S. airline revenues of $205 billion in 2015 (BTS 2016). Moreover, all businesses pay special attention to regular customers, and PreCheck is likely to be especially pleasing to the passengers the airlines most treasure: frequent flyers.

Security delays also inflict considerable costs on the economy more generally (Mullainathan and Thaler 2016). Treverton et al. (2008) found that passengers value their time at about $40 per hour (in 2016 dollars), and a more recent study, conducted for the U.S. Transportation Research Board of the National Academies, recommends that the passenger value their time during check-in and security screening at $32.70 per hour (in 2016 dollars). Landau et al. (2015) recommend that this figure be used in cost-benefit analyses for government and private transportation projects and policies. If we do so, and if the PreCheck program reduces waiting times for expedited screening passengers by a modest 5 minutes and if 50% of passengers are approved for that program, and since TSA screened 708 million passengers in 2015 (TSA 2016) there would be savings of $965 million per year in passenger time along with $2 billion in increased airline revenues. All this in total would generate a total co-benefit of $3 billion per year. If all passengers went through PreCheck, this total would rise to nearly $6 billion per year.

Finally, some studies suggest there may be hundreds of automobile deaths yearly of people who choose to drive rather than fly short-haul routes (Blalock et al. 2007). If 50 of these lives were saved each year because PreCheck brought some of the drivers back to the airports, the total gain, or co-benefit, using standard measures of the value of human life, would be $375 million (Stewart and Mueller 2015).

Conclusions

This paper developed a risk and economic assessment of the Transportation Security Administration's PreCheck program (or TSA Pre✓®) considering threat likelihood, risk reduction, consequences, and co-benefits in a probabilistic terrorism risk framework. A reliability analysis of the overall system of aviation security allowed the rate of deterrence and disruption to be inferred for IED terrorist threats to aircraft in the United States. Risk analysis then found that existing layers of aviation security (without TSA PreCheck) reduce the risk of a passenger-borne IED attack by over 98% - that is they reduce a terrorist bomber's chance of success to less, probably far less, than one in 50. This level of risk reduction is very robust: security remains high even when the parameters that make it up are varied considerably. In particular, because of the large array of other security layers, overall risk reduction is relatively insensitive to how effective checkpoint screening is. A risk analysis of TSA PreCheck showed that most realistic combinations of parameter values lead to, at worst, a 0.3% reduction in this benefit while other combinations suggest that the benefit can be positive and reach up to 1%. Sensitivity analyses show that PreCheck most likely actually supplies an increase in overall risk reduction or benefit, if only a modest one. Meanwhile, the co-benefits of TSA PreCheck, which include reduced screening costs and improvement in the passenger experience, are considerable and can exceed several billion dollars per year.

Acknowledgements This research was supported by the United States Department of Homeland Security through the National Center for Risk and Economic Analysis of Terrorism Events (CREATE) under Agreement No. 2010-ST-061-RE0001-06. However, any opinions, findings, and conclusions or recommendations in this document are those of the authors and do not necessarily reflect views of the United States Department of Homeland Security or the University of Southern California.

References

Aaronson T (2013) The terror factory. Ig Publishing, Brooklyn

Abrahms M (2006) Why terrorism does not work. Int Secur 31(2):42–78

Abrahms M (2011) Does terrorism really work? Evolution in the conventional wisdom since 9/11. Def Peace Econ 22(6):583–594

Aratani, L. (2015), Change in TSA screening may mean longer waits at TSA checkpoints.The Washington Post

Baum P (2016) Violence in the skies: a history of aircraft hijacking and bombing. Summersdale Publishers, Chichester

Bayles F (1996) Planes don't blow up aviation experts assert. Int Herald Tribune

Beckner C (2015) Risk-based security and the aviation system: operational objectives and policy challenges, issue brief # 2015–02. The George Washington University, U.S, Center for Cyber & Homeland Security

Blalock G, Vrinda K, Simon DH (2007) The impact of post-9/11 airport security measures on the demand for air travel. J Law Econ 50(4):731–755

BTS (2016) Operating revenue: all U.S. carriers - all regions, bureau of transportation statistics, U.S. Department of Transportation, Washington, D.C.

Cha EJ, Ellingwood BR (2012) Risk-averse decision-making for civil infrastructure exposed to low-probability, high-consequence hazards. Reliab Eng Syst Saf 104:27–35

DHS (2016) Budget-in-brief fiscal year 2016. Department of Homeland Security, Washington, DC

Elias B (2009) Airport and aviation security: U.S. policy and strategy in the age of global terrorism. CRC Press, Boca Raton

Fletcher KC (2011) Aviation security: case for risk-based passenger screening. Master's Thesis, Naval Postgraduate School, California www.hsdl.org/?view&did=699603

Fletcher KC (2015) Risk-based security: assessing the path forward for TSA Pre✓®, written testimony of TSA chief risk officer Ken Fletcher for a house committee on homeland security, subcommittee on transportation security hearing, Washington, D.C.

GAO (2014) Aviation security: rapid growth in expedited passenger screening highlights need to plan effective security assessments, report number GAO-15-150, government accountability office, Washington, D.C.

GAO (2015) Aviation security, TSA's managed inclusion process expands passenger expedited screening, but TSA has not tested its security effectiveness, statement of Jennifer A. Grover, Director, homeland security and justice, testimony before the subcommittee on transportation security, committee on homeland security, house of representatives, Washington, D.C.

GBTA (2016) Satisfaction significantly higher for business travelers enrolled in TSA PreCheck, global business travel association, news release

Gillen D, Morrison WG (2015) Aviation security: costing, pricing, finance and performance. J Air Transp Manag 48:1–12

Gkritza K, Niemeier D, Mannering F (2006) Airport security screening and changing passenger satisfaction: an exploratory assessment. J Air Transp Manag 12(5):213–219

Global Terrorism Database (2016) National consortium for the study of terrorism and responses to terrorism (START), University of Maryland

Grant M, Stewart MG (2012) A systems model for probabilistic risk assessment of improvised explosive device attack. Int J Intel Defence Support Syst 5(1):75–93

Grant M, Stewart MG (2015) Probabilistic risk assessment for improvised explosive device attacks causing significant building damage. J Perform Constr Facil 29(5):B4014009

Hawley K, Means N (2012) Permanent emergency: inside the TSA and the fight for the future of American security. Palgrave Macmillan, New York

Holguin-Veras J, Xu N, Bhat C (2012) An assessment of the impacts of inspection times on the airline Industry's market share after September 11th. J Air Trans Manag 23(1):17–24

IATA (2013) Joint press release: ACI and IATA collaborate to deliver smart security, international air transport association, press release no. 70,

Jackson BA, LaTourette T (2015) Assessing the effectiveness of layered security for protecting the aviation system against adaptive adversaries. J Air Trans Manag 35:26–33

Jackson BA, Chan EW, LaTourrette T (2012a) Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. J Trans Secur 5:1–34

Jackson BA, LaTourrette T, Chan EW, Lundberg R, Morral AR, Frelinger DR (2012b) Efficient aviation security. RAND Corporation, Santa Monica

Jacobson SH, Karnani T, Kobza JE, Ritchie L (2006) A cost-benefit analysis of alternative device configurations for aviation checked baggage security screening. Risk Anal 26(2):297–310
Kenney M (2010) 'Dumb' yet deadly: local knowledge and poor tradecraft among Islamist militants in Britain and Spain. Stud Conflict Terrorism 31:1–22
Kriel, R. and Cruickshank, P. (2016) Source: 'Sophisticated' laptop bomb on Somali plane got through X-ray machine, *CNN*
Landau S, Weisbrod G, Gosling G, Williges C, Pumphrey M, Fowler M (2015) Passenger value of time, benefit-cost analysis, and airport capital investment decisions, volume 1: guidebook for valuing user time savings in airport capital investment decision analysis, contractors guidebook for ARCP 03–19, transportation research board of the national academies
Lee AJ, Jacobson SH (2011) The impact of aviation checkpoint queues on optimizing security screening effectiveness. Reliab Eng Syst Saf 96(8):900–911
Martonosi SE, Barnett A (2006) How effective is security screening of airline passengers? Interfaces 36(6): 545–552
Mathew JK, Hubbard SM and Bullock DM (2016) Impact of security reconfiguration and expedited security at Cincinnati/Northern Kentucky airport on reducing passenger wait time, *Transportation Research Board 95th Annual Meeting*, Washington, D.C.
McLay LA, Lee AJ, Jacobson SH (2010) Risk-based policies for airport security checkpoint screening. Transp Sci 44(3):333–349
Morral AR, Price CC, Oritz DS, Wilson B, LaTourrette T, Mobley BW, McKay S, Willis HH (2012) Modeling terrorism risk to the air transportation system. RAND Corporation, Santa Monica
Mueller J (2016) Terrorism since 9/11: the American cases. http://politicalscience.osu.edu/faculty/jmueller/SINCE.pdf. Accessed 20 May 2016
Mueller J, Stewart MG (2011) Terror, security, and money: balancing the risks, benefits, and costs of homeland security. Oxford University Press, New York
Mueller J, Stewart MG (2012) The terrorism delusion: America's overwrought response to September 11. Int Secur 37(1):81–110
Mueller J, Stewart MG (2014) Evaluating counterterrorism spending. J Econ Perspect 28(3):237–248
Mueller J, Stewart MG (2016a) Chasing ghosts: the policing of terrorism. Oxford University Press, Oxford and New York
Mueller J, Stewart MG (2016b) Conflating terrorism and insurgency, lawfare.com
Mullainathan, S. and Thaler, R.H. (2016) Waiting in line for the illusion of security. New York Times
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, 11-12
Poole RW (2015) Fresh thinking on aviation security. J Air Trans Manag 48:65–67
Price JC, Forrest JS (2013) Practical aviation security: predicting and preventing future threats. Butterworth-Heinemann, Oxford, UK
Reuters (2015) US airport screenings fail to detect mock weapons in 95% of tests, The Guardian, 3
Sewell EC, Lee AJ, Jacobson SH (2013) Optimal allocation of aviation security screening devices. J Transp Secur 6:103–116
Stewart MG, Melchers RE (1997) Probabilistic risk assessment of engineering systems. Chapman & Hall, London
Stewart MG, Mueller J (2008) A risk and cost-benefit assessment of U.S. Aviation Security Measures, J Trans Secur, 1(3):143–159.
Stewart MG, Mueller J (2011) Cost-benefit analysis of advanced imaging technology fully body scanners for airline passenger security screening. J Homel Secur Emerg Manag 8(1):Article 30
Stewart MG, Mueller J (2013a) Terrorism risks and cost-benefit analysis of aviation security. Risk Anal 33(5): 893–908
Stewart MG, Mueller J (2013b) Aviation security, risk assessment, and risk aversion for public decisionmaking. J Policy Anal Manage 32(3):615–633
Stewart MG, Mueller J (2014a) Risk and cost-benefit analysis of police counter-terrorism operations at Australian airports. J Policing Intell Counter Terrorism 9(2):98–116
Stewart MG, Mueller J (2014b) Cost-benefit analysis of airport security: are airports too safe? J Air Trans Manag 35:19–28
Stewart MG, Mueller J (2015) Responsible policy analysis in aviation security with an evaluation of PreCheck. J Air Trans Manag 48(September):13–22

Stewart MG, Mueller J (2016) Risk-based passenger screening: risk and economic assessment of TSA PreCheck, increased security at reduced cost?, Research report no. 283.06.2016, Centre for Infrastructure Performance and Reliability, the University of Newcastle

Stewart MG, Ellingwood BR, Mueller J (2011) Homeland security: a case study in risk aversion for public decision-making. International Journal of Risk Assessment and Management 15(5/6):367–386

Stone CA, Zissu A (2007) Registered traveler program: the financial value of registering the good guys. Rev Policy Res 24(5):443–462

Sunstein CR (2002) The cost-benefit state: the future of regulatory protection. ABA Publishing, American Bar Association, Chicago

Treverton GF, Adams JL, Dertouzous J, Dutt A, Everingham SF, Larson EV (2008) The costs of responding to the terrorist threats. In: Keefer P, Loayza N (eds) Terrorism, economic development, and political openness. Cambridge University Press, New York

TSA (2012) http://www.tsa.gov/what_we_do/layers/index.shtm

TSA (2014) Written testimony of TSA administrator John Pistole for a senate committee on commerce, science, and transportation hearing titled “TSA oversight: confronting America's transportation security challenges”

TSA (2016) TSA releases 2015 statistics, national press release. Transportation Security Administration, Washington, D.C.

von Winterfeldt D, O’Sullivan TM (2006) Should We protect commercial airplanes against surface-to-air missile attacks by terrorists? Decis Anal 3(2):63–75

Walsh B (2009) Why it’s not easy to detonate a bomb on board. Time

Willis HH, 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 Anal 28:325

Wong S, Brooks N (2015) Evolving risk-based security: a review of current issues and emerging trends impacting security screening in the aviation industry. J Air Trans Manag 48:60–64