Transportation
Security
Administration

Office of Security Technology

Cost Benefit Analysis (CBA) for the Procurement of Advanced Imaging Technology (AIT) Classified Risk Analysis

June 2011

Version 3.0

REVISION HISTORY

VERSION	DATE REVISED	REVISED BY	REVISIONS
1.0	6/30/2010	Matt Martin	
1.1	7/1/2010	Matt Martin	Edits by Andrew Cox
1.2	7/19/2010	Matt Martin	Additional analysis for 180pph throughput
1.3	8/6/2010	Matt Martin	
1.4	8/12/2010	Matt Martin	Added tables for numbers displayed in charts
1.5	8/17/2010	Matt Martin	Added RMAT and TSSRA Comparison
1.6	9/1/2010	Jen LeMoine	Updated tables with traffic numbers
1.7	9/13/2010	Jen LeMoine	Updated Consequence Tables with TSSRA numbers
1.8	9/17/10	Jen LeMoine	Edits by Dawn Riddle
2.0	3/16/11	Jen LeMoine	Updated report based on AIT briefing to Ms. Rossides
2.1	4/4/11	Jen LeMoine	Edits by Andrew Cox
2.2	4/19/11	Jen LeMoine	Edits by Nick Bianchini
3.0	6/21/11	Jen LeMoine	Updated reports with new LCCEs

will check to see whe it came out of draft.

added new tool RMat about 2yrs ago + GAO questions

Table of Contents

49 USC 114(r) and 49 CFR 1520

List of Figures

List of Tables

(U) Risk Overview

(U) In this cost-benefit analysis (CBA) of Advanced Imagining Technology (AIT), benefit is measured by the percent reduction of attack success and consequence reduction.[1] Attack success is a measure of probability of the adversary achieving their attack objectives given a specific set of tactics on a particular target. Three countermeasure options were considered against the relevant attack scenarios: Existing baseline security (Walk through metal detector (WTMD)), Alternative 1 (AIT), and Alternative 2 (Standard Pat Down (SPD) with WTMD-referred to as SPD throughout this report). The SPD was chosen as an alternative because it was considered to be qualitatively comparable to the AIT. Both countermeasures have the capability of detecting anomalies, such as weapons, on the body, and both might deter an adversary from conducting a body-bomb attack. Clearly, the operational and security effectiveness for these countermeasures can be quite different.

(U) This analysis is biased towards the worst-reasonable attack case in that the details of adversary concealment methods and tactics were considered relatively unfavorable to the AIT technology. Furthermore, one of the deployment scenarios, the "conservative" case, assumes no improvement of capability over time. Therefore, the analytic outputs in the following sections are anchored on one end of the spectrum by what TSA believes to be a conservative evaluation of the aviation security system performance that is plausibly biased in favor of the adversary. While the analysis for the most conservative performance forecast does not assume improvement in AIT technology, it is likely that over the next seven years performance may show significant gains. Therefore, multiple AIT performance forecasts were analyzed in this assessment and will be outlined in greater detail in the following section. These other forecasts fill out the rest of our analytic spectrum. For these more progressive forecasts, the Office of Security Technology (OST) is able to increase the throughput of AIT to match the throughput of a two lane set of AT X-Ray machines. This, in turn, would allow full AIT coverage with a far smaller number of purchased machines.

(U) Given these considerations, our analysis shows that even the conservative deployment forecast of AIT (Alternative 1) appears to perform the best compared to SPD and Baseline.

(U/SSI) The following additional findings arise from the assessment of the risk reduction value of each alternative regardless of AIT technology improvements:[2]

49 USC 114(r) and 49 CFR 1520

[1] See Appendix A for a definition of consequence.

[2] See Appendix A for definition of risk.

- Assuming a body-bomb attack, AIT is the more cost effective solution as compared to SPD and Baseline.
- The potential range of damage prevented by AIT is significant compared to the lifecycle cost of the AIT. The difference between the prevented damage and the lifecycle cost of AIT represents the benefit in our cost-benefit analysis.

(U) Multiple AIT performance forecasts were analyzed due to the possibility of various technology improvements

(U) TSA is designing and implementing AIT advances that will allow throughput to return to 180 passengers per hour for AT X-Ray machines, and potentially up to 360 passengers per hour for AIT machines starting in year four. Additionally, if AIT machines are able to shrink in size to fit in smaller lanes (i.e. CAT IV lanes), these improvements will eventually provide a) enough throughput for the AIT machines to allow a 2-1 configuration with full AIT screening and b) a small enough size to deploy to all checkpoint lanes. This will result in greater risk reduction and fewer overall AIT machines needed.

(U) Since the likelihood and effect of technology improvements to AIT is unknown, this risk assessment performed analysis on Alternative 1 (AIT) using three different performance forecasts:[3]

1. **Conservative case** – Assumes no technology improvements; therefore, the probability that an AIT detects anomalies of the body remains constant and never increases, throughput remains at 150 passengers per hour, and AIT machines are never able to shrink in size to fit in smaller lanes.
2. **Projected case** – Slight technology enhancements are realized. The probability of detection (P(d)) for AIT machines increases incrementally and throughput gradually increases to 210 passengers per hour. Additionally, all lane sets are covered due to technology improvements that allows for production of smaller AIT machines.
3. **Maximum theoretical best case (best case)** – Significant improvements to AIT technology are realized. P(d) for AIT machines gradually increases and throughput steadily increases to 360 passengers per hour. It is also assumes that the production of smaller AIT machines is possible. This scenario is feasible, but has significant technology risks associated with it making it a challenge to meet the performance forecast.

(U) The conservative and best cases represent the boundaries of the risk spectrum. The projected case falls within these boundaries.

---

[3] See Appendix B for additional information on the three AIT performance forecasts.

(U)

		Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
Conservative	AT X-Ray Throughput	150	150	150	150	150	150	150
	AIT Throughput	150	150	150	150	150	150	150
Projected	AT X-Ray Throughput	150	150	150	150	150	150	150
	AIT Throughput	150	165	180	210	210	210	210
Best case	AT X-Ray Throughput	150	150	165	180	180	180	180
	AIT Throughput	150	180	240	360	360	360	360

Table 1: AT X-Ray and AIT throughput per machine by performance forecast

(U) As shown is Table 1, for the first year, throughput and the rate of risk reduction would stay at the 150 passenger per hour level, which represents the current throughput of the AIT machines that TSA is currently procuring and deploying. However, during Phase II for the best case performance forecast, it is expected that throughput will increase up to 180 passengers per hour due to a combination of ATR rollouts, image processing speed enhancements, and passenger education improvements. The speed of AT X-Ray machines will also increase up to 180 passengers per hour each, and up to 360 passengers per hour for a two lane set. In Phase III of the best case performance forecast, throughput for the individual AIT machines will reach up to 240 passengers per hour, and eventually to full operating capacity of 360 passengers per hour. This improvement would permit more people to be screened by the lanes with AIT machines, allowing the 2-1 configuration. This will not impact overall checkpoint throughput or risk reduction compared to deployments without AIT advances.

(U) Assumptions

(U) High-end and low-end adversaries have unique characteristics that cause differences in countermeasure performance

(U) While the Risk Management Analysis Tool (RMAT) assumes the range of adversaries faced by TSA have similar intent to do the aviation system harm, it does not assume that adversary groups that threaten the aviation security system are identical in their capability to harm the system. The high-end and low-end adversaries were modeled to represent different points on the spectrum of adversary capability to account for these differences, which can influence the risk effectiveness of each alternative countermeasure.

(U) The high-end adversary is assumed to have extensive information about aviation security, high weapon making skills, higher resources, and better planning skills. Additionally, the high-end adversary is capable of marshalling resources to conduct multiple parallel attacks with highly skilled attack agents. Their ability to conduct surveillance and learn from these observations allows them to easily avoid specific countermeasures if there are alternative paths to their target.

(U) In contrast, low-end adversaries have limited information about aviation security, low weapon making skills, low resources, poor planning skills, and low patience. Their lower capability means they are less able to conduct adequate planning and surveillance and are indifferent to avoiding countermeasures. It is important to note that the low-end adversary is also significantly less capable of conducting multiple parallel attacks, which means low-end adversaries have a lower potential consequence when compared to the high-end adversary for a single attack set.

(U) *The distinction between the high-end and low-end adversaries represents each end of the capability spectrum. Since TSA cannot predict the future (i.e. the type of adversary that will attempt an attack), the overall capability spectrum provides key insights about adversary characteristics to assist TSA in allocating resources using a least regrets performance forecast.*

(U) Smaller throughput lanes and airports that are unable to fit an AIT machine need a equivalent alternative countermeasure to be implemented

(U) The attack path that an adversary selects is dependent upon whether the agent's profile skews closer to the high-end or low-end of the capability spectrum. The high-end adversary is able to identify the lanes that have the lowest detection capabilities and always chooses to go to those lanes. This is an important insight as the conservative performance forecast has 150 lanes that will not have an AIT due to facility restrictions and/or low traffic volume numbers that do not justify an AIT.

(U) Thus, the high-end adversaries will always choose to go to those 150 lanes unless a comparable countermeasure is put in place. The SPD is a qualitatively comparable alternative countermeasure to the AIT. For this reason, and for the purposes of this CBA, Alternative 1 (AIT) includes a limited deployment of SPD to those 150 lanes. *However, any alternative countermeasure to the AIT can be used, as long as it will detect the same attack types as the AIT and provides a comparable level of detection.*

(U) The AIT equivalent, in this case SPD, is necessary because in contrast to the low-end adversary, the high-end adversary intentionally avoids lanes that do not have an AIT or a comparable alternative countermeasure. At the other end of the threat spectrum, the probability of a low-end adversary encountering an AIT is equivalent to the overall percentage of traffic exposed to AIT screening.[4] A high-end adversary seeks the weakest point in the aviation system within the constraints of his assigned tactics, mission, surveillance, learning, and planning capability. However, the key limitation of the SPD is that it cannot be conducted on passengers with anything resembling the operational efficiency of the AIT and it is a relatively invasive

---

[4] See Appendix B for definition of adversary exposure.

procedure unlikely to be tolerated by the American public if applied broadly. In short, it is roughly comparable from a security perspective but is not operationally viable.

(U) The threat level of the adversary remains constant

49 USC 114(r) and 49 CFR 1520

[redacted]

(U) Conclusions

49 USC 114(r) and 49 CFR 1520

[redacted]

(U/SSI) Achieved consequence is a function of damage and likelihood of a particular attack type succeeding. In essence, achieved consequence is similar to the concept of expected value. The study compared the achieved consequence scores for the following four attack types:

49 USC 114(r) and 49 CFR 1520

[redacted]

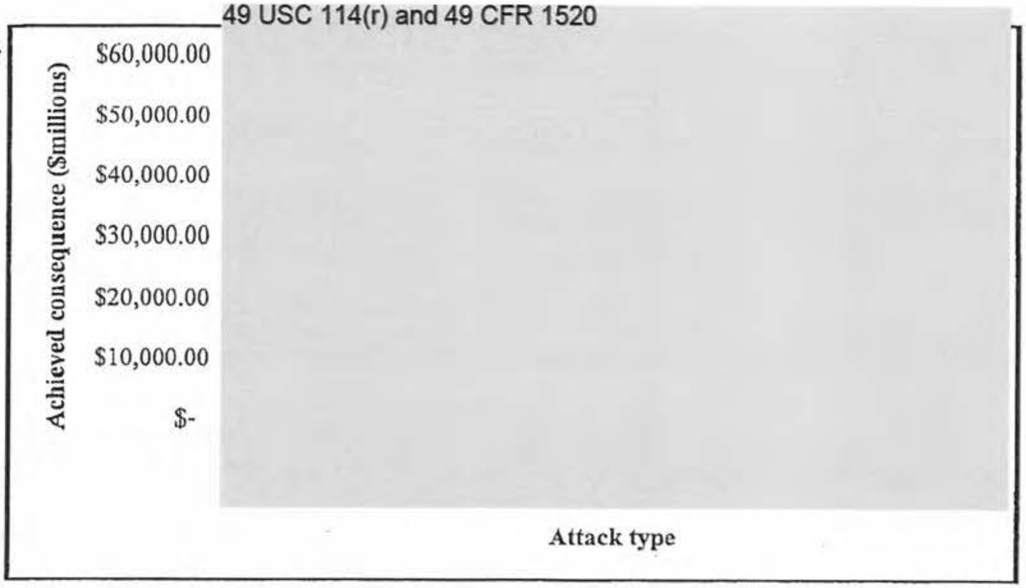
(U) RMAT calculates the probability that the adversary will execute a successful attack for each attack type given a set number of attack agents on his team, which determines the number of attempted parallel attacks.[6] The better the countermeasure is against the attack type, the greater the reduction will be in the adversary's probability of success and achieved consequences.

---

[5] See Appendix E for additional information on threat-shifting.

[6] RMAT measures the likelihood of a particular attack succeeding given an adversary's choice of that attack. TSSRA measures the likelihood of an adversary choosing a particular type of attack.

~~(S)~~



[redacted]

Figure 1: Achieved consequence by attack type

49 USC 114(r) and 49 CFR 1520

[redacted]

49 USC 114(r) and 49 CFR 1520

[redacted]

49 USC 114(r) and 49 CFR 1520

[redacted]

49 USC 114(r) and 49 CFR 1520

[redacted]

---

[7] See Appendix A for the definition of relative reduction.

49 USC 114(r) and 49 CFR 1520

2010

(S)

Type	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
Alt. 1 (AIT-Conservative)	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual
Alt. 1 (AIT-Projected)	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual
Alt. 1 (AIT-Best case)	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual
Alt. 2 (SPD)	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual

Table 2: Relative and actual percent reduction in attack success for Alternative 1 (AIT) and Alternative 2 (SPD) vs. baseline against the low-end adversary[8]

Compared
to the whole
Check point system
no WMD to AIT or SPD

[8] Source for relative and actual numbers: RMAP Study Post Processing DataforChartsByCM Tab

~~(S)~~

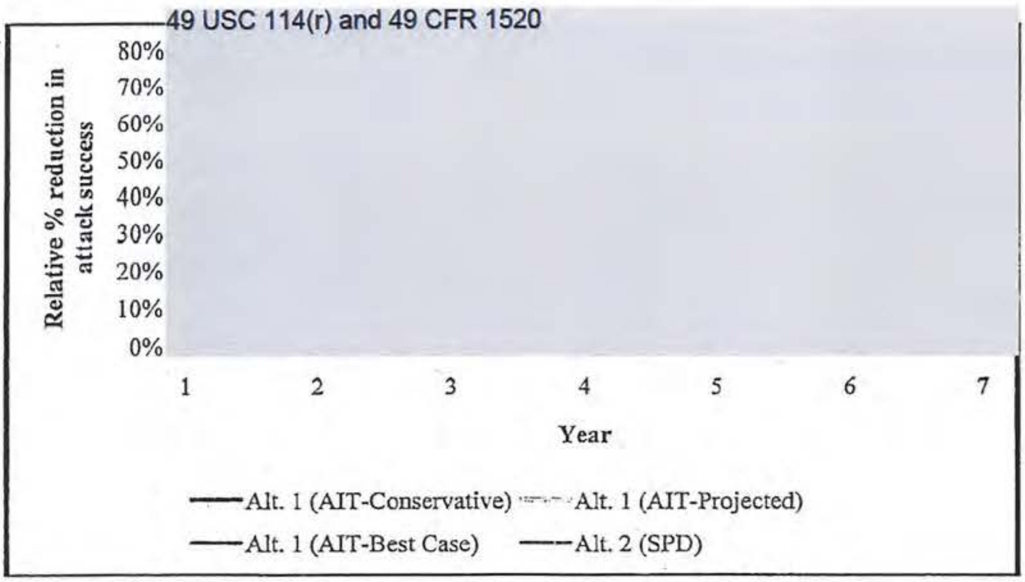


Figure 2: Relative percent reduction in attack success for Alternative 1 (AIT) and Alternative 2 (SPD) vs. baseline against the low-end adversary

~~(S)~~

Type	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
Alt. 1 (AIT-Conservative)	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual
Alt. 1 (AIT-Projected)	49 USC 114(r) Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual
Alt. 1 (AIT-Best case)	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) and Actual	49 USC 114(r) and Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual
Alt. 2 (SPD)	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual	49 USC 114(r) and Relative 49 USC 114(r) Actual

Table 3: Relative and actual percent reduction in attack success for Alternative 1 (AIT) and Alternative 2 (SPD) vs. baseline against the high-end adversary[9]

[9] Source for relative and actual numbers: RMAP Study Post Processing DataforChartsByCM Tab

(S)

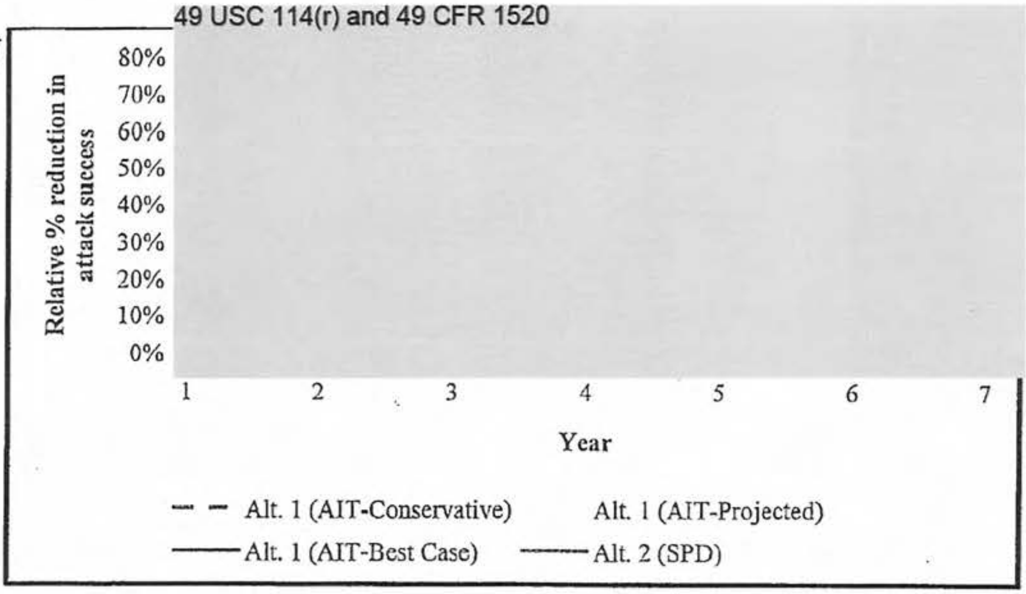


Figure 3: Relative percent reduction in attack success for Alternative 1 (AIT) and Alternative 2 (SPD) vs. baseline against the high-end adversary

49 USC 114(r) and 49 CFR 1520

49 USC 114(r) and 49 CFR 1520

(U) This analysis compares each alternative's change in attack success to the overall gross cost of implementation.[10] In the comparison, the cost and percent chance of success for Alternative 1 (AIT) for all performance forecasts is based on full deployment figures.

(S)

	Baseline	Alt. 1 (AIT-Conservative)	Alt. 1 (AIT-Projected)	Alt. 1 (AIT-Best case)	Alt. 2 (SPD)
Total gross costs (over 13 years)[11]	$6,732,671,005	$11,181,691,015	$11,181,691,015	$8,813,501,095	$17,234,267,379
Relative attack success reduction over baseline	-	49 USC 114(r) and 49 CFR (High-End) 49 USC 114(r) and 49 CFR (Low-End)	49 USC 114(r) and 49 (High-End) 49 USC 114(r) (Low-End)	49 USC 114(r) and 49 (High-End) 49 USC 114(r) and (Low-End)	49 USC 114(r) and (High-End) 49 USC (Low-End)
Chance of adversary complete success	49 USC 114(r) and (High-End) 49 USC 114(r) and (Low-End)	49 USC 114(r) and (High-End) 49 USC 114(r) (Low-End)	49 USC 114(r) and (High-End) 49 USC 114(r) (Low-End)	49 USC 114(r) and (High-End) 49 USC 114(r) (Low-End)	49 USC 114(r) and (High-End) 49 USC (Low-End)
*Cost per additional reduction in actual attack success percentage point**	-	(S) **$931,807,585** (High-End) (S) **$698,855,688** (Low-End)	(S) **$385,575,552** (High-End) (S) **$486,160,479** (Low-End)	(S) **$214,963,441** (High-End) (S) **$352,540,044** (Low-End)	(S) **$2,872,377,896** (High-End) (S) **$5,744,755,793** (Low-End)

*Each additional percentage of risk reduction costs X amount of dollars.

Table 4: Relative attack success reduction vs. total gross costs of all countermeasures

But as the technology improves the cost to deploy the technology decreases. must if cost saving come from increased throughput

~~(S)~~ Overall, the baseline alternative is one of the least costly countermeasures, but the baseline also has the greatest chance of a successful attack for either adversary type out of all alternatives in this analysis: 49 USC 114(r) and for the high-end adversary and 49 USC 114(r) and for the low-end adversary.

~~(S)~~ Alternative 1 (AIT-Conservative) is estimated to cost $11,181,691,015 and reduces a high-end adversary's overall chance of a successful attack to 49 USC 114(r) a ~~(S)~~ 21% relative reduction over the baseline. A low-end adversary has a 49 USC 114(r) chance of a successful attack with full deployment of AITs, a ~~(S)~~ 48% reduction over the baseline.

~~(S)~~ As the probability of detection and capabilities improve for AIT machines, the chance of a successful attack will decrease which means these numbers represent the lower-bound of AIT performance against an adversary based on the available performance data. Therefore, when compared to the baseline, under the projected performance forecast (Alternative 1 (AIT-Projected)), the chance of complete attack success for a high-end and low-end adversary is

[10] Total gross amount is comprised of baseline and AIT/SPD cost. Due to overlapping costs, the baseline total cost cannot be subtracted from the AIT or SPD totals.

[11] See PSP LCCE estimate for details.

lowered to 49 USC 114(r) [redacted] and 49 USC 114(r) [redacted] respectively and the estimated cost is $11,181,691,015. The likelihood that an adversary has complete attack success is reduced further for Alternative 1 (AIT-Best case), which is also the least costly alternative, at $8,813,501,095. Compared to the baseline, the best case performance forecast lowers a high-end adversary's chance of complete attack success to (S) 13% and reduces the chance of complete success for the low-end adversary to (S) 8%. Currently, program and technology risks are significant enough to make the best case performance forecast difficult to achieve.

49 USC 114(r) and 49 CFR 1520 [redacted]

(S) Alternative 2 (SPD) is estimated to cost $17,234,267,379, and yields an (S) 11% relative reduction for a high-end adversary, with 49 USC 114(r) and [redacted] chance of a successful attack. For a low-end adversary, the chance of a successful attack is reduced to 49 USC 114(r) and [redacted] a relative reduction of only (S) 9% from the baseline. This alternative is the most costly and has the lowest reduction in attack success; therefore, SPD is the least cost effective countermeasure.

49 USC 114(r) and 49 CFR 1520 [redacted]

(U) The potential range of damage prevented by AIT is significant compared to the lifecycle cost of the AIT

(U/SSI) This study analyzes the lifecycle cost of Alternative 1 (AIT) for all performance forecast to the potential damage of one to thirteen attacks, using the following attack types:

49 USC 114(r) and 49 CFR 1520 [redacted]

~~(S)~~

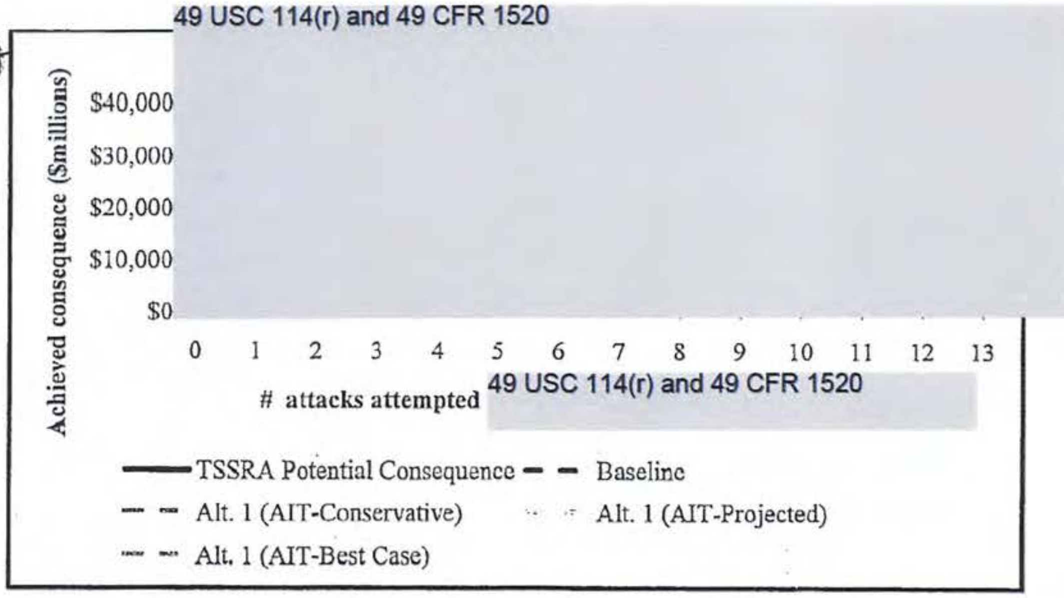


Figure 4: Achieved consequence comparison between baseline and Alternative 1 (AIT) for all performance forecasts for the <u>low-end adversary</u>. The further the distance from the TSSRA Potential Consequence curve, the better the payoff.

~~(S)~~

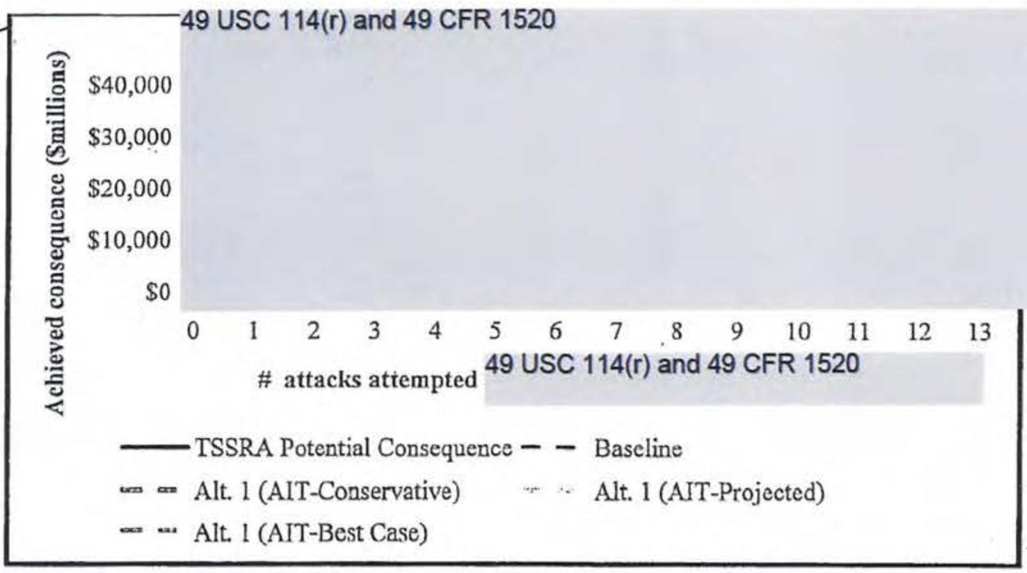


Figure 5: Achieved consequence comparison between baseline and Alternative 1 (AIT) for all performance forecasts for the <u>high-end adversary</u>. The further the distance from the TSSRA Potential Consequence curve, the better the payoff.

49 USC 114(r) and 49 CFR 1520

~~(S)~~

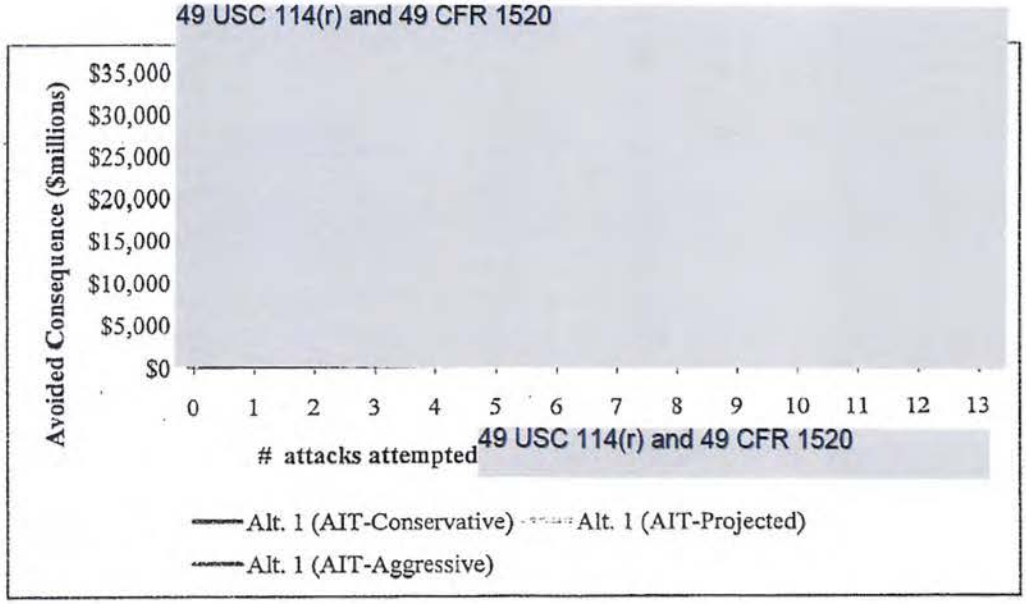


Figure 6: Consequence avoided between baseline and Alternative 1 (AIT) vs. AIT 13-Year Lifecycle Cost for the <u>low-end adversary</u>

~~(S)~~

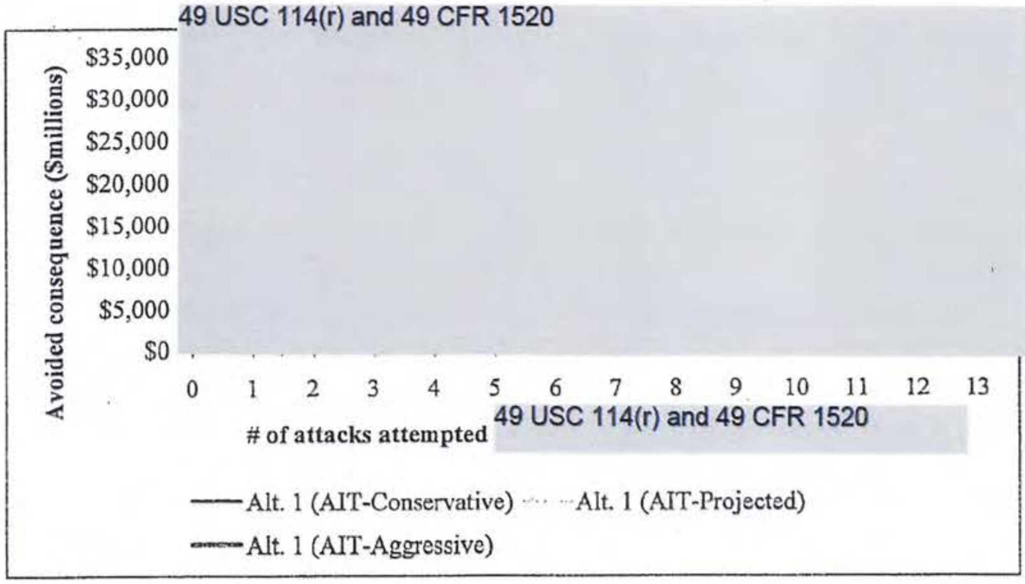


Figure 7: Consequence avoided between baseline and Alternative 1 (AIT) vs. AIT 13-Year Lifecycle Cost for the <u>high-end adversary</u>

49 USC 114(r) and 49 CFR 1520

[redacted]

49 USC 114(r) and 49 CFR 1520

(U) Appendix A: Definitions

(U) Risk

(U) Risk is defined as achieved consequences.

(U) Actual Attack Success Reduction

(U) Actual success percent figures represent the actual reduction in attack success when compared to the baseline with the same weapon and adversary type.

$$\text{Actual Success Reduction} = \text{Baseline Attack Success \%} - \text{Alternative Attack Success \%}$$

(U) Relative Reduction in Attack Success

~~(S)~~Relative reduction in attack success is needed to show the change in attack success from the baseline. This is due to the variation in the baseline attack success numbers between attack types, as well as adversary types. For example, the baseline probability of a low-end attacker completely succeeding with a body-bomb in the sensitive area is 49 USC 114(r) and while the same attack carried out by the low-end attacker has a 49 USC 114(r) chance of success when AIT is implemented. This yields a 49 USC 114(r) relative reduction in attack success.

$$\text{Relative Reduction in Attack Success} = \frac{\text{Baseline Attack Success \%} - \text{Alternative Attack Success \%}}{\text{Baseline Attack Success \%}}$$

(U) Achieved Consequence

(U) Achieved consequence is the value used in this analysis to measure risk. It is a function of potential damage (direct deaths, direct costs, and indirect costs) and the probability of attack success. TSSRA methodology is used to calculate the potential damage and RMAT data is used to determine the probability of attack success.

$$\text{Achieved Consequence} = [F(\text{Deaths}, \text{Direct Costs}, \text{Indirect Costs})] * P_{\text{attack success}}$$

(U) Avoided Consequence

(U) Avoided consequence is the monetized change in attack success after deploying a countermeasure. The probability of the baseline attack success can change after closing vulnerability gaps. The goal is to deploy better countermeasures to reduce the likelihood that the adversary will be successful. The greater the avoided consequence, the greater reduction of attack success.

$$\text{Avoided Consequence} = \text{Baseline Achieved Consequence} - \text{Countermeasure Achieved Consequence}$$

(U) The relative attack success calculation eliminates the differences between baseline success outcomes for the various attack types.

(U) Appendix B: Exposure

(U) Exposure calculations

(U) An adversary's chance of exposure to a countermeasure is instrumental in determining its overall effectiveness. Exposure rate is the probability that an adversary will be exposed to the countermeasure. For a low-end adversary, their chance of encountering an AIT is roughly equivalent to the percentage of traffic screened by the countermeasure. This is due to the low-end adversary's inability to explicitly avoid AIT screening. For a high-end adversary, their chance of encountering an AIT is near zero until full deployment due to their knowledge of the aviation system and ability to avoid countermeasures that are relatively static and not fully deployed. Due to the complex airport traffic patterns and the variation in screening percentages between different configurations of AIT machines, an approximation for the traffic flowing through was calculated in order to determine exposure.

(U) Further, in order to determine the effectiveness of a deployment it is important to be able to forecast changes in exposure caused by changes in configuration assumptions. For instance, in the case of the AIT deployment, assumptions about future improvements in AT and AIT throughput are also explored. This is why this exposure analysis is necessary and not just a simple download of existing OSO's Performance Management Information System (PMIS)[12] data on throughput.

(U) Step 1: Assumptions

(U) Traffic flows were derived from a combination of actual throughput from OSO's Performance Information Management System (PIMS) and assumed AIT deployment and traffic patterns. Since airport traffic is not consistent across all lanes in an airport, or even all lanes within a category of airports, traffic screened is not directly proportional to the number of lanes equipped with AIT. There are also size restrictions on AIT deployments in the first two years, so any lanes smaller than 12' are unable to have an AIT deployed to them initially. This size restriction results in not all lanes are able to handle AIT machines until the third year, when it is expected that the WTMDs will begin to be removed from the size restricted lanes, allowing AITs to fit in the remaining lanes. With advances, in smaller CAT IV airports, reduced size AITs will be deployed to fit the unique size restrictions at those facilities.

(U) In order to calculate projected traffic flow and adversary exposure to AIT, assumptions had to be made in order to account for new lane designs, traffic patterns, and projected SOP changes. The following assumptions were made:

1. The highest traffic lanes at checkpoints will receive AITs first, if they cannot fit AITs, then traffic would be shifted to lanes with AIT.

[12] PMIS collects and analyzes airport operational data, including the number of passengers screened by each machine at all the airports across the USA.

2. AIT lanes will be the first to open and last to close, meaning they would be the lanes that are open the longest at a given checkpoint.
3. Traffic flow per lane in each checkpoint is similar in each of the five categories of airports.
4. 2-1 configured lanes have an exposure rate proportional to maximum capacity. For example, a 2-1 lane set with an AIT machine that has 150 passenger per hour throughput has 50% exposure rate to AIT (150/300 = 50%).
5. 2-2 and 1-1 lanes have 100% exposure rate to AIT.

(U) The throughput and AIT deployment numbers used for the conservative performance forecast calculations can be seen in Table 5 below.

(U)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
Total lanes	2,130	2,155	2,180	2,204	2,228	2,254	2,278
Cumulative AIT	500 Units	1,000 units	1,275 units	1,407 units	1,540 units	1,670 units	1,800 units
No. of lanes covered	907	1,183	2,030	2,054	2,078	2,104	2,128
WTMD in Configuration	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1
Throughput per AIT	150	150	150	150	150	150	150
Throughput per AT X-Ray	150	150	150	150	150	150	150

Table 5: AIT throughput and deployment assumptions for the conservative performance forecast

(U) Step 2: Using existing traffic data to calculate percent traffic per lane

(U) For each airport category (CAT X, CAT I, etc.), the average number of lanes per checkpoint was calculated. Then, the average traffic flows were calculated for each lane at a checkpoint using several CAT X checkpoints that were able to provide a representative view of traffic. This provided a traffic function that was used to calculate traffic per lane. For CAT X airports, this was given by the equation $y = -0.048x + 0.3$ (shown in Figure 8). This line shows that the first lane at a checkpoint gets around 30% of traffic at a checkpoint, and decreases around 5% for each additional lane until six lanes.

(U)

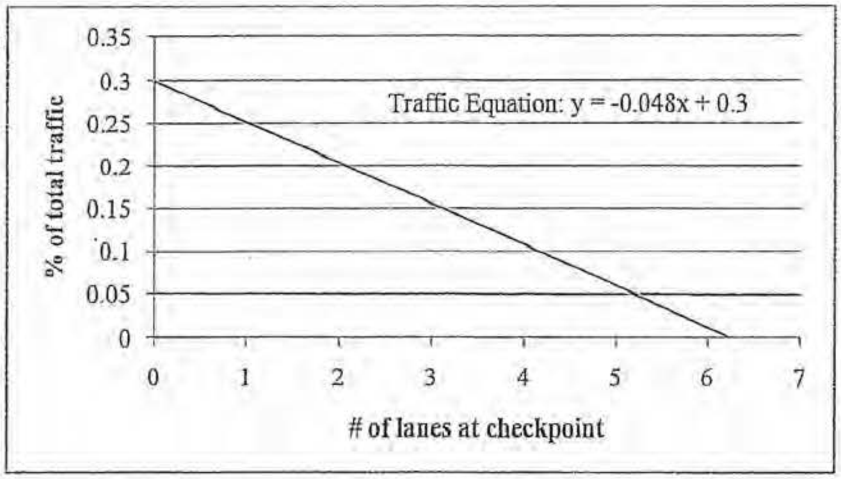


Figure 8: Traffic equation at CAT X airports

(U) Combining this traffic line with the estimated AIT deployment numbers gives the percentage of traffic covered by an AIT for each airport category over time. This leaves us with an average of 3.33 AITs per checkpoint, after considering that 2-2 lanes have full throughput, and 1-1 lanes have 100% screening but half the throughput of a two lane set, and 2-1 lanes only have 50% screening.[13] This number can be used to find the area under the curve as a percentage of the total area, shown in Figure 9.

(U) Using the traffic function, 3.33 represents 71% of the total area under the line, giving us the amount of traffic screened by AITs for year two at CAT X airports.

(U)

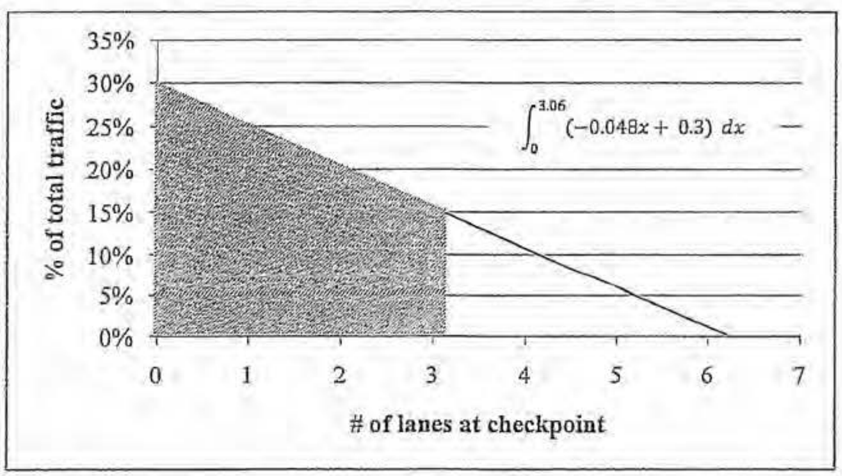


Figure 9: Traffic screened by AIT in year two at CAT X airports for conservative performance forecast

[13] Source: Exposure Calculation Spreadsheet

(U) Step 3: Determine total exposure to AIT screening

(U) Based on the estimated AIT deployment numbers, the traffic function, overall PMIS traffic, and a correction factor of 90% for CAT X lanes (due to deployments of AIT not always being at the busiest checkpoints), the total traffic covered by airport category is given by the equation below:

$$Total\ Traffic\ Covered = \%\ of\ lanes\ covered * Total\ CAT\ Traffic * Correction\ Factor$$

(U) For each of the seven years, this process was repeated for CAT X airport. The results in the following exposure rates:

U/SSI)

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
AIT Per Checkpoint	1.23	3.33	3.70	4.40	5.10	5.71	5.97
Percentage of CAT X Traffic	33%	71%	85%	92%	97%	100%	100%
Total CAT X Traffic Screened	125,190,135	274,402,538	325,004,860	354,347,023	373,830,872	383,812,617	383,812,617
Percentage of National Traffic	20%	44%	52%	56%	60%	61%	61%

Table 6: Total exposure to AIT at CAT X airports for the conservative performance forecast

(U) The process outlined above was also repeated all seven years for CAT I checkpoints. For CAT II, CAT III, and CAT IV checkpoints, it was determined that many of them were similar in size and that the traffic lines were nearly linear, so it was assumed that the amount of traffic screened by AITs was one-to-one in relation to the percentage of checkpoints that have AITs deployed. For example, deployment of AIT at 42% of checkpoints at CAT III airports (the targeted amount in year two) results in 42% of traffic screened by AIT at CAT III airports. Using this methodology for each airport category provided us with the total overall exposure based on the number of AITs deployed. The numbers for each category, as well as the total AIT coverage can be seen in Figure 10 below.

(U/SSI)

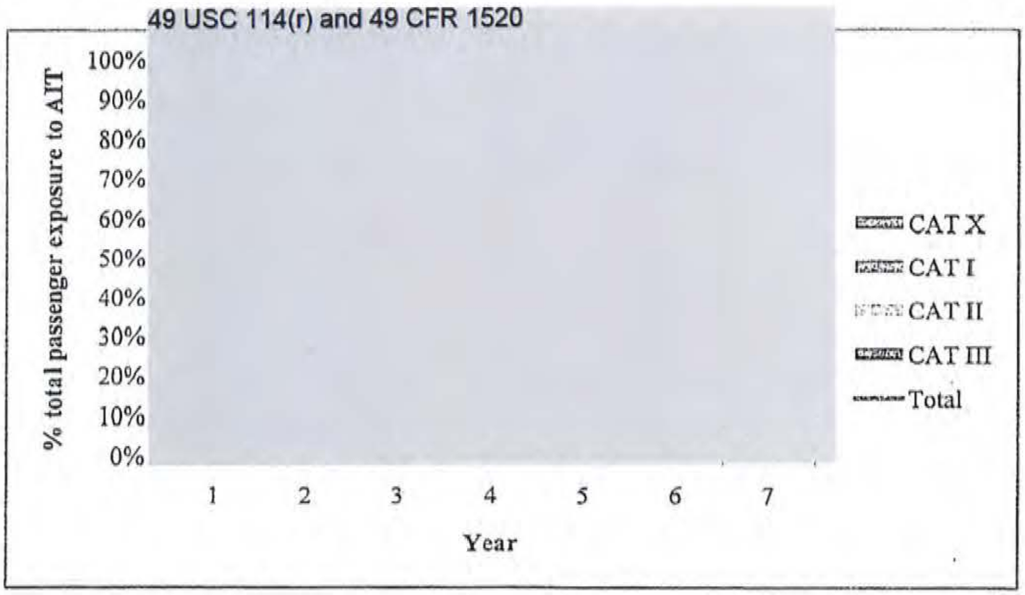


Figure 10: Total exposure to AIT by airport category for conservative performance forecast

(U/SSI)

Year	1	2	3	4	5	6	7
CAT X	49 USC 114(r) and 49 CFR 1520						
CAT I							
CAT II							
CAT III							
Total							

Table 7: Total exposure to AIT by airport category for conservative performance forecast

program decision not to include CAT IV

(U) This analysis represents throughput and traffic rates observed in the airport screening system and the deployed AITs using the conservative performance forecast. While exposure in this estimate does not hit 100% of traffic, it does come close to full coverage. *However, OST is projecting technological improvements that will increase the coverage to all lanes and checkpoints while reducing the number of purchased AITs significantly.*

(U) Step 4: Assumption changes for modified AIT throughput to 210 or 360 passengers per hour

(U) The exposure numbers calculated in the previous section reflect the conservative performance forecast to checkpoint throughput. Currently, throughput is approximately 150 passengers per hour for each AT X-Ray machine and AIT machine. However, TSA is targeting throughput improvements to 180 passengers per hour for each AT X-Ray and 210 to 360 passengers per hour for AIT machines. This improvement to a throughput of 360 passengers per hour for the AIT would allow a 2-1 AIT configuration without impacting overall checkpoint throughput. The targeted throughput rates can be seen in Table 8 and 9 for the projected and best case performance forecasts.

(U)

Item	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
Total lanes	2,130	2,155	2,180	2,204	2,228	2,254	2,278
Cumulative AIT	500 units	1,000 units	1,275 units	1,407 units	1,540 units	1,670 units	1,800 units
No. of lanes covered	907	1,183	2,030	2,054	2,078	2,136	2,278
WTMD in Configuration	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	No WTMD
Throughput per AIT	150	165	180	210	210	210	210
Throughput per AT X-Ray	150	150	165	180	180	180	180

Table 8: AIT and AT X-Ray throughput estimates for the projected performance forecast

(U)

Item	Year 1	Year 2	Year 3	Year 4
Total lanes	2,130	2,155	2,180	2,204
Cumulative AIT	500 units	1,000 units	1,275 units	1,337 units
No. of lanes covered	907	1,847	2,130	2,204
WTMD in Configuration	WTMD at lanes of 2-1	WTMD at lanes of 2-1	WTMD at lanes of 2-1	No WTMD
Throughput per AIT	150	180	240	360
Throughput per AT X-Ray	150	150	165	180

Table 9: AIT and AT X-Ray throughput estimates for the best case performance forecast

(U) For the best case performance forecast, the benefit of the increased throughput means that fewer machines would need to be purchased in order to reach full AIT deployment; therefore 100% AIT coverage is reached in year 4, 3 years earlier than with the conservative or projected performance forecast. However, when additional lanes are added to the aviation system, additional AITs will need to be purchased to maintain 100% exposure.

(U) Step 5: Determine lanes per checkpoint change and AIT exposure change caused by increased exposure

(U) For the first two years, throughput would not change at the checkpoint level; however the number of people that can be screened by AIT machines increases from 50% of traffic to 60% of traffic. In the third year, throughput at each individual checkpoint AT X-Ray machine will increase 10% and AIT throughput will increase by a third. This modifies the traffic line, increasing the slope and y-intercepts by 10%. This results in a line given by y = -0.0581x + 0.33, shown in Figure 11.

(U)

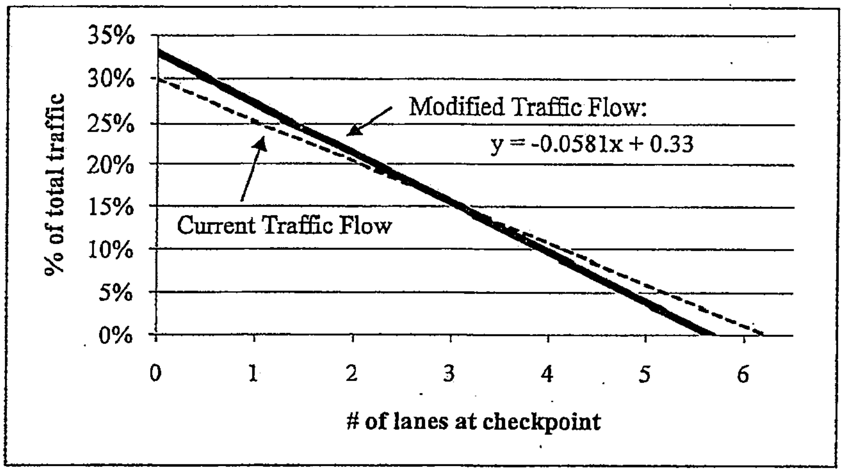


Figure 11: Modified traffic line at CAT X airports for year three

(U) Using the method outlined in the first section, along with the modified traffic line and modified AIT deployment numbers, the functional exposure rate for all four to seven years (depending on performance forecast) of AIT deployment can be determined. The functional exposure rates for CAT X traffic are outlined in Tables 10 and 11 for the projected and best case performance forecasts. The overall modified exposures for all airports are shown in Figures 12 and 13.

(U/SSI)

	Year 1	Year 2	Year 3	Year 4	Year 5	Year 6	Year 7
AIT Per Checkpoint	1.23	3.33	4.16	5.02	5.44	5.71	5.71
Percentage of CAT X Traffic	33%	71%	90%	97%	99%	100%	100%
Total CAT X Traffic Screened	125,190,135	274,402,538	345,212,236	372,223,982	379,698,770	383,812,617	383,812,617
Percentage of National Traffic	20%	44%	55%	59%	61%	61%	61%

Table 10: Exposure to AIT at increased throughput for the projected performance forecast

(U/SSI)

	Year 1	Year 2	Year 3	Year 4
AIT Per Checkpoint	1.23	3.60	4.00	N/A
Percentage of Traffic	33%	75%	91%	100%
Total CAT X Traffic Screened	125,190,135	287,926,614	350,412,989	383,812,617
Percentage of total Traffic	20%	46%	56%	61%

Table 11: Exposure to AIT at increased throughput for the best case performance forecast

(U/SSI)

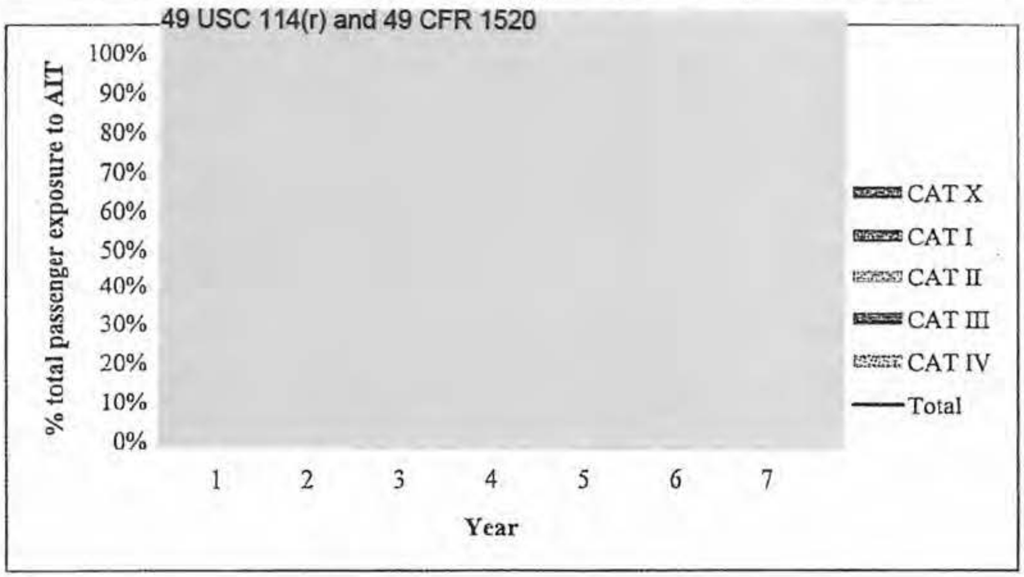


Figure 12: Exposure to AIT by airport category for projected performance forecast

~~SECRET~~

(U/SSI)

Year	1	2	3	4	5	6	7
CAT X	49 USC 114(r) and 49 CFR 1520						
CAT I							
CAT II							
CAT III							
CAT IV							
Total							

Table 12: Exposure to AIT by airport category for projected performance forecast

(U/SSI)

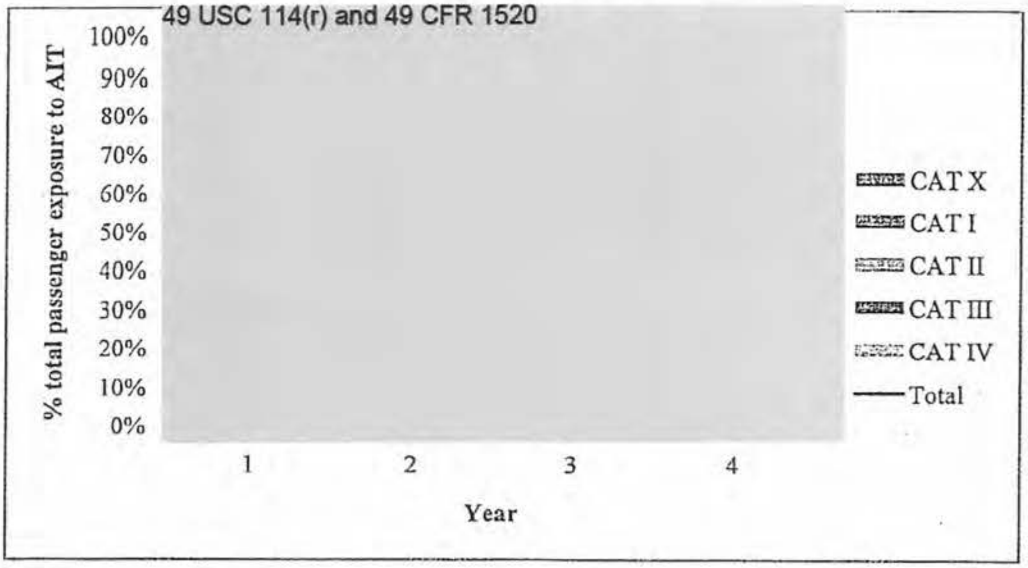


Figure 13: Exposure to AIT by airport category for projected performance forecast

(U/SSI)

Year	1	2	3	4
CAT X	49 USC 114(r) and 49 CFR 1520			
CAT I				
CAT II				
CAT III				
CAT IV				
Total				

did analysis using CAT IV because knew someone would ask why.

Table 13: Exposure to AIT by airport category for best case performance forecast

49 USC 114(r) and 49 CFR 1520

~~SECRET~~

49 USC 114(r) and 49 CFR 1520

[redacted]

(U) How Exposure Helps Drive Investment Decisions

(U) Understanding exposure directly relates to the effectiveness and risk reduction of deployed countermeasures. Each countermeasure is only as good as the amount of people that it can screen. Using the percentage of traffic screened in combination with RMAT, risk reduction can be determined to drive risk-based decisions.

(U) The exposure calculations can also help decision makers decide between multiple options. For this CBA, exposure using the conservative throughput and 1,800 AIT machines would top out a 49 USC [redacted] exposure. However, if money is invested into higher throughput AIT machines, 100% of traffic would be screened by year four with a much smaller number of machines (if the best case performance forecast is feasible).

(U) Appendix C: Risk Management Analysis Tool (RMAT)

(U) The RMAT model includes the following components:

- The aviation security system, utilizing all relevant and available system performance and vulnerability data
- Airplane vulnerability information based on the best available industry knowledge
- Simulated adversary agents modeled on the best available threat and intelligence inputs Agents include low-skill adversaries and high-skill adversaries
- A set of adversary scenarios which define mission, tactics, and resources for the adversary based on threat and intelligence inputs
- Proposed countermeasures and their expected performance based on the latest available laboratory and operational data
- An econometric model developed by the U.S. Commercial Aviation Partnership (USCAP) which estimates economic impacts to the aviation industry

(U) RMAT simulates both high and low skilled adversaries to account for the heterogeneous nature and differing capabilities of aviation terrorists. A high-skilled adversary is capable of conducting surveillance to exploit gaps in countermeasure coverage in the system. A low-skilled adversary is indifferent to countermeasure coverage and seeks the most convenient path to complete his mission. Phases of an individual simulation run include basic adversary learning, resource acquisition, basic tactical adjustment, and attack execution.

(U) RMAT executes between 200 and 300 Monte-Carlo simulation runs of adversary attacks to characterize the baseline system performance. The Monte-Carlo cycles allow the simulation to isolate the most likely adversary behavior given the scenario constraints and component performance uncertainties. The key metrics of aviation security system performance for each run are 1) *full and partial attack success expressed as a percentage* and 2) *achieved consequences consisting of deaths, direct damage, and indirect economic damage to the aviation industry*. A defined countermeasure is then introduced into the model (e.g., the Tier 2, 2 weight) as an addition to the aviation security system. RMAT then re-runs the same adversary scenarios against the updated aviation security system with the new countermeasures. The same parameters are then used to gage the new system performance. The differences in attack success and achieved consequences between baseline and alternative countermeasure implementations are used to gauge the risk-reduction effectiveness. Figure 5.0 below provides an overview of how the entire Risk Management Analysis Process (RMAP) is executed. RMAT supports the simulation phase shown.

(U/SSI)

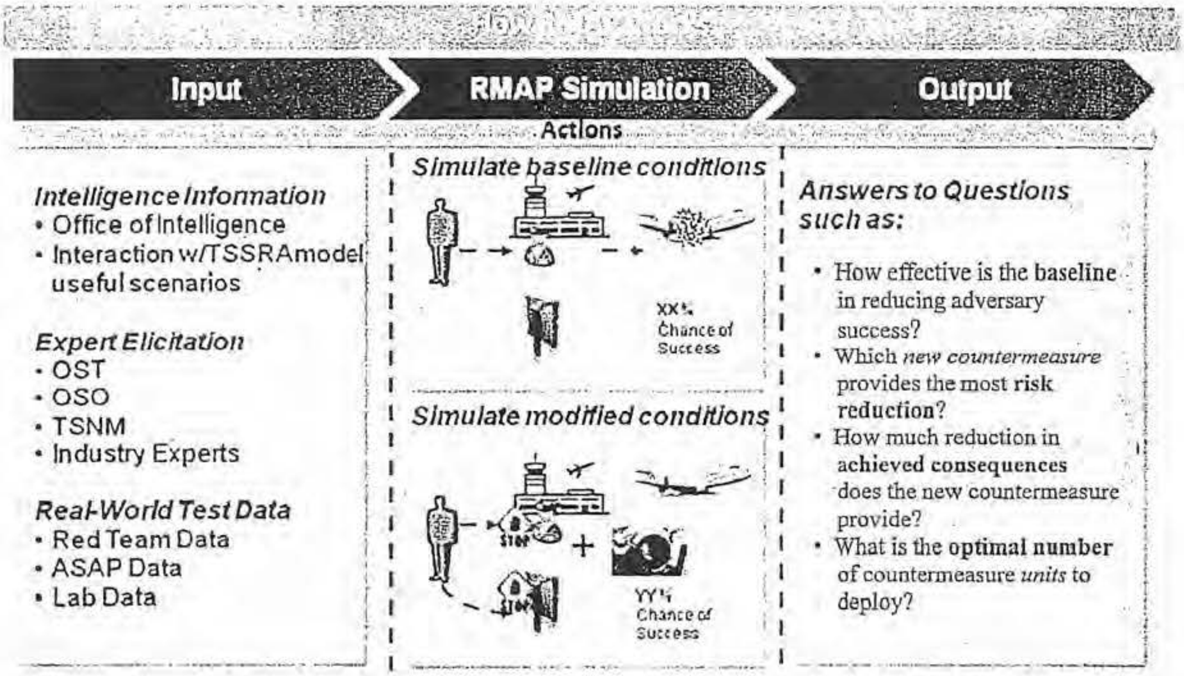


Figure 14: How RMAP Works

(U) Currently, RMAT does not explicitly take into account tactical deterrence or "threat-shifting" effects of countermeasures due to the extreme difficulty of quantitatively estimating this effect. TSA defines "threat-shifting" as 'a response of adaptive adversaries to perceived countermeasures or obstructions, in which the adversaries change some characteristic of their intent to do harm in order to avoid or overcome the countermeasure or obstacle.' TSA has proposed that this definition be entered into the DHS Risk Lexicon.

(U) Appendix D: RMAT and TSSRA Comparison

(U) TSA has two complimentary risk analysis processes, RMAT and the Transportation Sector Security Risk Assessment (TSSRA). TSSRA is a broad, high-level "strategic" risk assessment whose primary or initial purpose is to establish a terrorism risk "baseline" or "landscape" across all modes of transportation (within TSA's responsibility). The output of TSSRA is a risk "landscape" used to identify where further near-term attention is warranted. In contrast, RMAT is a simulation computer model which produces a higher-fidelity view of a narrower baseline covering more-detailed risk issues in commercial aviation. It is particularly designed to enable comparative assessment of specific prospective countermeasures against this baseline. RMAT's greater detail and computer power allows for much more detailed and higher-fidelity exploration of specific countermeasure and system performance than would be possible for TSSRA. It's important to distinguish these differences because TSSRA and RMAP serve different purposes and present different ways of looking at a scenario.

(U) How do TSSRA and RMAT work together? First, TSSRA's broad, high level approach is complimentary to RMAT's growing, but narrow focus on commercial aviation. Within this construct, TSSRA can provide valuable input (along with other criteria) as to where RMAT grows next. More concretely, RMAT uses TSSRA as a guide to determine what should be modeled and analyzed. Conversely, TSSRA uses RMAT as a way of validating TSSRA scenario risk estimates.

(U)

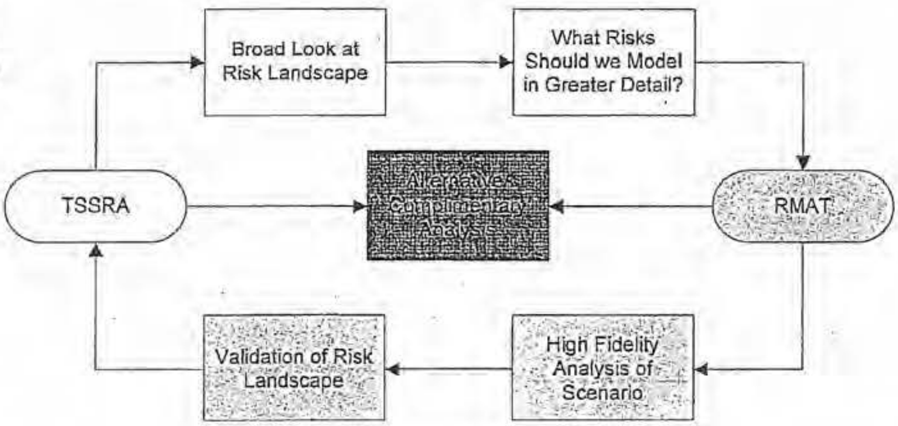


Figure 15: RMAT and TSSRA Comparison

(U) In this CBA document, the risk analysis team used the TSSRA consequence calculations for body bombs. TSSRA estimates national level consequences while RMAP estimates aviation domain consequences only. RMAP consequences are essentially a subset of the TSSRA consequences. TSSRA and RMAP produce comparable results when assumptions are itemized and accounted for. Both TSSRA and RMAP will be integrating their consequence analysis into one process that will continue to show the domain and national level consequences.

(U) Appendix E: Threat-shifting

(U) Threat-shifting occurs when an adversary alters their attack by shifting elements of their plan in some way. HSSAI's report on threat-shifting, *Assessing the Threat of Shifting Effects of Aviation Security Measures on Terrorist Behaviors*, explains that "shifting may include delaying the attack, switching the target, allocating more or different resources, or changing the weapon and/or tactic of the attack."[14] When an adversary is motivated to devise ways of overcoming security measures to carry out an attack rather than abandoning the attack altogether, threat-shifting may occur. Therefore, whenever new countermeasure technology is implemented, TSA must realize that closing a capability gap in one area of aviation security may cause the adversary to shift to a more attractive threat scenario. The figure below visually explains possible threat-shifting effects of security measures.[15]

(U/SSI)

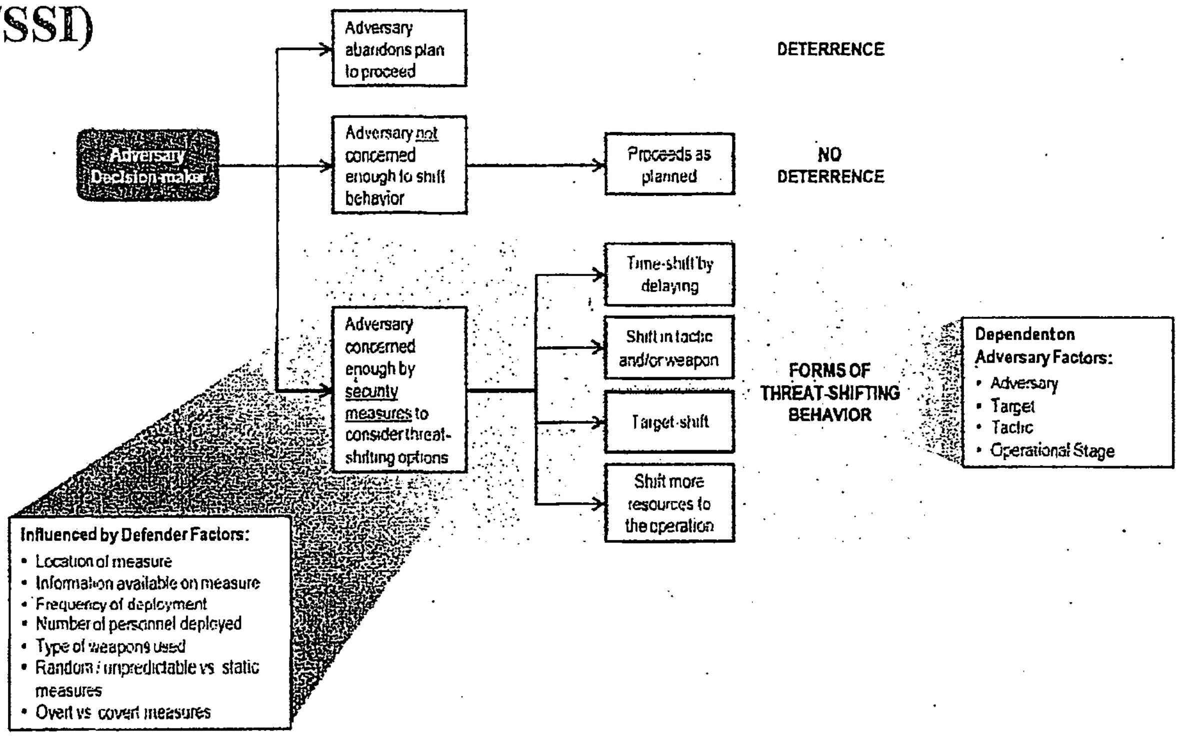


Figure 16: Threat-shifting effects of security measures

---

[14] Homeland Security Studies and Analysis Institute. (September 17, 2010). *Assessing the Threat of Shifting Effects of Aviation Security Measures on Terrorist Behaviors.* P. 1

[15] Homeland Security Studies and Analysis Institute. (September 17, 2010). *Assessing the Threat of Shifting Effects of Aviation Security Measures on Terrorist Behaviors.* P. 70

(U) For example, once all checkpoints have AIT machines, a body- bomb may no longer be the most attractive attack path, causing the adversary to shift to another threat type, as shown in Figures 17 and 18. It is important to note that the adversary may shift to an attack path that has potentially high consequences and high vulnerability (i.e. an RPG attack). Since TSA cannot predict what the adversary will do, a least regrets strategy should be considered. An example of a least regrets strategy could include developing technologies that address cross-threat capabilities.

(U)

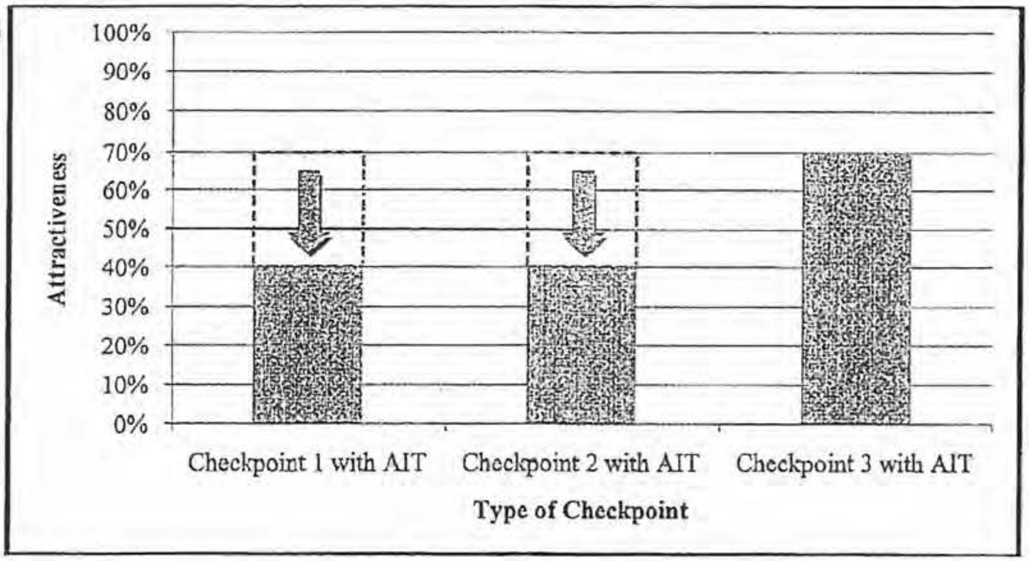


Figure 17: Notional threat-shifting during implementation of AIT by checkpoint type

(U)

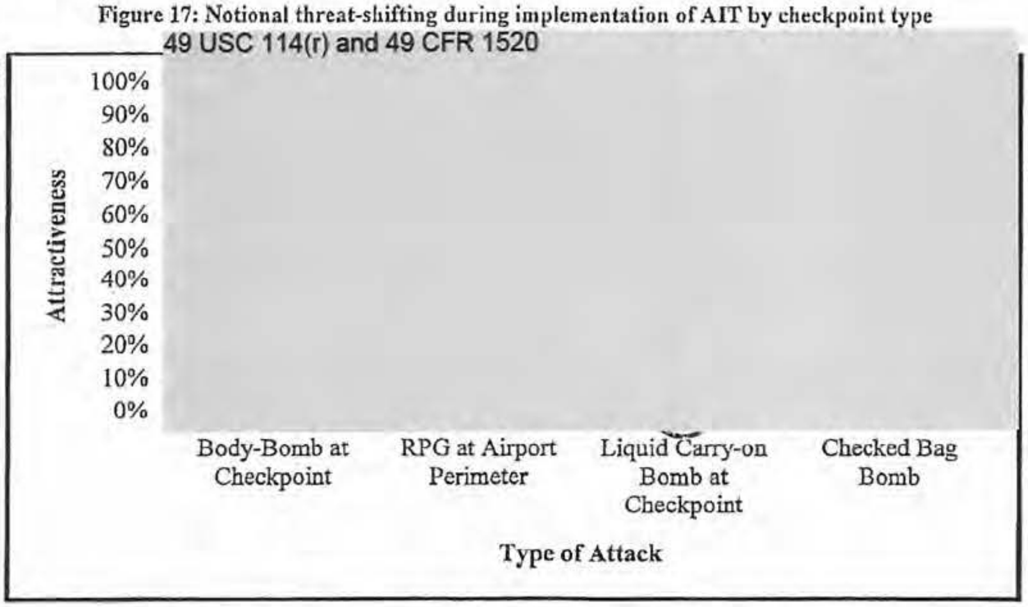


Figure 18: Notional threat-shifting after implementation of AIT

Glossary

AIT	Advanced Imaging Technology
ATR	Automatic Target Recognition
FAA	Federal Aviation Administration
HME	Home Made Explosive
ETP	Explosives Trace Portal
IEEE	Institute of Electrical and Electronics Engineers
IO	Image Operator
LCCE	Life Cycle Cost Estimate
MMW	Millimeter Wave
NCRP	National Council on Radiation Protection
OSO	Office of Security Operations
OST	Office of Security Technology
OT&E	Operational Test and Evaluation
P_d	Probability of Detection
P_{fa}	Probability of False Alarm
PIA	Privacy Impact Assessment
PMIS	Performance Management Information System
QT&E	Qualification Test and Evaluation
RACD	Risk Analysis Capability and Design
RMAT	Risk Management Analysis Tool
RFI	Radio Frequency Interference
SBS	Standard Body Search
SPD	Standard Pat-Down Procedure
SO	System Operator
SOP	Standard Operating Procedure
TSO	Transportation Security Officer
WMTD	Walk Through Metal Detector