



**November 20, 2015
1:00 p.m. – 3:30 p.m.
601 South 12th Street
Arlington, VA 22202**

Meeting Minutes

Summary

The purpose of the Aviation Security Advisory Committee's (ASAC) Annual Public Meeting was to summarize 2015 accomplishments and discuss the agenda for 2016. The committee was updated on the implementation status of the Airport Access Control Report. It also received updates from all subcommittees. Congressional bills effecting TSA and ASAC were discussed. Public attendees were given the opportunity to provide remarks. Attachment A is the agenda for the meeting.

Meeting Comes to Order

Dean Walter, the ASAC Designated Federal Officer (DFO), called the meeting to order. This meeting was convened pursuant to a Federal Register Notice dated November 5, 2015. The meeting was open to the public, fulfilling the requirements of 49 U.S.C. 44946(c)(4)(B).

Opening Remarks

TSA Executive Sponsor, Victoria Newhouse; ASAC Chairman, Steve Alterman; and ASAC Vice-Chairman, Ken Dunlap each made brief opening remarks, and welcomed new ASAC members: Major Lane Hagin of the Atlanta Police Department, Airport Precinct, representing the Airport Law Enforcement Agencies Network; and Anthony Graziano of the United Brotherhood of Carpenters (UBC). The Chairman also informed the group that Administrator Peter Neffenger and Deputy Administrator Mark Hatfield could not attend the meeting.

Roll Call and Member Remarks

A roll call was taken during the committee member introductions. Members were given an opportunity for remarks. Anthony Graziano provided an overview of UBC and how it could assist ASAC. Chris Witkowski proposed that the committee look at vulnerabilities related to aircraft onboard communications and data transmission. TSA will consider providing a briefing on this issue at a future meeting.

Review of 2015 Recommendations

Dean Walter provided a summary of the recommendations approved by the committee this year. 2015 was a very active year for the Committee, which approved and submitted 39 recommendations to improve aviation security to the Administrator. These consist of the following:

- 6 Air Cargo Recommendations, approved February 2, 2015, and May 5, 2015
- 1 General Aviation Recommendation, approved February 17, 2015



- 28 Airport Employee Screening and Access Control Recommendations, approved April 8, 2015
- 4 Airport Perimeter Security Recommendations, approved September 2, 2015

To manage the workload, TSA developed a project management tool to track the implementation, obstacles and challenges, priorities, and milestones for each recommendation. The recommendations are prioritized based on the perceived level of risk reduction, implementation cost to TSA, and timeframe.

Update on implementing the Airport Access Control Report

Ken Dunlap, who served as the Chairman of the Airport Access Control Working Group, provided a status summary on the 28 recommendations from the Airport Access Control Report. Several recommendations are completed, but most are ongoing.

The Working Group reconvened on November 9, 2015, to evaluate progress. The members reviewed the implementation plan and status for each recommendation, and grouped them into three categories (Expectations Met/On Track; Additional Work/Information Required; and Expectation Not Met) to assist deliberations during the next meeting. In general, there are four areas where the Working Group would like to reengage with TSA: 1) Playbook coordination with airport operators; 2) Information Circular/Security Directive impact; 3) Rap-Back program status; and 4) national employee database status.

A full project review is scheduled for December 15, 2015, where project managers will discuss the implementation approach and status with the Working Group. The Working Group will also look to prioritize the remaining recommendations.

A full project review is scheduled for December 15, 2015, where project managers will discuss the implementation approach and status with the Working Group. The Working Group will look to prioritize the remaining recommendations.

Subcommittee Updates

The co-chairpersons for each subcommittee provided an update, covering progress to date and focus areas going forward. A new subcommittee was formed to look at Security Technology issues. There are now a total of five subcommittees.

New committee members were encouraged to join any subcommittees that align with their interests.

International Aviation Subcommittee Update

The co-chairmen noted that the Subcommittee did not have any new topics for action. However, discussions continue on efforts to mitigate the inbound threat to the United States. The following priorities were established for 2016: 1) focus efforts to mitigate the inbound threat to the United States; 2) expand recognition of trusted traveler programs (where applicable); 3) coordination of



international technology standards for screening and detection equipment and; 4) international air cargo security. The Subcommittee will also provide international input and collaborate with the other subcommittees (Air Cargo, Commercial Airports, and Security Technology) on any common initiatives or topics.

General Aviation (GA) Subcommittee Update

The co-chairmen reported that the subcommittee has made significant progress developing a proposed rewrite of 49CFR1552 regarding vetting of foreign nationals for flight screening. This is a tentative agenda item for the next ASAC meeting.

The co-chairmen discussed the armed security officer requirement in the Ronald Reagan Washington National Airport (DCA) Access Standard Security Program (DASSP). TSA briefed this issue to ASAC, which concurred with TSA's recommendation to remove the requirement, at the February 17, 2015, ASAC meeting. TSA will continue to work with other government agencies regarding the necessary concurrences and is also in the process of briefing the issue to the new TSA Administrator.

One committee member asked the Subcommittee to consider looking at Temporary Flight Restriction procedures.

Air Cargo Subcommittee Updates

The co-chairpersons reported that the Subcommittee met multiple times in 2015. The focus of 2016 will be to implement the recommendations that were approved in 2015. The group will also continue to consider changes to the Air Cargo Advanced Screening Program. Mutual recognition of security practices with international partners is an area of interest. Air Cargo Security Research & Development Working Group will be active in 2016. Its relationship to the newly formed Security Technology Subcommittee needs to be determined.

A subcommittee teleconference is scheduled for the near future.

Commercial Airports Subcommittee Update

The co-chairman reflected that four recommendations on Perimeter Security were approved at the September 2, 2015, ASAC meeting. The Subcommittee is now working with TSA on implementation. No additional meetings are scheduled at this point since much of this work overlaps with the Airport Access Control Working Group.

Security Technology Subcommittee Update

This Subcommittee is still in the formative stages. One teleconference call was held in November to discuss a preliminary framework. An in-person meeting is scheduled for January 21, 2016. The group's initial focus is to review TSA's Strategic Five-Year Technology Investment Plan for Aviation Security. The group will also look at technical standards and requirements for passenger baggage, and potentially cargo screening. There is also interest in looking at innovative airport security



technologies. Finally, the relationship of this Subcommittee to the others will be established over the next year.

2016 Committee Agenda

The following 2016 full Committee meetings are scheduled:

- Tuesday, February 2, 10:00 A.M. - 4:00 P.M.
- Tuesday, May 10, 1:00 P.M. - 4:00 P.M.
- September (TBD)
- December - Annual Public meeting (TBD)

Legislative Update

Committee members were updated on the following pieces of legislation that may affect the aviation industry:

- H.R. 2843 - TSA PreCheck Expansion Act, was passed by the House with a goal of increasing the traveling public's enrollment options.
- H.R. 3102 - Airport Access Control Security Improvement Act of 2015, was passed by the U.S. House Subcommittee on Aviation. This bill focuses on insider threat and airport employee screening. This bill would mandate several parts of the Airport Access Control Report.

Members were encouraged to stay informed of the activities of Congress, as each bill has an ASAC component.

Public Comment Period

Dean Walter opened the public comment period for statements. He stated that members of the public were asked to make advance arrangements to present oral statements at this meeting. Douglas Kidd, Executive Director of the National Association of Airline Passengers (NAAP), requested an opportunity to speak. Mr. Walter mentioned that he reserves the right to limit time for comments and Mr. Kidd would have three minutes to make a statement. If he could not finish his comments in the time allotted, he could submit comments to Mr. Walter or on the docket, and they will become part of the official record.

Mr. Kidd provided a report (Attachment C) on his organization's dissatisfaction with the ASAC Airport Access Control Report. He discussed the ASAC Report's deficiencies, and provided NAAP recommendations for improving airport security and the passenger experience. NAAP's position is that the same standards of security should apply to all who enter airport facilities, whether they are passengers, security personnel, or airport and airline employees. In order to be effective, airport security policies and procedures should, at all times, be reasonable, consistent, and uniform, and carried out with the highest degree of integrity and professional care. Other concerns included baggage theft, drug smuggling, weapons smuggling, and other criminal activity. The ASAC Report



did not cover management/leadership oversight, employee corruption. Mr. Kidd emphasized the importance of 100% screening at airports including TSA employees going in and out of airports.

Mr. Walter thanked Mr. Kidd for his comments and stated that they would be included in the official record of the meeting.

Administrative Discussion

Mr. Alterman noted that the next ASAC meeting is scheduled for Tuesday, February 2, 2016, from 10:00 a.m.-4:00 p.m., and will include a working lunch. The Agenda for this meeting is in-process. Suggestions for agenda items can be sent to Dean Walter.

Adjournment

Mr. Alterman asked for any last comments, and with none received, adjourned the meeting at approximately 3:20 p.m.

Summary of Action Items:

- Re-establish monthly Subcommittee Co-Chairs calls to share information and ensure consistency in work plans (Walter)
- Research advisory committees at other agencies who may be participating in similar or overlapping activities (Walter)
- Distribute, prior to the February 2016 meeting, a draft of the required Aviation Security Stakeholder Participation Act Annual Report (Walter)
- Request an SSI-level intelligence briefing (Walter)

Certification of Detailed Minutes

I hereby certify that this is an accurate record of the activities of the Aviation Security Advisory Committee on November 20, 2015.

A handwritten signature in black ink that reads "Stephen A. Alterman". The signature is written in a cursive style and is positioned above a horizontal line.

Stephen A. Alterman
Chairman



Attachment A: Meeting Agenda

1. Review of 2015 Recommendations
2. Status update on implementing the Airport Access Control Report
3. Subcommittee:
 - a. International Aviation – Status Update
 - b. General Aviation – Status Update
 - c. Air Cargo – Status Update
 - d. Commercial Airports – Status Update
 - e. Security Technology – Status Update
4. Discussion of 2016 Committee Agenda
5. Legislative Update
 - a. H.R. 2843, TSA PreCheck Expansion Act
 - b. H.R. 3102, Airport Access Control Security Improvement Act of 2015
6. Public comment period
7. Administrative discussion
8. Closing comments and adjournment



Attachment B: Meeting Attendees

Name	Organization	Status
Steve Alterman	CAA	Chair
Alan Black	DFW	Member
Scott Broyles	National Safe Skies Alliance	Member
Colleen Chamberlain	AAAE	Member
Joe Dalton	NetJets	Member
Joe DePete	ALPA	Member
Ken Dunlap	IATA	Vice-Chair
Daniel Fisher	ARSA	Member
Brandon Fried	AfA	Member
Tony Graziano	UBC	Member
Jillian M. Gustafson	NADA	Member
Lane Hagin	ALEAN	Member
Jens Hennig	GAMA	Member
Lorraine Howerton	USTRavel	Member
Glenn Johnson	VPAF103	Member
Kenneth Mortensen	Privacy	Member
Susan Presti	TIACA	Member
Craig Spence	AOPA	Member
Eric Thacker	A4A	Member
Chris Witkowski	AFA-CWA	Member
Victoria Newhouse	TSA Executive Sponsor	Federal
Kevin Knott	DHS/TSA	Federal
Marc Rossi	DHS/TSA	Federal
Craig Lynes	DHS/TSA	Federal
Keith Goll	DHS/TSA	Federal
Dean Walter	DFO	Federal
Bob Vogt	DHS/TSA	Federal
Karin Glasgow	DHS/TSA	Federal
Thomas Friedman	DHS/TSA	Federal
Dan Berdych	DFW Airport	Public



Name	Organization	Status
Sean Cusson	ACI-NA	Public
Maryanne DeMarco	CAPA	Public
Lauren Lacey Haertlein	GAMA	Public
Stephen Holl	MWAA	Public
Douglas Kidd	NAAP	Public
Kathy Lawton	DFW Airport	Public
Dawn Lucini	Telos ID	Public
Phillip Mongeau	DFW Airport	Public
Mike Mullen	EAA	Public
Alex Psilakis	Monument Policy Group	Public
Sarah Wolf	NBAA	Public



Attachment C: Public Comment

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS - A Review of the Final Report of the Aviation Security Advisory Committee's Working Group on Airport Access Control

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

866-869-2500

www.right2fly.org

By Hand

November 20, 2015

Office of the Administrator
Transportation Security Administration
601 South 12th Street
Arlington, VA 20598

Dear Sir,

We have reviewed the FINAL REPORT OF THE AVIATION SECURITY ADVISORY COMMITTEE'S WORKING GROUP ON AIRPORT ACCESS CONTROL. We believe it is our duty to take issue with this report, to call to your attention its deficiencies, and to make our own recommendations for improving airport security, and the passenger experience.

It is our position that the same standards of security should apply to all who use airport facilities, be they passengers, security personnel, or airport and airline employees. As the recent case of gun smuggling illustrated so vividly, it is pointless and of little value to set aside the concourse and gate areas as "sterile"; and then to allow airport and/or security employees, *with their bags*, to enter into these areas with no screening at all. I have personally witnessed this.

Our association respectfully submits that in order to be effective, airport security policies and procedures should, at all times, be *reasonable, consistent, and uniform*, and carried out with the highest degree of integrity and professional care. This has not always been the case; and we are hopeful that you will take matters in hand for the sake of passengers, employees, and the nation at large.

We are enclosing with this letter our review of the ASAC report noted above, as well as our report as a member of ASAC's Passenger Advocacy Subcommittee, together with other material that we believe to be relevant. Please feel free to contact us directly or through your staff.

Sincerely,

Douglas Kidd
Executive Director

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

The National Association of Airline Passengers is a non-profit membership association organized in 2010 to protect the rights of airline passengers, crew, and airport personnel. It was a member of FAA's Portable Electronic Devices Aviation Rulemaking Committee and a member of ASAC's Passenger Advocacy Subcommittee in 2013. On October 6, 2015, it sponsored *a Symposium on Airport Security* at National Airport.

The association takes a great interest in the safety and security of passengers in general and the screening process in particular. Passengers are required to comply with TSA's security policies and submit to TSA's security procedures. Many passengers find these policies unreasonable, the procedures abusive; and their implementation haphazard and inconsistent. TSA's attitude toward passenger compliance is strict; even an inadvertent breach of the security checkpoint (by a passenger) can cause the airport to go into lockdown, delay countless flights, and result in passengers being ordered off an aircraft at gunpoint.¹

In contrast to the strict security procedures applied to passengers, airport and TSA employees operate on what may best be described as an "honor system"², entering and leaving secure and sterile areas, with their bags, with no screening at all, subject only to an occasional spot check.³

¹ **Paramilitary Police in Miami Force Passengers to Leave Plane at Gunpoint**, <http://www.globalresearch.ca/paramilitary-police-in-miami-force-passengers-to-leave-plane-at-gunpoint/5488214> , <http://www.miamiherald.com/news/local/community/miami-dade/article44080464.html>

² a system (as at a college) whereby persons are trusted to abide by the regulations (as for a code of conduct) without supervision or surveillance <http://www.merriam-webster.com/dictionary/honor%20system>

³ An inspection or investigation that is carried out at random or limited to a few instances. <http://www.thefreedictionary.com/spot-check>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Not surprisingly, this arrangement is subject to widespread abuse, and has allowed baggage theft⁴, drug smuggling⁵, weapons smuggling⁶, and other criminal activity⁷ to flourish at airports. Even TSA employees⁸ have been drawn into these activities.⁹

The recent case of gun smuggling at Hartsfield-Jackson Atlanta International Airport that prompted TSA's review of its procedures was not the first or only case of smuggling at US airports under TSA supervision. The resulting publicity, however, was sufficiently embarrassing to TSA that it turned to the Aviation Security Advisory Committee (ASAC) for "assistance with reevaluating airport employee screening in light of the discovery of an alleged weapons smuggling operation at a major airport that used passenger airliners to transport the contraband." The advisory committee was asked to identify new security measures for industry employees to address potential vulnerabilities related to the sterile areas¹⁰ of US airports.

⁴ <http://www.usatoday.com/story/todayinthesky/2014/03/27/busted-police-allege-lax-theft-ring-stole-from-fliers-bags/6949949/>

⁵ "46 people indicted in drug-smuggling bust at Dallas-Fort Worth airport"
https://www.washingtonpost.com/local/trafficandcommuting/undercover-sting-snags-would-be-airline-drug-smugglers-at-dallas-fort-worth/2015/07/15/4d016a0e-2b04-11e5-bd33-395c05608059_story.html

⁶ Two men worked together to smuggle guns and ammunition on at least 20 flights from Atlanta to New York from May to December, officials said. <http://www.cnn.com/2014/12/23/us/delta-employee-gun-smuggling/>

⁷ Syracuse airport worker made terrorist threat, said he'd 'shoot everybody,' police say
<http://www.syracuse.com/crime/index.ssf/2015/05/syracuse-airport-worker-made-terrorist-threat-said-hed-shoot-everybody-police-say.html>

⁸ NBC 5 in the Dallas-Fort Worth area reports police arrested at least two TSA officers in a sting operation involving stolen parking passes. <http://downtrend.com/james/dfw-airport-police-bust-tsa-officers-in-theft-ring>

⁹ Two former TSA employees and a former Delta worker admitted Wednesday to smuggling drugs at Atlanta's Hartsfield-Jackson International Airport.
<http://www.wsbtv.com/news/news/delta-tsa-employees-admit-smuggling-drugs-at-atlan/nJTKx/>

¹⁰ The "Sterile Area" refers to portions of an airport defined in the airport security program that provides passengers access to boarding aircraft and to which the access generally is controlled by TSA, an aircraft operator, or a foreign air carrier. See **Security Threat Assessment for SIDA and Sterile Area Workers Privacy Impact Assessment June 15, 2004**

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

In response to this request, the ASAC convened a working group (WG) composed of its members, TSA staff, and other experts to study the problems set before it, and submitted its Final Report on Airport Access Control to Acting Administrator Melvin Carraway on April 8, 2015.

The ASAC/Working Group's Report

Among other findings, the report concluded that 100 percent physical screening of airport employees was not cost-effective, and that there were significant differences in the threats posed by criminal activity and terrorism. It recommended increased “random and unpredictable” employee screening/inspection, more thorough background checks and continuous criminal activity monitoring, and better control of airport identification media and access points.

It also advocated for expanded domestic intelligence collection and better use and sharing of airport security assessment results. These recommendations were said to have been “developed within the context of Risk-Based Security (RBS).

Our Review of the Working Group's Report

Our review of the working group's report was based upon TSA's statutory mandate, its duty of care, and the principals of Risk Based Security.

http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sida_sw.pdf

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Statutory mandate:

The Transportation Security Administration was formed to undertake a number of functions, the most visible of which is the screening of passengers and their bags¹¹. In addition, the Under Secretary/Administrator is required to ensure the adequacy of security measures¹² at airports,¹³ and to correct deficiencies when discovered.¹⁴

Federal statutes do not explicitly require 100 percent physical security screening of airport employees, however, the TSA administrator is to require “...*screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport*¹⁵ ... *that will assure at least the same level of protection as will result from screening of passengers and their baggage.*”¹⁶

¹¹ 49 USC §44901(a) The Under Secretary of Transportation for Security shall provide for the screening of all passengers and property...that will be carried aboard a passenger aircraft operated by an air carrier or foreign air carrier in air transportation or intrastate air transportation.

¹² 49 USC §44903 (h) (4) Airport perimeter screening.— The Under Secretary—
(A) shall require, as soon as practicable after the date of enactment of this subsection, screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport in the United States described in section 44903 (c);
(B) shall prescribe specific requirements for such screening and inspection that will assure **at least the same level of protection as will result from screening of passengers and their baggage;**

¹³ 49 USC §114(f) Additional Duties and Powers.— In addition to carrying out the functions specified in subsections (d) and (e), the Under Secretary shall—

(11) oversee the implementation, and ensure the adequacy, of security measures at airports and other transportation facilities;

¹⁴ 49 USC §44904(e) Improving Security.— The Under Secretary shall take necessary actions to improve domestic air transportation security by correcting any deficiencies in that security discovered in the assessments, analyses, and monitoring carried out under this section.

¹⁵ 49 USC §44903 (h) (4) (A)

¹⁶ 49 USC §44903 (h) (4) (B)

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Duty of Care:¹⁷

Care is the opposite of *Negligence*, which can be defined as “The omission to do something which a reasonable man, guided by those ordinary considerations which ordinarily regulate human affairs, would do, or the doing of something which a reasonable and prudent man would not do.”

In this regard, we believe passengers and the public have a right to expect the employees of the TSA to exercise reasonable and *ordinary care*, if not *great care*, in the performance of their duties; that is, the same “*high degree of care*” which it is the duty of a carrier (airline) to exercise toward its passengers.

“Ordinary care is that degree of care which persons of ordinary care and prudence are accustomed to use and employ, under the same or similar circumstances, in order to conduct the enterprise in which they are engaged to a safe and successful termination, having due regard to the rights of others and the objects to be accomplished.”

Great care is such as persons of ordinary prudence usually exercise about affairs of their own which are of great importance; or it is that degree of care usually bestowed upon the matter in hand by the most competent, prudent, and careful persons having to do with the particular subject.

A *high degree of care* is that degree of care which a very cautious, careful, and prudent person would exercise under the same or similar circumstances, and the failure to exercise which, where required by law to do so, is negligence. It means the highest degree required where human safety is at stake, and the highest degree to the usage and practice of very careful, skillful, and diligent persons engaged in the same business by similar means or agencies.

¹⁷ See Black's Law Dictionary, Third Edition, 1933, Pages 280-281

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Risk Based Security:

Risk management is the identification, assessment, and prioritization of risks (defined in ISO 31000 as *the effect of uncertainty on objectives*) followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events.¹⁸

For the most part, these methods consist of the following elements, performed, more or less, in the following order.

1. identify, characterize threats
2. assess the vulnerability of critical assets to specific threats
3. determine the risk (i.e. the expected likelihood and consequences of specific types of attacks on specific assets)
4. identify ways to reduce those risks
5. prioritize risk reduction measures based on a strategy

The impact of the risk event is commonly assessed on a scale of 1 to 5, where 1 and 5 represent the minimum and maximum possible impact of an occurrence of a risk.

The probability of occurrence is likewise commonly assessed on a scale from 1 to 5, where 1 represents a very low probability of the risk event actually occurring while 5 represents a very high probability of occurrence. This axis may be expressed in either mathematical terms (event occurs once a year, once in ten years, once in 100 years etc.) or may be expressed in "plain English" (event has occurred here very often; event has been known to occur here; event has been known to occur in the industry etc.).

The **composite risk index** thus can take values ranging (typically) from 1 through 25, as shown below:

¹⁸ https://en.wikipedia.org/wiki/Risk_management

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

		Consequence					
		How severe could the outcomes be if the risk event occurred? →					
		1	2	3	4	5	
		Insignificant	Minor	Significant	Major	Severe	
Likelihood	↑ What's the chance the of the risk occurring?	5 Almost Certain	5 Medium	10 High	15 Very high	20 Extreme	25 Extreme
	4 Likely	4 Medium	8 Medium	12 High	16 Very high	20 Extreme	
	3 Moderate	3 Low	6 Medium	9 Medium	12 High	15 Very high	
	2 Unlikely	2 Very low	4 Low	6 Medium	8 Medium	10 High	
	1 Rare	1 Very low	2 Very low	3 Low	4 Medium	5 Medium	

Figure 1-Risk Matrix¹⁹

Ideally, risk prevention/mitigation strategies and resources are applied to those areas representing the greatest risk of loss; that is, those events that are both severe in consequence and likely in occurrence.

ISO 31000:2009 gives a list on how to deal with risk:²⁰

1. Avoiding the risk.
2. Accepting/Retaining the risk
3. Removing the risk source
4. Changing the likelihood/Changing the consequences
5. Share/Transfer the risk with/to another party or parties

¹⁹ http://www.nma.gov.au/about_us/ips/policies/collection_care_and_preservation_policy

²⁰ https://en.wikipedia.org/wiki/ISO_31000

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

A comparison of Passenger and Insider Screening

Passengers: U.S. law requires airlines operating flights to, from, or through the United States to provide the Department of Homeland Security (DHS), U.S. Customs and Border Protection (CBP), with certain passenger reservation information, called Passenger Name Record (PNR) data, primarily for purposes of preventing, detecting, investigating, and prosecuting terrorist offenses and related crimes and certain other crimes that are transnational in nature.²¹

Employees: The Transportation Security Administration has the statutory responsibility for requiring by regulation “employment investigation[s], including a criminal history record check and a review of available law enforcement data bases and records of other governmental and international agencies” for individuals who have “unescorted access” to the secure areas of airports and aircraft.²²

In addition to a name based check (similar to the PNR above) the TSA Credentialing Program Office (CPO) also conducts a *fingerprint* based checks on SIDA and Sterile Area Workers with the FBI.

At the airport, Employees and their bags may bypass security and obtain entry to the sterile area by swiping their card key and entering a code; passengers must submit to physical screening. Both passengers and employees are subject to additional “random and unpredictable” within the sterile area.

²¹ http://www.cbp.gov/sites/default/files/documents/pnr_privacy.pdf

²² http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_sida_sw.pdf

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

The similarities and differences between passenger and employee screening may be summarized as follows:

	<u>PASSENGERS</u>	<u>EMPLOYEES</u>
BACKGROUND CHECK	NO	YES
PASSENGER NAME CHECK	YES	NO?!
RANDOM SCREENING	YES	YES
MANDATORY BAGGAGE X-RAY	YES	NO
MANDATORY PHYSICAL SCREENING	YES	NO

The primary difference between the screening of passengers and employees seems to be *the substitution of the fingerprint/background check for physical screening.*

The primary difference between the screening of passengers and employees seems to be *the substitution of the fingerprint/background check for physical screening.* The working group justified this difference based on the following:²³

- The “robust nature” of employee pre screening. (fingerprint background check)

*“DHS (Department of Homeland Security) officials have told us that job applicants in the fast-food industry typically undergo a more robust background check than applicants for a TWIC card,” said Senator Mark Warner, referring to the TSA-issued Transportation Worker Identity Credential.*²⁴

- The need to apply finite aviation resources efficiently and effectively.
- The perceived difference between the threat posed by criminal activity and terrorism.

²³ <http://www.tsa.gov/sites/default/files/asac-employee-screening-working-group-04-15.pdf> (page 2)

²⁴ <http://www.infowars.com/senator-blasts-tsa-fast-food-joints-do-better-employee-background-checks/>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Problems and Shortcomings of the Working Group's Report:

As we reviewed the Working Group's report, we noted the following shortcomings:

1. The report did not recognize TSA's specific statutory duty to require *"...screening or inspection of all individuals, goods, property, vehicles, and other equipment before entry into a secured area of an airport²⁵... that will assure at least the same level of protection as will result from screening of passengers and their baggage."²⁶*
2. None of the proposed "solutions", relating to *screening and inspection, vetting of employees*, or *internal controls on airport-issued credentials*, would have stopped or prevented the gun smuggling scheme from taking place.
3. Airport employees and their bags would still be allowed to bypass security and gain entry into the "sterile" areas of the airport without being screened.
4. The report ignores the corrupting and corrosive effect of criminal activity on the integrity TSA's workforce and screening operations.²⁷
5. The report did not address the lack of employee supervision and management oversight that allowed security breaches to occur.

²⁵ 49 USC §44903 (h) (4) (A)

²⁶ 49 USC §44903 (h) (4) (B)

²⁷ [Convicted TSA Officer Reveals Secrets of Thefts at Airports](http://abcnews.go.com/Blotter/convicted-tsa-officer-reveals-secrets-thefts-airports/story?id=17339513), ABC News, Sept. 28, 2012
<http://abcnews.go.com/Blotter/convicted-tsa-officer-reveals-secrets-thefts-airports/story?id=17339513>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Our Conclusions:

Our review of the circumstances surrounding this and other security breaches leads us to the following conclusions:

1. Minimum, uniform standards for entry into the “secure/restricted” (employees only) and “sterile” areas of the airport (i.e. concourse/gate areas) are required by law and essential to create and maintain a secure environment.
2. Less than 100% screening of airport and security employees invites and encourages abuse by those who would not ordinarily be tempted.
3. Any security vulnerability that can be exploited for petty criminal enterprise can/will be exploited for larger terrorist purposes.
4. Improved background checks and random employee screening (i.e., spot checks) do not guarantee the continued trustworthiness and integrity and of an individual or a group of employees.
5. Managers and supervisors have a responsibility to insure their subordinates’ compliance with security procedures within the secure and sterile areas of the airport.
6. The assumptions used by the Working Group in the context of applying a Risk Based Security Approach Model to criminal activity were flawed, and the conclusions reached on this subject cannot and should not be relied upon.

Our Recommendations:

1. All airport employees, including TSA and local law enforcement, should be subject to screening before entry into or exit from the secure or sterile areas of the airport. (100% screening)
2. **All airport employees should be bonded.**

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

3. TSA management should take steps to ensure adequate supervision and management oversight of all airport employees.
4. Risk Based Security must be regarded as a means to an end, (adequate security) and not an end in itself, or be used to justify or rationalize unsound or inadequate security practices.
5. If risk management techniques are to be applied, TSA should contract with reputable professional firms for these services, rather than relying on advisory committee members or staff who may lack the necessary background, training, or experience in this field.
6. Criminal activity by airport or TSA employees must be regarded as serious breach of security any time it occurs, and is as much a threat to the safety and security of aircraft and passengers as terrorism.

Discussion: How could this happen?

While the Working Group's report focused on airport employee access, it must be pointed out that all of the incidents involving theft, smuggling, and other illegal activity took place under the very noses of uniformed TSA personnel, and that in more than a few cases TSA employees either "looked the other way" or were actively involved in the theft and smuggling operations themselves. One may legitimately ask: How could this happen? Where were the supervisors? Where was management? Where were the Federal Security Directors? Best practices and industry standards are of no value if there is lax, ineffective, or absent leadership and supervision.

The illegal activities within the secure/sterile areas of airports are not isolated incidents, nor the fault of "a few bad apples". They are the natural result of a lack of adequate supervision, poor management, and ultimately, a failure of leadership.

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

“Virtually every significant case of employee misconduct had warning signs that leaders either ignored or failed to recognize as important. Furthermore, leaders themselves lie at the core of both the cause and solution to corruption. Past research has repeatedly confirmed that most scandals start with one employee doing relatively small unethical acts and grows to whatever level the leadership allows.”²⁸

“What you allow, you encourage.”²⁹

It should be noted that all of this has occurred in spite of the existence of the very measures that the working group is recommending. All of the airport employees involved went through background checks³⁰, were properly credentialed and badged, and were subject to random and unpredictable screening procedures (i.e., spot checks). Indeed, the weakness of these procedures was so apparent that one employee told the undercover officer that “after completing the security check ... he would fly the drugs on his person to their final destination.”³¹

Moreover, TSA (and the public) has been aware of these deficiencies and weaknesses for some time. In 2010, an experienced commercial airline pilot, Chris Liu, drew attention to these known weaknesses by posting video on YouTube and his own website. Mr. Liu stated the following:

²⁸ How & Why a Department or Jail Becomes Corrupt, by Neal Trautman, Ph.D.

²⁹ What Will Matter, By Michael Josephson,

³⁰ “...you have to wonder just who did the security background on these new employees. If one was done, I doubted its accuracy and thoroughness. And I doubt if one was even done at all.”
<http://www.policemag.com/blog/gangs/story/2008/10/gangs-at-the-airport.aspx>

³¹ 46 people charged in drug-distribution conspiracy involving flights out of D/FW Airport
<http://crimeblog.dallasnews.com/2015/07/46-people-charged-in-drug-distribution-conspiracy-involving-flights-out-of-dfw-airport.html/>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

*“The real problem is that ground crews can access the airport tarmac and any aircraft, **without** having to go through any level of immediate screening and can therefore bring anything they want onto a waiting aircraft, drugs and bombs included. The doors, gates and other access points where they can access the tarmac are not being manned by TSA and certainly do not have the same metal detectors, body scanners, x-ray equipment, dogs or other security measures that the rest of us are all too painfully forced to undergo. This has, unfortunately, lead to a total lack of security.”³²*

This problem is not unique to airports. Schools face much the same problems:

To make any metal detection program effective, school access during the rest of the school day, during off hours, and during special activities needs to be tightly controlled. A motivated student can defeat a lax system. If there is a comprehensive metal detection program at the front entrance to the school, but the back entrance through the cafeteria is unguarded, the funding and efforts put into a well-meaning program can be wasted.

A successful metal detection program cannot be poorly funded or run by an administration that is reticent to make major changes to school policies and procedures.³³

³² <http://www.patriotpilot.com/aboutme.html>

³³ The Appropriate and Effective Use of Security Technologies in U.S. Schools, U.S. Department of Justice, National Institute of Justice 1999, Page 74

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Why 100 percent screening is important:

The failure to screen all airport and security employees nullifies any value of even the most stringent passenger and baggage screening. A passenger could be stripped naked, have his clothing x-rayed and physically examined, be put through a cat-scan machine; and TSA could be 100% certain that he was not carrying a weapon, explosive, or other prohibited item. He could then dress, collect his belongings, and obtain weapons, explosives, or other contraband items from some unscreened airport employee whose only concern would be avoiding any "random or unpredictable screening."

The situation with regard to checked baggage is even worse. A reasonable person might expect that with TSA personnel on the job, his bags would be safe from pilfering or being used to smuggle weapons, explosives, or other contraband onboard an aircraft. He would be wrong. TSA employees have been known to "look the other way" while others pilfered bags, or even to engage in theft themselves. This is not the worst part, however. Once TSA screens baggage, it turns these screened bags over to unscreened baggage handlers, and washes its collective hands of any responsibility.

According to Regional TSA spokeswoman Sari Koshetz, "Once we've checked your bags for explosives and other materials, it is handed over to the airline and it is their responsibility to keep that bag safe and un-tampered with."³⁴

100 percent screening of employees is important for another reason. It lets employees and passengers know that their work, their workplace, their security, the passengers and businesses they serve are important, and that they should be careful never to give opportunity to criminals or terrorists.

³⁴ Baggage handlers stealing from check Baggage handlers stealing from checked bags
<http://www.wvltv.com/story/news/local/investigations/katie-moore/2015/05/19/baggage-handlers-stealing-from-checked-bags/27625539/>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Misapplication of Risk Based Security Principles

Risk Based Security involves analyzing risks and taking steps to avoid, control, and mitigate that risk. We respectfully submit that the working group made a serious misjudgment when it concluded that "...there were significant differences between the threats posed by criminal activity and terrorism..." Referring to the threat matrix on page 7 of this report, we see that this conclusion can only be justified if we assume such smuggling operations are rare or unlikely (1-2) and their consequences insignificant or minor (1-2). The composite risk index would be 4 or less, i.e., low to very low.

There appears to be no lack of individuals who are willing, if not anxious, to risk smuggling of guns and/or drugs for profit.³⁵ From a risk management perspective, we must recognize that a weakness that has been exposed and exploited once can be exploited again:

"If they can put guns on the plane this time," said Brooklyn District Attorney Kenneth Thompson, "they could have easily put a bomb on one of those planes."³⁶

The chances that an individual willing to engage in illegal activity might find himself smuggling something other than he bargained for cannot be discounted. Accordingly, we cannot assume the likelihood of exploitation of this vulnerability to be rare or unlikely, but rather almost certain (5) and the consequences as severe, if not catastrophic (5), resulting in a composite risk index of **25 – EXTREME**.

³⁵ 46 people charged in drug-distribution conspiracy involving flights out of D/FW Airport
<http://crimeblog.dallasnews.com/2015/07/46-people-charged-in-drug-distribution-conspiracy-involving-flights-out-of-dfw-airport.html/>

³⁶ DA: Guns smuggled on planes in Atlanta an 'egregious' security breach
<http://www.cnn.com/2014/12/23/us/delta-employee-gun-smuggling/>

NATIONAL ASSOCIATION OF AIRLINE PASSENGERS

A Review of the Final Report Of the Aviation Security Advisory Committee's Working Group on Airport Access Control

Maintaining Integrity and Ethics in the workplace:

As stated in the Working Group's report, "Good security begins with good people" something we have emphasized previously to the ASAC. However, one of the biggest challenges any organization faces is keeping good employees from becoming discouraged, dissatisfied, or disgruntled. If leadership is distant and indifferent, this will be reflected in the attitudes of employees. As previously stated:

"Virtually every significant case of employee misconduct had warning signs that leaders either ignored or failed to recognize as important. Furthermore, leaders themselves lie at the core of both the cause and solution to corruption. Past research has repeatedly confirmed that most scandals start with one employee doing relatively small unethical acts and grows to whatever level the leadership allows."³⁷

It is important to recognize that a culture of indifference and corruption can begin with a single individual³⁸, and then grow to infect an entire location, and even spread to the highest levels of leadership. In the same manner, however, positive and ethical leadership can spread those higher qualities throughout an organization. We respectfully submit that positive leadership, and the examples set by management and supervisors can make the difference between a workforce that "looks the other way" and one that does not give opportunity to criminals or terrorists.

³⁷ How & Why a Department or Jail Becomes Corrupt, by Neal Trautman, Ph.D.

³⁸ Law Enforcement Ethics . . . The Continuum of Compromise, Published by: The Police Chief Magazine January 1998 http://emotionalsurvival.com/law_enforcement_ethics.htm