Calhoun: The NPS Institutional Archive

DSpace Repository

Theses and Dissertations   1. Thesis and Dissertation Collection, all items

2007-12

Securing the aviation transportation system

Oldham, Paul M.

Monterey California. Naval Postgraduate School

https://hdl.handle.net/10945/3155

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

SECURING THE AVIATION TRANSPORTATION SYSTEM

by

Paul Oldham

December 2007

Co-Advisors: Thomas Bruneau
                                                Robert O'Connell

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		*Form Approved OMB No. 0704-0188*
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.		
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2007	**3. REPORT TYPE AND DATES COVERED** Master's Thesis
4. TITLE AND SUBTITLE Securing the Aviation Transportation System		**5. FUNDING NUMBERS**
6. AUTHOR(S) Paul M. Oldham		
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A		**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.		
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		**12b. DISTRIBUTION CODE** A

13. ABSTRACT (maximum 200 words)

The vulnerability of the Aviation Transportation System was once again highlighted on September 11, 2001. Hijacking was not a new phenomenon in aviation; it erupted in the late 1960s, hijackers used commercial airliners for transportation to Cuba. The hijack incidents slowly became more violent. Aviation security legislation and measures were championed after each major aviation hijack incident, but they were not always fully implemented. What was the status of aviation security leading up to 9/11? Have the improvements made to the Aviation Transportation System since 9/11 made the system less vulnerable?

This thesis presents a comparative study of domestic aviation security measures applied to commercial passenger aviation. Security initiatives, the implementation of those initiatives, and security policies both pre and post 9/11 are described and examined in an effort to determine if the domestic Aviation Transportation System is more secure now than it was prior to September 11.

14. SUBJECT TERMS Aviation, Transportation, Security, Layered Defense			**15. NUMBER OF PAGES** 93
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

THIS PAGE INTENTIONALLY LEFT BLANK

SECURING THE AVIATION TRANSPORTATION SYSTEM

Paul M. Oldham
Major, United States Air Force
B.A., George Mason University, 1993
M.S., Embry-Riddle Aeronautical University, 2003

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)**

from the

**NAVAL POSTGRADUATE SCHOOL
December 2007**

Author: Paul Oldham

Approved by: Thomas C. Bruneau
                   Thesis Co-Advisor

                   Robert O'Connell
                   Thesis Co-Advisor

                   Douglas Porch
                   Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The vulnerability of the Aviation Transportation System was once again highlighted on September 11, 2001. Hijacking was not a new phenomenon in aviation; it erupted in the late 1960s, hijackers used commercial airliners for transportation to Cuba. The hijack incidents slowly became more violent. Aviation security legislation and measures were championed after each major aviation hijack incident, but they were not always fully implemented. What was the status of aviation security leading up to 9/11? Have the improvements made to the Aviation Transportation System since 9/11 made the system less vulnerable?

This thesis presents a comparative study of domestic aviation security measures applied to commercial passenger aviation. Security initiatives, the implementation of those initiatives, and security policies both pre and post 9/11 are described and examined in an effort to determine if the domestic Aviation Transportation System is more secure now than it was prior to September 11.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I would like to thank my thesis advisors, Dr. Thomas Bruneau and Dr. Robert O'Connell, for their expertise and guidance during the course of this work. Last but not least, thank you Amelia, Olivia and Sandy for your patience.

THIS PAGE INTENTIONALLY LEFT BLANK

I.   INTRODUCTION

A.   PURPOSE

This thesis examines domestic aviation security measures that have been implemented since the September 11, 2001, terrorist attacks on the Unites States. The purpose is to determine if the domestic Aviation Transportation System is more secure now than it was prior to September 11.

B.   BACKGROUND

By 8:00 A.M. on the morning of September 11, 2001, nineteen hijackers had defeated the civil aviation security measures that America had in place in order to prevent a hijacking.[1]

The 9/11 Commission made multiple recommendations in their report including gaining international support to counter terrorism and track terrorist financing, stopping the spread of weapons of mass destruction, improvements to border security, emergency disaster response improvements, and improvements to the nations intelligence operations.[2] This thesis will focus on an additional area identified by the 9/11 Commission requiring improvement, aviation security. Where are we now in terms of aviation security? What security improvements have been completed and is the Aviation Transportation System more or less secure from the threat of terrorism?

The United States Aviation Transportation System is a critical infrastructure.[3] As such, it *must* be enveloped with a level of security that will ensure both the safety of travelers from the threat of terrorism, and also facilitate the secure mass movement of both people and goods. In 2003 alone, U.S air carriers transported over 595 million

---

[1] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 4.

[2] Ibid., 361-423.

[3] President of the United States, *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets*, (Washington D.C.: 2003), 54.

passengers aboard commercial aircraft.[4] In that same year, over 20,000 persons were intercepted at airport screening checkpoints carrying box cutters.[5] The importance of effective aviation security is crucial in order to protect the public traveler, but it is also a necessary deterrent to terrorist threats.

The threat to aviation security is persistent. A lack of diligence in aviation security will almost certainly welcome the persistent threat of terrorism. Determining where efforts or measures have been implemented may help to focus efforts on areas that have not been fortified. Have the current implementation of post 9/11 security measures reduced the vulnerability of commercial aviation to terrorist attack? What are the deficiencies of the system? Where should future efforts be focused?

Security efforts in aviation have been under continual scrutiny following 9/11, and viewpoints on the effectiveness of those efforts vary considerably. Opinions range from suggesting that the entire security strategy is flawed, to the U.S. has overreacted to terrorism, to the stance that current security improvements have had little effect on securing commercial aviation.

Some aviation security experts contend that increased security efforts essentially have little or no effect. The Aviation and Transportation of Security Act of 2001 created the Transportation Security Administration, federalized airport screeners, and directed the screening of all checked baggage for explosives.[6] Some aviation security analysts argue that the 100% screening of all checked baggage mandated by Congress actually was a detriment to national security due to the fact that the measures diverted funds, attention,

---

[4] U.S. Bureau of Transportation Statistics, *U.S. Air Carrier Aircraft Departures, Enplaned Revenue Passengers, and Enplaned Revenue Tons*, Available from http://www.bts.gov/publications/national_transportation_statistics/html/table_01_34.html (accessed 27 May 2007).

[5] U.S. Bureau of Transportation Statistics, *Prohibited Items Intercepted at Airport Screening Checkpoints*, Available from http://www.bts.gov/publications/national_transportation_statistics/2006/html/table_02_16b.html (accessed 26 May 2007).

[6] United States 107th Congress, *Aviation and Transportation Security Act,* National Transportation Library online Available from http://ntl.bts.gov/faq/avtsa.html (accessed 27 May 2007).

and resources from passenger and carry-on baggage screening.[7] A similar view is that the heavy emphasis on passenger screening leaves other areas vulnerable to attack such as airline cargo security.[8] While passenger checked luggage is required to be screened for explosives, only a small portion of air cargo is ever inspected.[9]

The federalization of airport screeners was another post 9/11 measure. The goal was to standardize screening efforts at all airports through centralization of control under the Transportation Security Administration. The Government Accountability Office has found that current airport screening efforts are little better than what existed prior to the "federalized" effort.[10] The report highlights areas of concern such as efforts to hire baggage screeners as well as the ability to effectively train the screening workforce.[11] The evidence cited tends to strengthen the argument that post 9/11 provisions have had little impact on security efforts. Chairman of the Subcommittee on Aviation, Congressman John Mica stated, "TSA's current baggage screening system …does not even afford us more effective security screening."[12]

Another stronger argument about the current approach to aviation security is that it is fundamentally flawed.[13] One basic flaw that is pointed out in the current security model is that it is premised on an equal-risk model.[14] Current procedures presume that all air travelers are equally likely to be a threat, and therefore all travelers require equal

[7] Grace Jean, "Focus on Checked Bag Screening has Detracted from Aviation Security," *National Defense* 91, 640 (2007), 30.

[8] Eben Kaplan, "Targets for Terrorists: Post-9/11 Aviation Security," Council on Foreign Relations online article, 7 September 2006, Available from http://www.cfr.org/publication/11397/targets_for_terrorists.html (accessed 27 May 2007).

[9] David Randall Peterman, *Transportation Security: Issues for the 109th Congress* (Washington D.C.: CRS, 2006), 5.

[10] Ibid.

[11] United States General Accounting Office, *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts* (Washington D.C.: GAO, 2004), 9.

[12] Eben Kaplan, "Targets for Terrorists: Post-9/11 Aviation Security," Council on Foreign Relations online article, 7 September 2006, Available from http://www.cfr.org/publication/11397/targets_for_terrorists.html (accessed 27 May 2007)

[13] Robert W. Poole, Jr., "Airport Security: Time for a New Model," Reason Foundation online article, January 2006, Available from http://www.reason.org/airportssecurity (accessed 21 May 2007), 1.

[14] Ibid., 1-3.

attention in terms of screening measures.[15] This creates a non-focused security effort rather than steering resources to pinpoint persons of risk. A second criticism is that the current efforts are too focused on detecting or restricting dangerous objects as opposed to people.[16] The contention is that the focus of security is more aligned with preventing another 9/11 scenario by keeping dangerous items off of aircraft. If inflicting mass casualties was the sole desire, a terrorist could simply target travelers in a crowded airport, therefore the focus of the effort should be aimed at targeting dangerous people, not objects.[17] While the point is valid, a counter argument is that the last two foiled aviation related terrorist incidents, the shoe bomber and the liquid-gel bombing plot, highlight the reoccurring theme of attempting to get aboard an aircraft in order to inflict damage while airborne.

Terrorists continue to innovate new methods to bypass or breach aviation security in order to utilize commercial aircraft as a means to an end. Even after increased international aviation security efforts following 9/11, terrorist Richard Reid managed to board an American Airlines flight in Paris in December 2001 with explosives contained in his shoe.[18] Security measures in other countries followed the U.S. by focusing efforts on passengers' shoes. Then in August 2006, British authorities arrested twenty-four suspects plotting to simultaneously blow up ten U.S. bound passenger aircraft using yet another technique, liquid explosives hidden in their carry-on luggage.[19] TSA Administrator David Stone told the Senate Commerce, Science and Transportation

---

[15] Robert W. Poole, Jr., "Airport Security: Time for a New Model," Reason Foundation online article, January 2006, Available from http://www.reason.org/airportssecurity (accessed 21 May 2007), 1-3.

[16] Ibid., 22.

[17] Ibid., 23.

[18] Kevin A. O'Brien, "France," in *Europe Confronts Terrorism*, ed Karen Von Hippel (New York: Palgrave Macmillan, 2005), 38.

[19] John Ward Anderson and Karen De Young, "Plot to Bomb U.S.-Bound Jets Is Foiled," *Washington Post*, 11 Aug 2006, Available from http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html (accessed 27 May 2007).

Committee in 2005 that "the greatest risk is still that a plane may be targeted for attack or used to carry out an attack.[20]

One other viewpoint is that the threat of terrorism has been completely blown out of proportion. That perceived risks are usually much greater than actual risks, and spectacular risks are more grossly exaggerated than common risks.[21] For example, there were over 38,000 motor vehicle-related fatalities in the same year as the September 11 terrorist attacks.[22] By sheer body count, vehicle accidents take a far greater toll of life than September 11. A motor vehicle related incident is also far more probable for the average U.S. citizen to experience, than being a victim of a terrorist attack. Yet traffic and highway safety is in no way on equal footing to safeguarding the public and critical infrastructures from possible acts of terrorism.

Given a persistent threat to aviation security and the varied views of security measures what is the status of aviation security within the U.S.? Have security efforts reduced the vulnerability of commercial aviation? Have 9/11 deficiencies been rectified and if not what is the causal reason? Where should security efforts be focused?

C.   METHODOLOGY

The research methodology used will compare security measures before and after 9/11. A comparative study of security measures will describe and examine security initiatives, the implementation of those initiatives, and security policies. This study will use a United States General Accounting Office Risk Management Model recommended for the Transportation Security Administration.[23] This model contains three variables,

---

[20] Chris Strohm, "TSA Chief Says aviation attacks still pose greatest risk," Government Executive.com, 15 February 2005, Available from http://www.govexec.com/dailyfed/0205/021505c1.htm (accessed 27 May 2007).

[21] Bruce Schneier, *Beyond Fear: Thinking Sensibly About Security in an Uncertain World* (New York: Copernicus Books, 2003), 26.

[22] United States Bureau of Transportation Statistics, *Motor Vehicle Fatalities, Vehicle-Miles, and Associated Rates by Highway Functional System,* Available from http://www.bts.gov/publications/national_transportation_statistics/html/table_02_18.html (accessed 27 May 2007).

[23] United States General Accounting Office, *Aviation Security: Efforts to Measure Effectiveness and Address Challenges* (Washington D.C.: GAO, 2003), 14.

the likelihood of the threat, the criticality of the asset, and the vulnerability of the system. The first two variables will remain constant as the likelihood of the threat to commercial aviation is historically proven, and the criticality of the asset in this study has only one facet, the commercial airliner. The third variable then is what will be focused on, the vulnerability of the system. The security measures will be categorized into one of three functional layers, access, physical security or direct action. Within each layer, the number of protective measures will then be examined against pre 9/11 measures to draw conclusions as to the improvement in vulnerability reduction.

The 9/11 commission deficiencies will also be compared to the current security initiatives in an effort to determine if the deficiencies have been rectified. If deficiencies have not been countered, possible causal aspects such as funding constraints, training or oversight problems will be discussed to recommend areas for further focus.

D.   AVIATION PIRACY EVOLUTION

Aviation Piracy is not a new phenomenon. Aviation hijackings occurred as early 1931 when Peruvian Revolutionaries hijacked a Pan American Ford Trimotor mail plane in order to distribute propaganda leaflets.[24] As the aviation age progressed, so too did aviation related crimes. Why? Terrorists exploit new technologies as a means to achieve their goals. David Rapoport chronicles four waves of modern terrorist groups from the 1800s to the late 1970s, and associated with the swell of each new wave of terrorists, was a new transportation or communication technology that was susceptible to terrorist exploitation.[25] In this case, aviation hijacking or the exploitation of commercial aviation became the new modus operandi of the international terrorist. The rash of terrorist hijackings that occurred in the late 1960s and early 1970s coincided with the dawn of commercial jet aviation. The modern era of trans continental travel was growing, and with it so grew the exploitation of modern commercial jetliners.

---

[24] Peter St. John, *Air Piracy, Airport Security, and International Terrorism* (New York: Quorum Books, 1991), 5.

[25] David Rapoport, "The Four Waves of Modern Terrorism," in *Attacking Terrorism: Elements of A grand Strategy,* ed. Audrey Kurth Kronin and James Ludes, (Washington DC: Georgetown University Press, 2004), 47.

1. Hijackings

The first aircraft hijacked within the United States occurred in 1961.[26] Antuilo Ramirez Ortiz forced a National Airlines Convair flight crew at gunpoint to fly the aircraft to Communist Cuba.[27] This marked the starting point of a rash of aviation hijacking events in the United States, which gained a significant swell in the latter part of the decade. Between 1968 and 1972, 326 aircraft hijack attempts occurred throughout the world.[28] Of those 326 hijackings, 124 occurred within the United States.[29] In 1968 alone there were twenty aircraft hijackings in the U.S.[30] Initially, the rationale for hijacking an aircraft was for transportation, but the rationale soon expanded. Robert Holden's article, "The Contagiousness of Aircraft Hijacking," placed aircraft hijackings into one of two main categories depending on the demand or desired objective of the hijacker, either hijacking for extortion or hijacking for transportation.[31]

a. Transportation

As aircraft hijacking incidents grew in number, the objective of hijackers tended to focus more on securing transportation to a desired destination. In the 1960s, the majority of aviation hijack incidents in the United States were the result of aircraft being diverted to Cuba. Out of 111 aircraft hijackings whose hijackers solely sought a means of transportation from the United States, ninety of those were destined for Cuba.[32] In 1968 alone there were nineteen U.S. domestic flights that were hijacked to Cuba, and in 1969, this trend spiked to thirty-nine hijackings within the U.S. and all but two were

---

[26] United States Department of State, *Significant Terrorist Incidents, 1961-2003: A Brief Chronology*, Available from http://www.state.gov/r/pa/ho/pubs/fs/5902.htm (accessed 2 Aug 2007).

[27] Jin-Tai Choi, *Aviation Terrorism* (New York: St. Martin's Press, 1994), 23.

[28] Judy Rumerman, "Aviation Security," U.S. Centennial Commission of Flight, Available from http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm (accessed 3 Aug 2007).

[29] William M. Landes, "An Economic Study of U.S. Aircraft Hijacking, 1961-1976," *Journal of Law and Economics* Vol. 21, No. 1 (1978): 1.

[30] Laura Dugan et al., "Testing A Rational Choice Model of Airline Hijackings," *Criminology* 43 no. 4 (2005): 1041.

[31] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 878-879.

[32] Ibid.

seeking destination Cuba as an objective.[33] Many of these incident hijackers were of Cuban birth and only desired to return to their homeland, as travel to Cuba from the U.S. was banned.[34] Some hijackings however, were not only characterized by a desire to utilize commercial aviation as a source of transportation, but also held additional hijacker demands.

b.   *Extortion*

Initially, hijackers desiring a means of transportation dominated aircraft hijackings, but as the act of air piracy grew, so to did the reasons for hijacking aircraft. Hijackers requested additional demands and extortion became a common reason in addition to modern conveyance. Extortion objectives ranged from political objectives to prisoner release to media attention.[35] In the U.S. however, monetary gain was the primary reason for extortion related hijacking attempts.[36]

The first extortion related hijacking in the U.S. occurred in 1970 at Dulles Airport, Virginia when an aircraft was held for ransom by a hijacker demanding $100 million dollars.[37] Another similar U.S. hijacking occurred the following year when a hijacker demanded a monetary ransom and then forced the crew to fly the aircraft to the Bahamas.[38] The extortion element was not isolated to the U.S., as extortion hijackings were occurring worldwide as well. Five more extortion related hijackings occurred within the U.S. in 1971, one of which hijackers demanded the release of several Black Panther members from prison.[39] The most notable extortion related hijacking of 1971

---

[33] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 881-882.

[34] Ibid., 877.

[35] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 644.

[36] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 879.

[37] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No. 4 (1973): 646.

[38] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 885.

[39] Ibid., 882-885.

was unquestionably the DB Cooper heist in which he demanded a ransom of $200,000 dollars and two parachutes.[40] He subsequently jumped from the rear door of the Boeing 727 while it was in-flight and was never caught nor the money recovered.

The following year, 1972, there were thirty-one hijackings within the U.S., and of those thirty-one, nineteen were extortion related, but hijacking rates began to decline.[41] In 1973 only two aircraft hijacking occurred the U.S.[42] Between 1973 and 1982, the average number of U.S. hijackings per year was only 9.3 as compared to twenty-nine per year between 1968-1972.[43] The high rate of hijackings in the United States did not rise again until the 1980s.[44]

2.   Implications for Security

In the earliest days of aviation, hijacking was a minor concern. It was not an element of focus even though the act of hijacking an aircraft became more prevalent. U.S. hijacking incidents in the late 1960s became commonplace for passengers and flight crews. In 1969 at least one hijacking occurred each month.[45] Aircrews began to carry approach information for airports in Cuba, and aircrew training emphasized compliance with hijackers as diplomatic procedures were in place for the return of aircraft and passengers.[46] Compliance and non-resistance were the focal points to eventually gain the release of passengers and crew. Hijackers would issue their demands, be delivered to their destination and eventually, passengers and aircraft would be returned to the U.S. From the U.S. perspective, this is how hijackings occurred. It wasn't until 1971 that the

---

[40] Jin-Tai Choi, *Aviation Terrorism* (New York: St. Martin's Press, 1994), 20.

[41] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 885.

[42] Laura Dugan et al., "Testing A Rational Choice Model of Airline Hijackings," *Criminology* 43 no. 4 (2005): 1041.

[43] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 885.

[44] Laura Dugan et al., "Testing A Rational Choice Model of Airline Hijackings," *Criminology* Vol. 43 No. 4 (2005): 1041.

[45] Robert T. Holden, "The Contagiousness of Aircraft Hijacking," *The American Journal of Sociology* (1986): 882.

[46] Ibid., 881.

first passenger was killed in the U.S. during an aircraft hijack.[47] Hijackings became more violent, as the killing of passengers and aircrews or the bombing of aircraft incidents escalated. In September 1970, the Popular Front for the Liberation of Palestine (PFLP), simultaneously hijacked and later destroyed four commercial airliners, two of which were U.S. aircraft.[48] This event was essentially the culmination or turning point of aviation hijackings for the era. It struck an international chord and drove the need to establish an international legal stance to counter the problem of hijacking.

As a result of the rising rate of airline hijackings, the Hague Convention for the Suppression of Unlawful Seizure of Aircraft was held in 1970. Sixty cooperating states agreed on provisions to enact legislation against hijacking, arrest and trial provisions, and active response measures such as blocking the runway or disabling the aircraft while on the ground to prevent it from taking off.[49] The Hague Convention also framed the difficult subject of jurisdiction. Hijacking had become not only an international problem but it created a gray area of jurisdictional boundary that hijackers traveling from country to country could exploit. Where did each country's authority begin and end? The Hague Convention sought to narrow that jurisdictional gap.[50] The Hague convention facilitated the groundwork to apprehend hijack perpetrators, as it was more punitive in nature than the Tokyo Convention of 1963, which tended to focus more on the return of aircraft.[51] Domestically, from 1961 through 1976, as the apprehension rates of domestic hijackers grew, the number of domestic hijacking incidents subsequently declined.[52] Prison sentences also increased in duration, which had a corollary impact. The average sentence

---

[47] Peter St. John, Air Piracy, Airport Security, and International Terrorism (New York: Quorum Books, 1991), 14.

[48] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 652.

[49] Sami Shubber, "Aircraft Hijacking under the Hague Convention 1970: A New Regime?" *The International and Comparative Law Quarterly* Vol. 22, No. 4. (1973): 708.

[50] Ibid., 718.

[51] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 667.

[52] William M. Landes, "An Economic Study of U.S. Aircraft Hijacking, 1961-1976," *Journal of Law and Economics* Vol. 21, No. 1 (1978): 2.

for those convicted of hijacking between 1972 and 1974 was thirty years.[53] The treaty between the U.S. and Cuba to curb the Cuba-hijack-movement also had a significant impact. Both countries signed a treaty in 1973 agreeing to either extradite or punish hijackers.[54] This treaty essentially alleviated the safe haven for asylum seekers regardless of which direction they were traveling, either to or from Cuba.

The security policies governing airport and airline security procedures also became more stringent. The Federal Aviation Administration provided the airlines the authority to deny travel to persons that would not consent to a search of their persons or luggage.[55] Warning signs were also posted in airports as reminders that it was a federal offense to carry concealed weapons or to hijack an aircraft.[56] In the face of ever increasing violent hijack events coupled with the aforementioned PFLP hijacking, on September 11, 1970, President Nixon introduced an anti-hijacking program that included expanding the Federal Sky Marshal program started in 1961.[57] These initial efforts were noteworthy, but in 1972 two U.S. aircraft were hijacked within days of each other resulting in the death of one airline employee, and another five persons injured. This incident spawned the 100% screening of boarding passengers policy, a mandatory inspection of carry-on luggage in January 1973, and the placement of armed guards at all airport boarding gates.[58] These security efforts were not limited only to policy as then current advanced technologies and science were also employed to enhance security operations such as the procurement of electronic security detection devices. In 1972, $3.5 million dollars was allotted to procure detection devices, resulting in the installation

---

[53] William M. Landes, "An Economic Study of U.S. Aircraft Hijacking, 1961-1976," *Journal of Law and Economics* Vol. 21, No. 1 (1978): 2.

[54] Ibid., 4.

[55] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 649.

[56] Ibid.

[57] United States 109th Congress, *Plane Clothes: Lack of Anonymity at The Federal Air Marshal Service Compromises Aviation and National Security* (Washington D.C.: GPO, 2006).

[58] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 649.

of metal detectors in airports by 1973.[59] The use of behavioral science was also employed to develop behavioral profiling training for airport personnel in order to identify potential hijackers.[60]

Following 1972, there was a rapid decline in the number of hijackings in the U.S., and there were zero hijackings in the first eight months of 1973.[61] An increasing number of anti-hijack related laws, security policies and applied security technologies were put into place that had a significant impact on the declining hijacking rate. These security measures had positive results. But it was an applied combination of international response, implemented legal tools with harsh penalty, improved security policy coupled with advanced technologies that successfully curbed the hijacking dilemma of the late 1960s and early 1970s.[62] There were still sporadic accounts of aircraft hijackings, but for a period of eight years following 1992, there were no hijack events within the United States.[63] Prior to 9/11, there was a significant lull in domestic hijack activity.

---

[59] Alona E. Evans, "Aircraft Hijacking: What Is Being Done," *The American Journal of International Law* Vol. 67, No.4 (1973): 649.

[60] Ibid.

[61] Ibid., 641.

[62] Landes, William M. "An Economic Study of U.S. Aircraft Hijacking, 1960-1976," *Journal of Law and Economics* (April 1978): 28.

[63] Laura Dugan et al., "Testing A Rational Choice Model of Airline Hijackings," *Criminology* 43 no. 4 (2005): 1041.

II.   FRAMING THE AVIATION SECURITY PROBLEM

A.   THE AVIATION TRANSPORTION SYSTEM

This primary focus of this thesis is one aspect of securing the Aviation Transportation System, the security measures applied to commercial aviation. In order to frame the security problem properly, however, a brief description of the Aviation Transportation System is necessary in order to illustrate the difficulty of providing foolproof security to a public mode of transportation. The sheer size of the Aviation Transportation System makes this an almost insurmountable task.

The Aviation Transportation System is comprised of aircraft, operators, airports, facilities and infrastructure, as well as services and airspace.[64] It is a multi-faceted system that includes both private and public involvement as well as seven federal government agencies. Both commercial and general aviation operations are conducted from over 19,800 airports throughout the U.S.[65]   The Transportation Security Administration estimates that there are a million airport employees including vendor workers employed at commercial airports throughout the country.[66] These numbers do not even include personnel located at remote FAA radar facilities or Flight Service Stations.

The complexity of these intertwined aviation elements is compounded by the numerous government agencies that are also woven within the fabric of the Aviation Transportation System. These agencies work to secure, maintain, and regulate the operations and infrastructure of the system. The Department of Transportation for instance manages the system infrastructure such as airport facilities. The Transportation Security Administration is the lead agency for security, and the Federal Aviation

---

[64] George W. Bush, *The National Strategy for Aviation Security*, (Washington D.C., 2007), Available from http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf (accessed 17 Aug 2007), 6.

[65] Ibid.

[66] United States General Accounting Office, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls* (Washington D.C.: GAO, 2004), 9.

Administration regulates operations, coordinates the nations massive volume of airspace, and controls the daily congestion of air traffic over flying our nation, the majority of which is general aviation.

Although general aviation has not been a primary target of terrorists, it never the less makes up a large portion of domestic aviation. Three quarters of all aircraft that take-off and land in the U.S. are general aviation aircraft.[67] In terms of persons and aircraft, general aviation operations involve over 550,000 pilots and 200,000 private aircraft.[68] While these numbers are significant, commercial aviation is by far the leading entity when viewed in terms movement volume, either of people or goods.

1. Commercial Aviation

Commercial aviation operations include both passenger airlines as well as commercial cargo carriers. In February 2006, 153 commercial air carriers, including commuter airlines were certified to conduct operations in the United States.[69] In that same year, certified air carriers employed 589,961 people at locations and airports throughout the aviation system.[70] And in 2005, 554 domestic airports were operating as commercial service airports.[71] The large number of commercial passenger carriers has provided terrorists with a variety of targets, and as passenger volume increases, so does an exploitation source for terrorists.

---

[67] United States Government Accountability Office, *General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector is Critical to Long-Term Success* (Washington, D.C.: GAO, 2004).

[68] Joseph S. Szyliowicz, "Aviation Security: Promise or Reality?" in *Homeland Security and Terrorism*, ed. Russell Howard, James Forest and Joanne Moore, 118 (New York: McGraw-Hill, 2006).

[69] Federal Aviation Administration, *U.S. Certified Air Carriers 2006*, Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/addresses/ (accessed 11 Sep 2007).

[70] United States Bureau of Transportation Statistics, *Employment Statistics,* Available from http://www.bts.gov/programs/airline_information/number_of_employees/ (accessed 11 Sep 2007).

[71] Federal Aviation Administration*, Primary and Non-Primary Commercial Service Airports*, Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/passenger/index.cfm?year=2005 (accessed 11 Sep 2007).

a. Passenger

Passenger airlines have been the principal target for terrorists in the aviation community. The volume and throughput of commercial passenger aviation exacerbates the aviation security problem. In 2006, there were 131 commercial passenger carriers that operated in or from the United States.[72] In 2005, U.S. passenger carriers ferried 701,509,325 travelers, and that number does not even include commuter airline enplanements.[73] The year prior, 672,018,635 passengers traveled on board commercial airliners.[74] These carriers transport millions of travelers each year, to and from hundreds of major airports, and handle more than 2.5 billion handheld and checked luggage.[75] In just one month in 2005, passenger commercial airlines flew 822,374 domestic flights.[76] Many of these commercial passenger carriers also simultaneously transport cargo within the lower bay of the aircraft, and cargo security presents yet another challenge to the aviation security arena.

b. Cargo

There are twenty-five air carriers within the U.S. that dedicate commercial flights solely to cargo.[77] Within the freight industry, airfreight ships the least amount of cargo annually in comparison to other industry modes of transportation such as rail or truck. However, the sheer tonnage freighted by air is still very large. In 2004, over one

---

[72] Federal Aviation Administration, *U.S. Certified Air Carriers 2006*, Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/addresses/ (accessed 11 Sep 2007).

[73] United States Bureau of Transportation Statistics, *Top 50 Airports by Passengers Enplaned On Large U.S. Carriers: 1995, 2004 and 2005*, Available from http://www.bts.gov/publications/state_transportation_statistics/state_transportation_statistics_2006/html/table_04_06.html (accessed 11 Sep 2007).

[74] Ibid.

[75] Joseph S. Szyliowicz, "Aviation Security: Promise or Reality?" in *Homeland Security and Terrorism*, ed. Russell Howard, James Forest and Joanne Moore, 109 (New York: McGraw-Hill, 2006).

[76] United States Bureau of Transportation Statistics, *Domestic Airline Travel in October*, Available from http://www.bts.gov/press_releases/2006/bts002_06/html/bts002_06.html#table_01 (accessed 11 Sep 2007).

[77] Federal Aviation Administration, *U.S. Certified Air Carriers 2006*, Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/addresses/ (accessed 11 Sep 2007).

billion tons of commercial air cargo was airlifted either by dedicated cargo or passenger-cargo commercial flights.[78] The commercial air cargo arena is also filled with additional actors. The "passenger" must be shipped which in turn invites additional entities to the aviation security arena. The movement of airfreight will involve the initial shipper, freight forwarders, logistic integrators, and airport logistic centers.[79] All of these groups will widen the security aperture and present additional security problems.

B. PRE-9/11 AVIATION SECURITY MEASURES

1. Building the Security Layers

The first wave of aviation hijackings was challenged by the development and implementation of passenger screening devices and regulated security processes. These initial security and screening efforts laid the foundation for security programs to follow, many of which in principal are still in use.

a. The 1980s and Pan Am Flight 103

In the 1980s, in the face of increased international hijacking events, President Reagan signed the International Security and Development Cooperation Act of 1985, which once again authorized funding to revive the Federal Air Marshal program.[80] Similar to the Anti-Hijacking Act of 1974, the US Foreign Assistance Act of 1985 allowed the secretary of transportation to levy even harsher penalties on foreign air carriers operating in the U.S. that failed to meet security standards.[81] Funding was also appropriated to further develop security and explosive detection technologies.[82] These

---

[78] United States Bureau of Transportation Statistics, *Domestic Flights: Air Revenue Ton Miles*, Available from http://www.bts.gov/press_releases/2006/bts002_06/html/bts002_06.html#table_01 (accessed 11 Sep 2007).

[79] The International Air Cargo Association, *The TIACA Manifesto,* Available from http://www.tiaca.org/content/chapter1.asp (accessed 14 Sep 2007).

[80] United States Department of Transportation, *A Chronology of Dates Significant in the Background, History and Development of the Department of Transportation*, Available from http://dotlibrary.dot.gov/Historian/chronology.htm (accessed 12 Sep 2007).

[81] Jin-Tai Choi, *Aviation Terrorism* (New York: St. Martin's Press, 1994), 34.

[82] Ibid.

16

technologies would soon become even more of a high interest item as emphasis shifted from guns and knives and moved towards finding explosives.

The shock value achieved by terrorists targeting commercial aviation was reinforced again in 1988 with the death of 270 persons flying on board a Pan Am 747 airliner. Aviation security was once again tested and penetrated by a bomb made of plastic explosive that was placed on board Pan American Flight 103, inside a piece of checked baggage. A timer detonated the bomb that exploded the aircraft in mid-air over Lockerbie, Scotland. The owner of the luggage was not on board. Although this flight did not depart from a U.S. airport, concern grew within the U.S. regarding domestic aviation security and the ability to screen and detect explosives. This concern would generate a presidential commission.

The Commission on Aviation Security and Terrorism convened in 1989 following Pan Am Flight 103 incident. The commission's charge was to evaluate then current aviation security policies and practices, and recommend improvements.   In general, the commission found that the aviation security system "was sorely lacking."[83] It noted shortcomings in intelligence information, specifically in gaining, accessing and disseminating intelligence, and also a lack of federal government oversight of airline and airport activities.[84]   The commission cited 64 recommendations to improve domestic aviation security, one of which was to establish minimum standards for hiring, training, and employing security personnel.[85] The commission also recommended placing Federal security managers at high risk airports to ensure airlines comply with security mandates.[86]

Following the Pan Am incident, the secretary of transportation directed the installation of new Thermal Neutron Analysis (TNA) explosive detection machines at

---

[83] Commission on Aviation Security and Terrorism, *Findings and Recommendations*, 15 May 1990, Available from http://www.globalsecurity.org/security/library/congress/1990_cr/s900511-terror.htm (accessed 12 Sep 2007).

[84] Ibid.

[85] Ibid.

[86] Ibid.

100 of the main commercial airports in the U.S.[87]   Only three machines were deployed for initial operational testing however, and their performance was evaluated as unsatisfactory.[88]   Due to these initial results, the aforementioned commission also recommended accelerating research to develop new explosive detection technologies.[89]

As a result of the commission's findings, President George H.W. Bush signed the Aviation Security Improvement Act of 1990, which codified the commission's recommendations.[90]   The act implemented security enhancements in three main areas, oversight, screener standards and explosive detection technology.[91]   New positions were created within FAA to provide security oversight.   The Act also required FAA to announce rules requiring airlines to apply standards for the hiring, continued employment, and training of security workers, to include criminal background checks.[92] The act also mandated FAA to accelerate research on explosive detection technology, and to deploy new explosive detection equipment by November 1993.[93]

It is important to note however, that several accounts indicate that the Aviation Security Improvement Act did little to improve aviation security. The intent to improve security was worthwhile, yet by the time another 747 accidentally exploded in mid-air in 1996 due to mechanical failure, airport security had not improved, explosive detection machines were not deployed to airports, airport screeners were still poorly trained, and suitcases were not matched to passengers on domestic flights.[94]

---

[87] Joseph S. Szyliowicz, "Aviation Security: Promise or Reality?" in *Homeland Security and Terrorism*, ed. Russell Howard, James Forest and Joanne Moore, 111 (New York: McGraw-Hill, 2006).

[88] Subcommittee on Aviation of the Committee on Transportation and Infrastructure, *Hearing on Deployment and Use of Security Technology,* Congress No. 107, Session No 1, 11 Oct 2001, Available from http://www.globalsecurity.org/security/library/congress/2001_h/011011-memo.htm (accessed 13 Sep 2007).

[89] Ibid.

[90] Marla Felcher, "U.S. Aviation Security: Before and After the September 11 Attacks," Understanding Government, Available from http://understanddinggov.org/reports/ (accessed 13 Sep 2007).

[91] Ibid.

[92] Ibid.

[93] Ibid.

[94] Ibid.

Almost simultaneous to the Commission on Aviation Security and Terrorism's hearings, the U.S. Government Accounting Office (GAO) completed its report on FAA's domestic and international security programs. GAO testimony before Congress noted that fundamental deficiencies existed in four areas of FAA's aviation security program: passenger screening, airport security controls, security inspections, and training requirements for security personnel.[95] The report cited that high turnover rates, low wages, and inadequate training hindered security screening effectiveness.[96] In terms of airport security, the report cited a lack of employee identification controls, and access to aircraft operation areas, or restricted areas was fairly open.[97] The report also noted that FAA airport security inspections were inadequately accomplished, and standards among different airline security training programs were lacking.[98]

A subsequent 1994 GAO report regarding the development of security technology referencing the Aviation Security and Improvement Act of 1990, reported that little progress had been made on deploying new explosive detection systems.[99] At the time of the report, six years had passed since the Pan Am 103 incident, and FAA was still assessing forty different detection technologies but none of them had fully met FAA's performance requirements to detect sophisticated plastic explosives.[100] As a result of these shortfalls, there still was no explosive detection capability for checked baggage.

b.   The 1990s and TWA Flight 800

The next major aviation security review was by the White House Commission on Aviation Safety and Security, chaired by then Vice President Al Gore. This commission was created less than one month after the mid-air explosion of another

---

[95] United States General Accounting Office, *Proactive Management of FAA's Security Program Needed* (Washington, D.C.: GAO, 1989), 1.

[96] Ibid., 4.

[97] Ibid., 6.

[98] Ibid., 10.

[99] United States General Accounting Office, *Aviation Security: Development of New Security Technology Has Not Met Expectations* (Washington, D.C.: GAO, 1989).

[100] Ibid.

U.S. 747 airliner. On July 17, 1996, TWA Flight 800 laden with 230 passengers and crew, exploded shortly after take off from New York's John F. Kennedy airport.[101] While investigators determined that the cause of the mid-air explosion of TWA Flight 800 was the eruption of the center fuel tank and not the result of a terrorist bomb, the accident itself looked too similar to Lockerbie. Incident eyewitnesses recounted seeing a streak of light heading towards the airliner from the ground, which many speculated was a man portable air defense missile, igniting the possibility of another terrorist attack. As a result of the TWA incident, President Clinton established the commission to study aviation security and safety issues, and to establish a plan to implement new explosive detection technology.[102]

The Commission on Aviation Safety and Security, which was also known as the Gore Commission, released its final report in 1997, which contained 31 recommendations to improve aviation security. Many of the recommendations were similar to those of the previous Aviation Security and Terrorism Commission in 1989 and tended to fall in one of three main areas: security and screening personnel, explosive detection technology, and the use of technology to facilitate passenger profiling, and passenger to bag-matching measures.

The airlines were responsible for screening passengers and their baggage, and for training the personnel that performed those duties. But training and standards varied from carrier to carrier. One notable Commission recommendation was to establish federally mandated standards for screener training, hiring, and operator performance standards.[103] The federal mandate would also apply to the operation of explosive detection systems, automated bag match technology, and profiling programs.[104] This mandate would apply set operating standards to all aspects of security screening in order to ensure continuity of operations among differing airlines and different security

---

[101] CNN, "TWA Flight 800 The Crash and Investigation," CNN Online, Available from http://www.cnn.com/US/9707/twa.800/ (accessed 11 Sep 2007).

[102] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C.: 1997), 5.

[103] Ibid., 18.

[104] Ibid.

companies. In order to increase the professionalism of the screener workforce, the Commission also recommended a national program to certify the screening companies.[105] Screening companies would be required to meet the established standards mandated for screener personnel, and company hiring evaluations would be based on screening performance, not the lowest contract cost bid. To further cultivate the profession, human factors were addressed such as implementing reward-performance programs and exploring the use of best practice initiatives.[106] The quality of the security workforce was previously addressed by the 1989 Commission which had also cited a need for training and hiring standards. The Gore Commission also recommended criminal background and FBI fingerprint checks for all security screeners and airport and airline employees with access to secure areas.[107]

Acquiring an explosive detection capability was still a high priority in the aviation security arena. To enable the FAA to satisfy the delinquent federal deadline of deploying an explosive detection technology, the Commission recommended deploying current existing available commercial technology.[108] To this point, only one explosive detection device had met FAA's operational requirements, but its performance was sluggish, and it was expensive. The Commission felt that by deploying current technology in use at international airports, while not meeting FAA's certification standards, it would provide some added measure of protection to aviation travelers.[109] In order to augment the detection technology, due to its protracted development, the Commission also recommended expanding the use and deployment of bomb-sniffing dogs.[110]

The third major area of the Commission's recommendations surrounded the use of technology to automate passenger profiling and to implement a 100% bag-

---

[105] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 20-26.

[106] Ibid.

[107] Ibid., 21-22.

[108] Ibid., 22.

[109] Ibid.

[110] Ibid., 24.

passenger match measure by December 31, 1997.[111] The checked bags of passengers selected either by an automated profiling program or at random, would then either be screened or matched to a boarded passenger.[112] These combined measures would first identify passengers of "risk," and second ensure that their bags were screened for explosives or that the passenger was on board the aircraft prior to the bag being loaded. This measure would counter the Lockerbie scenario of a checked bag with no owner-passenger on board, yet the scenario of a suicide bomber on an aircraft had not presented itself. One additional measure recommended by the Commission was to "aggressively test existing security systems" by increasing the use of "Red Teams" or adversary agents.[113] The Commission recommended incorporating red teaming as a standard element of airport security measures to continually re-assess airport security by finding vulnerabilities.

The Federal Aviation Reauthorization Act of 1996 was passed following the initial recommendations of the Commission on Aviation Safety and Security. The measures enacted that applied to the security workforce directed FAA to certify security screening companies, to develop uniform security screening performance standards, and to require employment background checks on screeners and security personnel associated with baggage or cargo functions.[114] In the arena of explosive detection, FAA was directed to assess, and deploy, explosive detection technologies that were currently available to commercial aviation.[115] Passenger profiling was also addressed but only to the extent that FAA and other agencies "should continue to assist air carriers in their development of passenger profiling programs."[116] The same held true in reference to a passenger bag-match program. Finally, the Act also directed periodic vulnerability assessments of airport security systems.

---

[111] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 28.

[112] Ibid.

[113] Ibid., 26.

[114] Federal Aviation Reauthorization Act of 1996, 49 USC 40101, 9 Oct 1996.

[115] Ibid.

[116] Ibid.

The Commission on Aviation Safety and Security's recommendations did meet with some success. In 1996, the FAA awarded six contracts to explosive detection technology manufacturers and ordered 54 explosive detection systems.[117] The FAA also received funding for 114 additional canine teams to augment technology based explosive detection measures, and FAA hired 300 new special agents to red team airport security.[118] Progress on an automated passenger profiling system had also been made. Northwest Airlines had been utilizing a passenger pre-screening program since 1996.[119] Through coordination between Northwest Airlines and the FAA, the implementation of the Computer Assisted Passenger Screening (CAPS) program began in 1998.[120]

Following the Presidential Commission's initial report however, GAO testimony in September 1996 on aviation security concluded that the aviation system still had significant flaws. The Federal Aviation Reauthorization Act of 1996 directed FAA to certify screening contractors, but by 2001, certification still was not complete.[121] The GAO testimony cited that, "Nearly every major aspect of the system, ranging from the screening of passengers, checked and carry-on baggage, mail, and cargo as well as access to secured areas within airports and aircraft, has weaknesses that terrorists could exploit."[122] Progress had been made at least in terms of security legislation, but the implementation of the security recommendations fell short of the intended operational application. Increased security measures meant increased security costs to the airlines. The lack of full implementation of many of the directed security initiatives left the security layers vulnerable.

---

[117] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 22-24.

[118] Ibid., 26.

[119] Paul Rosenzweig and Ha Nguyen, "CAPPS II Should Be Tested and Deployed," The Heritage Foundation, Available from http://www.heritage.org/Research/HomelandSecurity/BG1683.cfm (accessed 13 Sep 2007).

[120] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 25.

[121] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 8.

[122] United States General Accounting Office, *Aviation Security: Urgent Issues Need to be Addressed* (Washington, D.C.: GAO, 1996), 4.

2. Holes in the Layers – The Deficiencies

The aviation security system on September 11, 2001 was based on a layered system of security measures. The system was comprised of seven defensive layers composed of intelligence, passenger prescreening, airport access control, passenger checkpoint screening, passenger checked baggage screening, cargo screening, and on-board security.[123] The layered security concept can present a valid defense, but many of the layers on September 11 were porous, which once again placed aviation security concerns at the forefront of public and government concern. Even after two presidential commissions and two major legislative acts directed at improving aviation security, a GAO testimony at a Senate oversight hearing on Aviation Security in April 2000 cited that major vulnerabilities in the aviation security system still existed.[124]

The first layer was intelligence and in the scope of this study, intelligence pertains to aviation no-fly lists. In 2001, The FAA's no-fly list contained the names of persons that airlines were directed to deny commercial flight. However, in 2001, the FAA's passenger list contained less than 20 names.[125] By contrast, the State Department's watch list contained thousands of names of high interest persons.[126] The sharing of intelligence data, in this case terrorist lists with private companies or foreign air carrier governments was the concern and impediment.[127]

Passenger prescreening efforts in place in 2001 consisted of the Computer-Assisted Aviation Pre-Screening System (CAPS) program, developed in 1996.[128] CAPS would determine which passengers would undergo additional security scrutiny based on classified criteria. Under the FAA's rules however, if CAPS designated a traveler, air

---

[123] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 2.

[124] Gerald Dillingham, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 10.

[125] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 6.

[126] Ibid.

[127] Ibid., 4.

[128] Bart Elias, William Krouse and Ed Rappaport, *Homeland Security: Air Passenger Prescreening and Counterterrorism* (Washington D.C.: CRS, 2005), 6.

carriers were only required to screen the selectee's checked luggage for explosives or ensure the luggage was on the aircraft after the selectee boarded.[129] This logic was understandable in the wake of the Lockerbie incident. However, on 9/11, CAPS screened all nineteen hijackers, and only seven were designated as selectee's.[130] As a result, three of the selectee's had their bags screened for explosives and one had his bag held until he was confirmed on board the aircraft.[131] The other three hijackers did not check any luggage, which made their CAPS selection irrelevant.[132]

Airport access control posed an additional layer of security, although enforcement and compliance problems were significant. Access control is looked at in two respects, the background of the employees, and controlling access to secure areas. The background of security employees is significant as the objective is to sanitize the workforce from those with questionable backgrounds that may potentially compromise aviation security operations. The background checks that were mandated however, were based only on work history. FBI criminal checks were only required when there was a gap of 12 months or more in past employment history.[133] One review of six airports found that in 35% of the employee files reviewed, complete background checks were not accomplished and yet these employees were granted secure area access.[134] One contentious issue was the list of crimes that eliminated an employee from eligibility for secure area access. The list itself only contained 25 crimes, and did not include crimes such as assault with a deadly weapon, larceny, or drug possession.[135]

Access control was also weakened by the lack of enforcement of restricted area access. In 1999, the U.S. Department of Transportation Inspector General released the

---

[129] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 6.

[130] Ibid., 6-7.

[131] Ibid.

[132] Ibid.

[133] Alexis M. Stefani, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 24.

[134] Ibid., 28.

[135] Ibid., 24.

Airport Access Control Report. The report stipulated that at eight major airports, IG personnel were able to penetrate secure areas 117 times out of 173 attempts.[136] Agents were then able to board aircraft operated by 35 different carriers 117 times.[137] It is interesting to note that in 43 of the aircraft boardings, aviation employees ranging from flight crews to food service workers were also onboard but did not challenge the trespassers.[138]

Passenger checkpoint screening was the next layer of defense. Checkpoint screening involved a physical metal detector pass through stemming from aviation security measures of the 1970's and the X-ray screening of carry-on luggage for dangerous items such as guns or knives. These measures combined with the screener workforce made up the checkpoint screening system. This particular layer had continued to be plagued with sub par performance stemming from a lack of standards, training deficiencies and high turnover rates. A 1989 GAO report cited that the in-place passenger screening process could *not* ensure that firearms or explosives were prevented from being carried on board passenger aircraft.[139] Passenger screening was repeatedly addressed in testimony and aviation security commissions as an area of concern, primarily in training deficiencies, a lack of screening standards, and the quality and experience level of the screener.

Screener training was perhaps one of the most critisized areas of the passenger screening checkpoint. Since airlines were required to provide passenger security and usually sub-contracted that responsibility, there was no set standard in screener performance or training subject matter.[140] In addition, screeners were only required to have eight hours of training compared with the international average of forty hours.[141]

---

[136] Richard H. Bryan, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 6.

[137] Ibid.

[138] Ibid.

[139] United States General Accounting Office, *Proactive Management of FAA's Security Program Needed* (Washington, D.C.: GAO, 1989), 4.

[140] Ibid., 11.

[141] United States General Accounting Office, *Proactive Management of FAA's Security Program Needed* (Washington, D.C.: GAO, 1989), 37.

The 1996 Federal Aviation Reauthorization Act had directed FAA to certify security screening companies and to develop uniform security screening performance standards. However, GAO testimony in 2000 before the senate subcommittee on aviation, noted that neither of these initiatives was complete and that screener certification would not begin until 2002.[142] One additional note on standards or lack there of, was the FAA mandate to screen passengers for "dangerous items." Aside from guns, large knives, explosives or incendiary devices however, the FAA advised carriers to apply common sense as to what constituted a dangerous weapon.[143] The screening mandates themselves were ambiguous.

The screeners were also under watchful scrutiny. At many of the large airports, security screener turnover rates exceeded 100 percent per year.[144] In one year, one airport trained 1,000 screeners, and at the end of that year, only 140 remained.[145] The high turn over rate contributed to low screener experience levels and it impacted the supervisory capability of the security workforce. One of the primary reasons cited for the high turn over rate was the low hourly wage, which in 2000 averaged at $5.75 hour.[146] A low hourly wage combined with only a few hours of required training for a security screener softened the defensive layer of passenger checkpoint screening. Legislators continued to call on the need for technology to augment many security functions, yet the lynchpin in the equation was the lack of experience of the human operator. The lack of required training was the single most glaring deficiency in the U.S. civil aviation security system.[147]

Passenger checked baggage screening was an additional security layer. It relied on CAPPS, a Positive Passenger Bag Matching program, and the deployment of an explosive detection technology. By February 2000, CAPPS and a Positive Passenger

---

[142] Gerald Dillingham, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 8.

[143] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 8.

[144] Gerald Dillingham, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 7.

[145] Ibid.

[146] Ibid., 5-7.

[147] Jin-Tai Choi, *Aviation Terrorism* (New York: St. Martin's Press, 1994), 36-37.

Bag Matching program had been adopted by all major U.S. carriers.[148]   In addition, 111 Explosive Detection Systems and 552 Trace explosive detection devices had been deployed.[149]   However, airlines were not required to screen any more bags than the number of bags checked by selectees, and the Department of Transportation Inspector General's office testified that the explosive detection systems were underused.[150]   Over half of the explosive detection systems deployed were screening only 225 bags per day compared to the machines throughput capacity of 225 bags per hour.[151]   Another audit in 1999 revealed that screening personnel were not competent at operating the explosive detection equipment.[152]   Operators repeatedly failed detection tests because the operator would clear bags without searching them even though the machine had provided a warning.[153]   These performance failures unfortunately would point back to the ability of the operator and not necessarily the capability of the machine.

Another aviation security layer was cargo screening, specifically for cargos intended for transport in passenger aircraft.   As previously mentioned, commercial passenger aircraft routinely carry cargo in the aircraft belly along with passenger baggage. The 1996 Commission on Aviation Safety and Security had recommended that efforts should begin to address threats that could penetrate the aviation arena through the cargo venue.   The Commission recommended implementing known and unknown shipper profiles, shipper and forwarder employee screening procedures, and mandating the immediate examination of all cargo or move cargo onto only all-cargo carrier platforms.[154] The Commission also recommended the use of explosive detection systems to examine passenger airline cargo, and the development of a computer assisted cargo

---

[148] Thomas S. Hartwick, *Testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure*, Congress No. 106, Session No. 2, 16 Mar 2000.

[149] Ibid.

[150] Alexis M. Stefani, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 23-31.

[151] Ibid., 23.

[152] Ibid., 32.

[153] Ibid.

[154] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 19-54.

profiling system similar to the passenger screening system.[155] By 2000 FAA had implemented a known shipper program requiring cargo carriers and freight forwarders to establish security procedures for cargo from known and unknown shippers.[156] However, explosive detection systems were not developed, nor was legislation enacted to mandate it.[157]

The final defensive layer, comprised primarily of on-board security, was fairly limited. The Federal Air Marshal program was still active in 2001, but agent numbers had dwindled down to only 33 prior to September 11.[158] The Federal Air Marshals had also been directed to fly almost exclusively on international flights, not domestic.[159] Flight crews were trained to the "common strategy," cooperate with hijackers to eventually get the aircraft on the ground safely."[160] This latter notion no doubt was a protocol based on hijackings of earlier eras in which cooperation would eventually garner the release of passengers and crew.

A Department of Defense agency, Northern American Aerospace Defense Command (NORAD), which was operationally active, represented a last-chance measure in the final security layer. While NORAD was charged with the defense of the U.S. against airborne threats, its focus was on threats coming from outside U.S. borders.[161] The 9/11 Commission found NORAD unprepared to deal with a threat from within.[162] NORAD's alert fighter bases had dwindled in number to only seven with two aircraft on

[155] White House Commission on Aviation Safety and Security, *Final Report to President Clinton* (Washington D.C: 1997), 19-54.

[156] Bartholomew Elias, *Air Cargo Security* (Washington D.C.: CRS, 2003), 17.

[157] Ibid., 18.

[158] United States Congress, *Plane Clothes: Lack of Anonymity at The Federal Air Marshal Service Compromises Aviation and National Security*, Investigative Report by the Committee on the Judiciary (Washington D.C.: 2006).

[159] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 10.

[160] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 10-85.

[161] Ibid., 428.

[162] Ibid., 31.

alert at each base.[163] And while NORAD's training scenarios did occasionally address hijacked aircraft, the scenarios were focused on aircraft coming from overseas.[352]

The layers were in place, however, for the most part, each layer was hampered to some degree. One additional weakness that was noted in many reports was the lack of security foresight or of a strategic aviation security plan. This resulted in a reactive-security measure-implementation cycle. The weaknesses of the security system were highlighted after each major disaster and reactive measures were put in place to fix or rectify the fault. These fixes however, were not always carried through, or required extensive time to achieve completion. The 9/11 Commission noted that efforts to pass checkpoint screener performance regulations, implement anti-sabotage measures, and aviation security assessments were ongoing, but there were no increases in security measures in response to heightened threat levels in the spring and summer of 2001.[164]

Many security initiatives had been proposed over the course of the aviation-hijack historic timeline, and some were implemented. Leading up to 9/11, however, forty-two government reports had highlighted flaws or weaknesses in domestic aviation security.[165] The security layers were not impregnable and flaws in the security system still existed. As aviation hijackings faded from news headlines and the forefront of domestic concern, so to did the perceived threat to aviation. It would instead take another hi-jacking event of magnanimous proportions on September 11, 2001 to once again re-invoke the cycle of aviation security change.

---

[163] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.17* (Washington D.C.: 2004), 2.

[164] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 5.

[165] Marla Felcher, "U.S. Aviation Security: Before and After the September 11 Attacks," Understanding Government, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 6.

III.   AVIATION SECURITY ENHANCEMENTS

The events on September 11, 2001 once again brought aviation security to the center stage. The apparent cyclic nature of aviation security enhancements would begin again in the aftermath of one of the largest aviation related disasters in U.S. But the magnitude of the U.S.'s reaction would be significantly larger for many reasons. First, the September 11 hijackings were a terrorist incident that occurred within the continental U.S., not overseas. Second it involved multiple commercial airliners not just a single aircraft. Third it was a successful attack, 75% of the weapons used struck their targets. A fourth reason was the sheer magnitude of the attack, which killed 2,973 persons.[166] Finally, a contributing factor was the media coverage of the incident itself. The graphic nature captured on film of the second airliner impacting the World Trade Center, persons jumping to their death, and the collapse of both towers left an indelible impression. These reasons would fuel the entire nation to enact and support a wide spectrum of counterterrorist measures. Given the method of attack chosen by 9/11 terrorists, a logical choice was to focus efforts once again on aviation security.

Immediately following the 9/11 attacks, all aviation within the United States was grounded. Most of the nation's airports re-opened two days later, but there were noticeable changes in security measures. Curbside and offsite check-in was no longer available as passengers could only check in at airline ticket counters.[167] Only ticketed passengers could now proceed past the security checkpoints, and aircraft would be thoroughly searched prior to passenger boarding.[168] Vehicles could not be parked closer than 300 feet to passenger terminals, and passengers were no longer allowed to carry

---

[166] CNN, "U.S. deaths in Iraq, war on terror surpass 9/11 toll," CNN Online, Available from http://edition.cnn.com/2006/WORLD/meast/09/03/death.toll/ (accessed 28 Sep 2007).

[167] United States Department of Transportation, "Airports to Remain Closed, Mineta Says," Available from http://usinfo.state.gov/is/Archive_Index/Airports_to_Remain_Closed_Mineta_Says.html (accessed 14 Sep 2007).

[168] Ibid.

knives or cutting instruments on board, regardless of the blade size.[169]   Fighter caps were activated across the nation and NATO deployed E-3A Airborne Early Warning aircraft to patrol the skies over the U.S. These security implementations were immediate responses, but legislation shortly followed that would make significant organizational changes and continue to have a dramatic effect on aviation security.

A.   AVIATION AND TRANSPORTATION SECURITY ACT

The Aviation and Transportation Security Act was passed on November 19, 2001 and it brought sweeping changes to aviation and transportation security. Most, if not all of the current security measures were either created or redefined by this act; it essentially affected every layer of security in aviation. Two of the most significant changes the act instituted were the establishment of a new security organization and the federalization of aviation screeners.

The Aviation and Transportation Security Act created the Transportation Security Administration (TSA) under the Department of Transportation and assigned the head of the administration the responsibility of securing all modes of transportation to include aviation.   This move was significant because it severed the dual and sometimes competing missions of the Federal Aviation Administration, to promote civil air transportation while simultaneously ensuring its security. These two missions were often at odds. Any initiative put forth by FAA to stiffen security was usually rebutted by the airlines as being too costly or inducing inefficiency in passenger throughput. TSA was now able to focus solely on aviation security without the need for airline consensus.

The second significant action of the act was to establish a federal screener workforce. The screener workforce was now hired and trained by TSA in accordance with federal standards, not contracted to private companies by the airlines. TSA was also responsible for managing and testing its screener workforce to those standards in order to establish uniform screening procedures at all airports. Screener supervision was also

---

[169] Paul Zielbauer and John Sullivan, "After the Attacks: Airport Security; F.A.A. Announces Stricter Rules; Knives No Longer Allowed," *The New York Times,* 13 Sep 2001, Available from http://query.nytimes.com/gst/fullpage.html?res=9C07E6DC1038F930A2575AC0A9679C8B63 (accessed 14 Sep 2007).

addressed by requiring Federal Security Managers at all U.S. airports.[170] The Homeland Security Act of 2002 reorganized over 22 agencies and 170,000 employees, including realigning TSA under the Department of Homeland Security.[171] This move strengthened the weight of the newly created Transportation Security Administration, now backed by the sole government agency charged with homeland security for all critical infrastructure related transportation. While the Aviation and Transportation Security Act provided the nuts and bolts of aviation security, another composed plan of action would provide aviation security the foundations of purpose and mission.

B.   NATIONAL STRATEGY FOR AVIATION SECURTIY

The National Strategy for Aviation Security was released on 26 March 2007 following President Bush's direction to establish a comprehensive strategy to protect the nation from air threats.[172] The strategy's overarching purpose is to align Federal, State, local governments and the private sector into a cohesive, active, multi-layered security system.[173] It seeks to accomplish this in part by establishing national objectives, principles and goals in order to secure the aviation system. These are critical components to recognize. This strategy is what will allow and facilitate securing the aviation system. Having a strategy in place that provides general direction reduces the reactive nature of past security measures implementations.

1.   Focus and Aim Points

The Strategy is the overarching plan, and it is supported by seven supporting plans each with its own focus. The Aviation Transportation System Security Plan addresses measures being put into place to secure the aviation transportation system. It

---

[170] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001) Available from http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf (accessed 14 Sep 2007).

[171] Joseph S. Szyliowicz, "Aviation Security: Promise or Reality?" in *Homeland Security and Terrorism*, ed. Russell Howard, James Forest and Joanne Moore, 112 (New York: McGraw-Hill, 2006).

[172] George W. Bush, *The National Strategy for Aviation Security* (Washington, D.C.: 2007) Available from http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf (accessed 17 Aug2007).

[173] Ibid.

also clearly defines roles and responsibilities, which is important given the number of government agencies involved. For example, the Security Plan establishes that TSA is responsible for the vetting of passengers and aircrews flying into or out of the country, while Customs and Border Patrol is responsible for detecting, identifying and interdicting potential air threats.[174]

The Aviation Operational Threat Response Plan details immediate or direct action responses when either intercept operations, surface to air operations or on board armed action is deemed necessary.[175] Furthermore, this plan directs the integration of national level command centers to facilitate information flow and command decisions, which are required as rapidly as events unfold in the air domain.[176] This plan also establishes lead and supporting agencies, as well as roles and responsibilities depending on the situation at hand. For instance, TSA is exclusively responsible for directing law enforcement activity regarding passenger safety onboard still grounded hijacked aircraft once all external doors of the aircraft are closed, and until those doors are opened.[177]

The Aviation Transportation System Recovery Plan is the third supporting plan, and it delineates measures of recovery for the aviation system in the event of attack in both economic and operational aspects.[178] This plan along with the aforementioned two supporting plans make up the three main tiers of response options to counter aviation system threats: secure it, destroy the threat if security fails, and recover from the attack should one occur.

The Air Domain Surveillance and Intelligence Plan focuses primarily on integrating and sharing intelligence, information and surveillance data in order to create a

---

[174] United States Department of Homeland Security, *Aviation Transportation System Security Plan* (Washington, D.C.: 2007), Available from http://www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf (accessed 17 Aug 2007), 5-6.

[175] United States Department of Homeland Security, *Aviation Operational Threat Response Plan* (Washington, D.C.: 2007), Available from http://www.dhs.gov/xlibrary/assets/hspd16_opthreatrespplan.pdf (accessed 17 Aug 2007), 1.

[176] Ibid.

[177] Ibid., 8.

[178] George W. Bush, *The National Strategy for Aviation Security* (Washington, D.C.: 2007), Available from http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf (accessed 17 Aug 2007).

shared situational awareness among federal, state and local governments as well as international agencies.[179] The International Aviation Threat Reduction Plan addresses countering the acquisition of stand off weapons that could pose a threat to aviation operations.[180] The remaining two supporting plans, the Domestic Outreach Plan and the International Outreach Plan both focus on gaining domestic or international stakeholder cooperation in an effort to reduce aviation security vulnerabilities, with the latter plan being heavily dependant on the efforts of the State Department.

These documents as a whole, prescribe an overarching framework to support aviation security enhancement. The strategy provides the foundation upon which security enhancements since 9/11 can be built, and many of those enhancements are still in place and operational.

C. IMPLEMENTED MEASURES – WALKING THROUGH THE NEW LAYERS

1. Commercial Passenger Aviation

The Aviation Transportation System Security Plan designates the first two commercial aviation security layers as the Passenger, Employee and Crew Security Assurance layer and the Threat Object Screening and Detection layer, the former dealing with access to the aviation system and the latter dealing with passenger and baggage screening. The Aviation Operational Threat Response Plan addresses a third layer. These re-designated layers are not new, but significant changes have been implemented to these layers following 9/11, mainly as a result of the aforementioned Aviation and Transportation Security Act.

---

[179] United States Department of Homeland Security, *Air Domain Surveillance and Intelligence Integration Plan* (Washington, D.C.: 2007), Available from http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf (accessed 17 Aug 2007), 2.

[180] Ibid.

a.   *Access to Tickets and Terminal*

The Passenger, Employee and Crew Security Assurance layer employs multiple security measures in an attempt to limit access to commercial aviation to both passengers and employees with non-malicious intent. The first security measure checks passengers against an integrated list of known or suspected terrorists. Aviation watch lists evolved in the 1990s to reduce the terrorist risk to aviation, and to track drug smugglers.[181] But, different government and intelligence agencies each kept their own watch lists, which impeded any type of consolidated effort.[182] To correct this problem, the Aviation and Transportation Security Act directed TSA to establish database-sharing agreements with federal agencies. These databases would contain the names of persons of interest that could pose a risk to transportation or to national security, and TSA was required to promulgate that information to airlines.[183]

To facilitate the consolidation and distribution of watchlist data, the Terrorist Screening Center (TSC) was established in December 2003.[184] Administered by the FBI, the TSC merges information from multiple agencies and intelligence organizations into a Terrorist Screening Database that contains over 238,000 records, which TSA distributes a subset of to the airlines as no-fly or automatic selectee lists.[185] Assistant Secretary of Homeland Security for TSA, Kip Hawley stated that the

---

[181] Alan Gathrite, "No-fly list ensnares innocent travelers," *San Francisco Chronicle,* 8 Jun 2003, Available from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/06/08/MN253740.DTL (accessed 10 Sep 2007).

[182] Douglas Farah, *Blood From Stones,* (New York: Broadway Books, 2004), 184.

[183] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[184] United States Department of Justice, *Fact Sheet: The Terrorist Screening Center,* (Washington D.C.: 2003) Available from http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm (accessed 10 Sep 2007).

[185] William J. Krouse and Bart Elias, *Terrorist Watchlist Checks and Air Passenger Prescreening*, (Washington D.C.: CRS, 2006), 2-4.

employment of the no-fly list "stops people you would not want on your flight," and alluded to the fact that positive no-fly list passenger matches occur multiple times a week.[186]

Currently however, the airline, not TSA, is still responsible for screening passengers against aviation security no-fly and automatic selectee lists.[187] TSA is not scheduled to take over passenger no-fly list screening until Secure Flight, the next automated passenger prescreening program becomes operational in 2008.[188] TSA was directed to ensure that the next generation Computer-Assisted Passenger Prescreening System, CAPPS II, evaluated all passengers prior to boarding, but this system was abandoned in 2004 due to privacy and information data mining concerns.[189] As a result, CAPS, renamed to the Computer-Assisted Passenger Pre-Screening System (CAPPS) is still in use today. However, the system has been modified so that CAPPS selectee's are now subject to further searches of their persons as opposed to just their checked luggage as was the case prior to 9/11.[190]

Within this security layer, TSA also employs both uniformed and plain clothed Behavior Detection Teams modeled after a successful Israeli security tactic.[191] Behavior Detection Teams observe passenger behavior in an effort to identify unique behavior cues.[192] Behavior Detection Teams receive fifty-six hours of training to detect micro-expressions, or subtle facial muscle movements, which may identify suspicious

[186] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

[187] Bart Elias and William J. Krouse, *Terrorist Watchlist Checks and Air Passenger Screening* (Washington D.C.: CRS, 2006), 3.

[188] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

[189] John Frittelli, *Transportation Security: Issues for the 109th Congress* (Washington, D.C.: Congressional Research Service, 2005), 3.

[190] Bart Elias, William Krouse and Ed Rappaport, *Homeland Security: Air Passenger Prescreening and Counterterrorism,* (Washington D.C.: CRS, 2005), 7.

[191] Thomas Frank, "Airport Security arsenal adds behavior detection," USA Today, 25 Sep 2007, Available from http://www.usatoday.com/travel/flights/2007-09-25-behavior-detection_N.htm?csp=34 (accessed 10 Oct 2007).

[192] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

patterns of behavior or intent.[193] Behavior observation detection teams have identified over 150 people that upon further investigation, were subsequently arrested, crediting the success of the program.[194]

The second half of the Security Assurance Layer, employee access to the aviation system was also heavily scrutinized. All employees with regular access to aircraft and secure areas were required to have background checks which now include both a criminal history check coupled with a review of law enforcement databases.[195] Approximately 900,000 airport workers with unescorted access to secure areas underwent a fingerprint-based criminal history records check by December 6, 2002.[196] And by April 2004, fingerprint-based checks and watch list verifications were completed for an additional 100,000 airport workers who perform duties in sterile areas (the indoor gate area past the security check point).[197] These same requirements are also required for security screeners.[198]

Measures to improve access control to secure areas were also improved. In October 2007, airports began issuing secure area badges to employees only after criminal background checks are complete.[199] Also, the Aviation and Transportation Security Act directed TSA to regularly assess and test access control compliance with federal requirements.[200] It essentially stipulated that the same level of protection applied

---

[193] Thomas Frank, "Airport Security arsenal adds behavior detection," USA Today, 25 Sep 2007, Available from http://www.usatoday.com/travel/flights/2007-09-25-behavior-detection_N.htm?csp=34 (accessed 10 Oct 2007).

[194] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

[195] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[196] United States General Accounting Office, Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Control (Washington D.C.: GAO, 2004), 27.

[197] Ibid.

[198] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[199] Transportation Security Administration, "TSA Provides Another Layer of Security to Airport Employee Hiring," TSA Website, Available from http://www.tsa.gov/press/happenings/sida.shtm (accessed 22 Oct 2007).

[200] United States General Accounting Office, Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Control (Washington D.C.: GAO, 2004), 10.

to passengers and luggage should also be applied to any individual, goods or vehicles requiring entry into a secure area.[201]   To meet this requirement, TSA performs compliance inspections as well as covert testing and vulnerability assessments.[202]   In 2004, TSA inspections found a high percentage of airport operators in compliance with access control security requirements.[203]   It is also interesting to note that TSA's inspection technique is one of cooperation when non-compliance issues are discovered. Resolution is centered on a cooperative effort to determine why compliance failed and to find a solution, as opposed to the use of penalties such as administrative action or civil monetary penalties.[204]

b.   Terminal to Gate

The Threat Object Screening and Detection layer shifts the focus somewhat from detecting persons to detecting objects or weapons.   While Behavior Detection Teams and TSA Officers continue to observe and monitor passengers, the detection devices at security checkpoints are a significant element of this phase. Getting to the checkpoints however, is now only allowed for ticketed passengers, which is a change since 9/11.   This simple security measure was noted in a 2000 GAO congressional testimony as a usefully employed measure in five other countries.[205]   The implementation of this measure reduced the volume of persons that required screening, while also simultaneously reducing the volume of persons in the follow-on sterile area. Transportation Security Officers add an additional security measure by performing travel document checks prior to or at the security checkpoint, ensuring the traveler,

---

[201] United States, 107th Congress, <u>Aviation and Transportation Security Act of 2001, Pub. L. 107-71,</u> (Washington D.C.:2001).

[202] United States General Accounting Office, *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Control* (Washington D.C.: GAO, 2004), 10.

[203] Ibid., 11.

[204] Ibid., 12.

[205] Gerald Dillingham, *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*, Congress No. 106, Session No. 2, 6 Apr 2000, 14.

identification, and airline ticket match, and that the traveler identification is authentic.[206] Again, a simple measure to implement, which reduces the security gap by ensuring the ticket purchaser, whose name has been checked against a no-fly list, is the same person as the actual traveler.

Once at the security checkpoint, ticketed traveler compliance is essentially required in order to proceed. Passengers and carry-on luggage are still screened at the checkpoint through metal detectors and x-ray machines, however, beginning in 2004, TSA required all passengers to remove outer coats and jackets for X-ray before walking through the metal detector.[207] Computers require removal from carrying cases, and while it is not officially required, shoe removal is performed in lieu of facing the penalty of secondary screening selection.[208] Explosive Trace Detection machines were also installed at the checkpoint screening location to screen carry-on baggage for explosives. TSA screeners swab the luggage and the swab is then chemically analyzed for explosive residue or vapor.[209] A passenger designated as a selectee by CAPPS or other TSA procedure to receive additional screening, is either screened by hand-wand or a physical pat-down and their carry-on items are screened for explosives traces or physically searched.[210] Passengers whose carry-on baggage alarms the X-ray machine or who trip the walkthrough metal detector will receive the additional screening as well.[211]

Carry-on items that were once allowed to pass such as nail files, scissors, pocketknives regardless of blade length, matches and lighters containing fuel are

---

[206] Transportation Security Administration, "TSA Continues to Extend Security Beyond the Checkpoint, Assuming Document Checking Responsibility at Airports from Coast to Coast," TSA Website, Available at http://www.tsa.gov/press/happenings/document_checking.shtm (accessed 10 Oct 2007).

[207] Robert Longley, "Air Passengers Must Remove Coats For Security Screening" About.Com: US Gov Info / Resources, Available from http://usgovinfo.about.com/od/defenseandsecurity/a/coatsoff.htm (accessed 8 Oct 2007).

[208] George McClure, "Has Airport Security Improved Since 9/11?" IEE-USA Today's Engineer Online, Available from http://www.todaysengineer.org/2005/Jun/security.asp (accessed 8 Oct 2007).

[209] United States General Accountability Office, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved* (Washington, D.C.: GAO, 2007), 9.

[210] Ibid., 8-9.

[211] Ibid.

prohibited.[212] Although pointed scissors with a blade length less than four inches and tools less than seven inches in length are now authorized in carry-ons.[213] With the exception of medication and baby foods, which must be declared, carry-on liquids are now only allowed in bottled quantities of three ounces or less, they must fit inside a one-quart plastic bag, and only one bag is allowed per person.[214] TSA implemented this rule on 10 August 2006 following the foiled liquid bomb plot at Heathrow airport. The "three ounce bottle and bag rule" still allows a traveler to bring liquids onboard, while also mitigating the liquid bomb threat. TSA felt that if the quantity of liquid allowed is small enough, regardless of the liquid type, it would be non-threatening.[215] This eliminated the need for screeners to determine exactly what type of liquid is in every bottle of carry-on luggage.[216] Subsequently, if a screener finds the traveler or the contents of the bag suspicious, additional screening procedures may be taken such as conducting an interview, or closer examination of the travelers' carry-ons.[217] Pat-down searches were also authorized as part of the secondary screening process if warranted based on observations.[218] Random bag searches were also implemented following the Heathrow incident, as an additional security measure.[219]

Luggage placed in the aircraft belly has always been viewed as a potential weak point in aviation security. 100 percent checked baggage screening had always been

[212] Duane Woerth, Testimony before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the Committee on Homeland Security, Congress No. 109, Session No. 1, 16 May 2005.

[213] Transportation Security Administration, "Permitted and Prohibited Items," TSA Website, http://www.tsa.gov/travelers/airtravel/prohibited/permitted-prohibited-items.shtm#3 (accessed 20 Oct 2007).

[214] Transportation Security Administration, "3-1-1 for Carry-Ons," TSA Website, http://www.tsa.gov/311/index.shtm (accessed 12 Oct 2007).

[215] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

[216] Ibid.

[217] Ibid.

[218] Robert Longley, "Air Passengers Must Remove Coats For Security Screening" About.Com: US Gov Info / Resources, Available from http://usgovinfo.about.com/od/defenseandsecurity/a/coatsoff.htm (accessed 8 Oct 2007).

[219] MSNBC, "U.S. air passengers face increased air security," MSNBC Online, Available from http://www.msnbc.msn.com/id/14282396/ (accessed 11 Sep 2007).

trumped in lieu of baggage loading efficiency to minimize ground delays and airline claims of limited manpower. Prior to 9/11, only 5 percent of checked baggage was being screened for explosives.[220] Following 9/11 however, the Aviation and Transportation Security Act mandated that TSA install explosive detection machines in all commercial airports no later that 31 Dec 2002, and that all checked baggage would be screened by those systems.[221] TSA met the Congressional deadline by deploying more than two thousand detection machines by the end of 2002.[222] Deployments continued through June 2006 amounting to 1,600 Explosive Detection Systems and over 7,000 Explosive Trace Detection machines deployed through which all checked bags now pass prior to loading.[223] TSA has also increased the use of canine patrols trained in the detection of explosives.[224]

The Threat Object Screening and Detection layer depends not only on screening technology, but more so on the persons who operate the machines and the checkpoints. In an effort to alleviate the low performance of private screening efforts, the Aviation and Transportation Security Act mandated the deployment of federal screeners by November 2002.[225] The act also required the screeners to be proficient using new technology, and that they could recognize new weapons and threats.[226] In 2002, the

---

[220] Grace Jean, "Focus On Checked Baggage Screening Has Detracted From Aviation Security," National Defense Available from http://www.nationaldefensemagazine.org/issues/2007/March/FocusonChecked.htm (accessed 17 Oct 2007).

[221] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[222] Marla Felcher, "Before and After the September 11 Attacks," *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 2.

[223] United States Government Accountability Office, *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain* (Washington D.C.: GAO, 2007), 13.

[224] United States General Accountability Office, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved* (Washington, D.C.: GAO, 2007), 29.

[225] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[226] Ibid.

Department of Transportation submitted its federal plan for security screener training.[227] Included in the training were now standardized procedures to search carry-on bags, explosive detection machine image interpretation, and methods to detect concealed knives.[228] Now the checkpoint screening system was not only composed of screeners and technology, but now included standardized procedures for how to conduct screening.[229] These standards now provide a benchmark to measure against during TSA covert and overt self-inspections.

By November of that year, TSA had met its mandated deadline by hiring more than 55,000 screeners.[230] Federal screeners were now required to be a U.S. citizen, speak fluent English, and had to pass a criminal background check.[231] In one year, federal screeners confiscated nearly five million items ranging from 1.4 million knives to nearly 40,000 box cutters.[232] TSA's current screener training program entails three main pillars: the basic skill set for passenger and baggage screening, re-currency training, and technical training and certification for operating explosive detection devices.[233] Applying the recurrent training concept, federal screeners are now provided with weekly reports that identify new aviation threats, and examples of new concealment techniques

[227] The Department of Homeland Security, *Administration Homeland Security Actions Since September 11* (Washington D.C.: DHS, 2002), 22.

[228] Marla Felcher, "Before and After the September 11 Attacks, *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 8.

[229] United States General Accountability Office, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved* (Washington, D.C.: GAO, 2007), 10.

[230] Norman J. Rabkin, *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts* (Washington, D.C.: GAO, 2004), 9.

[231] Marla Felcher, "Before and After the September 11 Attacks, *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 7.

[232] Joseph S. Szyliowicz, "Aviation Security: Promise or Reality?" in *Homeland Security and Terrorism*, ed. Russell Howard, James Forest and Joanne Moore, 112 (New York: McGraw-Hill, 2006).

[233] Norman J. Rabkin, *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts* (Washington, D.C.: GAO, 2004), 11.

are also provided.[234] Screeners are also given threat briefings before and after each shift much the same as the proven military technique used in scenarios facing an operational threat.[235]

Many additional security measures are purposefully not discussed here such as the automated shoe scanner, millimeter wave passenger imaging technology and bottled liquid scanners, primarily because these technologies are not fully implemented. Many of these systems are deployed at some airports as pilot test beds, but they are not yet fully deployed at every airport as a standard equipment compliment to the security checkpoint.

c. Take Off / In-Flight

Once passengers are on board the aircraft, they have unknowingly entered the final layer of response options. Many of these options fall under the Aviation Operational Response Plan, when direct action may be required or implemented. Measures such as hardened cockpit doors and Temporary Flight Restrictions provide passive security measures, while on board air marshals and armed pilots provide active, final measures of on board security.

The Aviation and Transportation Security Act required the strengthening of cockpit doors and locks in an effort to make them impenetrable from the passenger side of the door.[236] The doors were also ordered to remain closed and locked during flight. As a result, FAA created new standards that required aircraft operators of more

---

[234] United States General Accountability Office, *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved* (Washington, D.C.: GAO, 2007), 19.

[235] Ibid.

[236] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

than 6,000 aircraft to install reinforced doors by April 2003.[237] These standards were designed not only to protect cockpits from intrusion, but also from small arms fire and fragmentation devices.[238]

A second passive security measure used in the final defensive layer is a Temporary Flight Restriction (TFR). Aviation eventually resumed over the U.S., in September 2001, however in an attempt to mitigate the risk of another 9/11, TFRs were and still are employed to minimize flight traffic over areas of national interest. A TFR is a four dimensional area of airspace defined by height, width, altitude and time in which air traffic is restricted to fly into. FAA or the Department of Defense establish TFRs or no-fly areas in the vicinity of or over national monuments, VIP movement areas, or areas of high interest such as chemical weapons storage depots.[239] Even national events such as the Indianapolis 500 or the 2006 Super Bowl warranted the need for a TFR.[240] There are also standing TFRs over Disneyland and Disney World in addition to the TFR that was placed around the nations capitol region that is still in effect. The second use of a TFR is to enhance situational awareness. By eliminating aircraft movement in a particular area, it becomes easier for both FAA controllers and Air Force Air Defense Sector personnel to monitor and identify aircraft that violate an active restricted area. Should an aircraft penetrate a TFR, direct action may be the only resort available, whether that action is from military fighters or armed personnel onboard.

The Aviation and Transportation Security Act revived the Federal Air Marshal force once again. Thousands of new air marshals were recruited, trained, and

---

[237] George W. Bush, *The Department of Homeland Security: Administration Homeland Security Actions Since September 11*, The White House, Available from http://www.whitehouse.gov/deptofhomeland/sect8.html (accessed 13 Oct 2007).

[238] CBS News, "Bulletproof Cockpit Doors a Reality," CBS News Online, Available from http://www.cbsnews.com/stories/2003/04/04/attack/main547827.shtml   (accessed 13 Oct 2007).

[239] Aircraft Owners and Pilots Association, "Senate to consider enhanced TFR enforcement over weapons storage facilities," AOPA Online, Available from http://www.aopa.org/whatsnew/newsitems/2002/02-3-138x.html (accessed 6 Dec 2006).

[240] Aircraft Owners and Pilots Association, "Serious security — Air Force says it will shoot Super Bowl TFR violators," AOPA Online, Available from http://www.aopa.org/whatsnew/newsitems/2006/060203superbowl.html accessed (6 Dec 2006).

deployed daily on twenty thousand domestic flights.[241] Non-stop, long distance flights, such as those hijacked on 9/11 were designated as a priority to have air marshals aboard.[242] The security act also permitted law enforcement personnel from federal, state and local governments to carry their firearm on board to assist air marshals, essentially increasing the size and coverage of the defensive measure.[243]

The arming of onboard personnel does not stop with law enforcement and Federal Marshals. The Federal Flight Deck Officer program was also initiated authorizing airline pilots to receive specialized training to qualify as an armed Federal Flight Deck Officer.[244] TSA has been training approximately one hundred officers a week, and expanded the program to also include cargo pilots and other flight crew members such as flight engineers.[245] By 2003, approximately five thousand commercial pilots had been trained as a Federal Flight Deck Officer.[246]

While Federal Air Marshals and armed pilots provide a direct action capability on board commercial passenger aircraft, Department of Defense assets are also on standby to provide an added measure of response in a final effort to thwart an aircraft hijacking. Organizationally, Northern Command has been established as a new unified command with the responsibility of defending the United States.[247] A rejuvenated North American Aerospace Defense Command is now the lead agency for Operation Noble Eagle, the protection of the Continental U.S. from airborne threats, which include those

---

[241] Marla Felcher, "Before and After the September 11 Attacks, *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 7.

[242] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[243] Ibid.

[244] Ibid.

[245] John Frittelli, *Transportation Security: Issues for the 109th Congress* (Washington D.C.: CRS, 2005), 5.

[246] Marla Felcher, "Before and After the September 11 Attacks, *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 11.

[247] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 427-428.

threats that originate from *within* U.S. borders.[248]   With its re-validated mission, NORAD's alert aircraft sites rose to thirty in 2002, up from the seven sites that were active on 9/11.[249] Military fighters now fly random Combat Air Patrols (CAP) over the nation under the control of Air Defense Sectors whose radar picture is now fused with FAA's radars, providing NORAD with an "inward look." And by 2005, NORAD's alert fighters had been scrambled nearly 1000 times since 9/11.[250] In the first ten months of 2004 alone, airborne fighters were committed from their CAPs more than 450 times to investigate aircraft of interest.[251] The Coast Guard as well as the Customs and Border Patrol also perform the air intercept mission.[252] These direct action measures are the last layer of defense against a hijacked aircraft, although one variable remains, the passengers onboard.

There are two additional security measures that are new to this layer, crew training and the response of the passengers on board. Since 9/11, an attitude of no tolerance seems to permeate among both passengers and crew. Flight crew and passengers are more active at reporting suspicious behavior and they are more likely to take decisive action when threatened.[253]   The anti-hijack training procedures taught to airline crews following September 11, were altered dramatically; pilots are now trained to confront and eliminate the hijack threat as opposed to follow the "common strategy" of cooperation.[254] In 2002, a passenger on a flight from Miami kicked in the bottom of the cockpit door and managed to gain partial access into the cockpit until the co-pilot hit him

[248] North American Aerospace Defense Command, *About NORAD,* Available from http://www.norad.mil/about/CONR.html (accessed 17 Oct 2007).

[249] Adam J. Hebert, "Noble Eagle Without End," *Air Force Magazine* 88, no.2 (2005), Available from http://www.afa.org/magazine/feb2005/0205eagle.asp (accessed 17 Oct 2007).

[250] Ibid.

[251] Ibid.

[252] Military.com, "CG Assumes National Capitol Region Intercept Mission," Available from http://www.military.com/features/0,15240,114999,00.html (accessed 17 Oct 2007).

[253] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html   (accessed 10 Oct 2007).

[254] Duane Woerth, Testimony before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the Committee on Homeland Security, Congress No. 109, Session No. 1, 16 May 2005.

in the head with an axe.[255] These changes in hijack training were directed in the Aviation and Transportation Security Act and included self-defense training, as well as defensive aircraft maneuvers.[256]

Passenger tolerance seems to have also been affected. Prior to 9/11, passengers tended to comply more than resist during a hijack event. In 1991, a counterterror study center in Canada released a list of the fifteen things a passenger can do during a hijacking, the first was don't be a hero, the fourth, try to rest, and the sixth, don't try to escape.[257] Following the events of 9/11 however, passengers seem to translate their lowered tolerance for hijacking into physical reaction. Such was the case of the passengers attempting to overtake the hijackers on Flight 77 after having learned of the two World Trade Center impacts on 9/11. Passengers also came to the aide of a flight attendant to successfully subdue shoe bomber Richard Reid on American Airlines Flight 63 in December 2001.

9/11 set the stage for our defensive build up of the commercial aviation sector. The Aviation and Transportation Security Act of 2001 put forward and implemented some of the most significant changes to date within the aviation security arena. From the establishment of new organizations, to the standing, overt, military defense operations, aviation security has been riddled with an extensive overhaul. Even passenger attitude is no longer one of compliance, but one of survival. Every layer of aviation security has either been strengthened with additional security measures or new layers have been added.

---

[255] CBS News, "Bulletproof Cockpit Doors a Reality," 4 Apr 2003, Available from http://www.cbsnews.com/stories/2003/04/04/attack/main547827.shtml (accessed 13 Oct 2007).

[256] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[257] Peter St. John, *Air Piracy, Airport Security, and International Terrorism* (New York: Quorum Books, 1991), 125.

IV. ASSESSING THE EFFORTS

A. ASSESSMENT

Pre and post 9/11 security layers have different names and vary in number. To facilitate a security measure comparison, three categories or layers are used to group security measures: Access, Physical Security, and Direct Action. The Access layer focuses on security measures to limit access of both passenger and employees to the aviation system. The Physical Screening layer encompasses measures and procedures to physically screen passengers, and carried or checked luggage. And finally, the Direct Action layer involves armed intervention and measures to support or prevent airborne intervention.
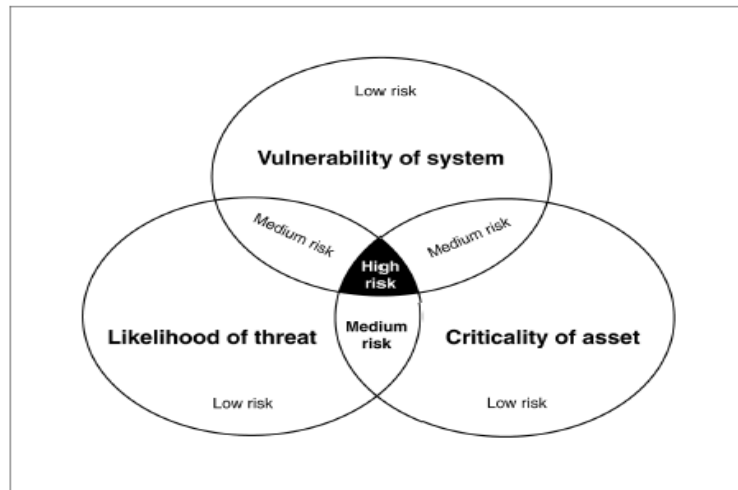

Figure 1.   Risk Management Approach[258]

Figure 1 illustrates a risk management approach to help focus aviation security efforts.[259]   Three variables are involved, the likelihood of threat, the criticality of the asset, and the vulnerability of the system. Focusing efforts where all three variables meet

---

[258] United States General Accounting Office, *Aviation Security: Efforts to Measure Effectiveness and Address Challenges* (Washington D.C.: GAO, 2003), 14.

[259] Ibid.

will aid in using limited resources in the most efficient manner. This model can also be used however, to illustrate the effectiveness of adding or strengthening additional layers of security when applied to commercial passenger aviation. The first two variables, the likelihood of the threat and the criticality of the asset remain constant. The likelihood of the threat to commercial aviation, specifically commercial airliners is historically proven with over 238 hijacking attempts on U.S. aircraft from 1930-1984 and eighty-seven explosions aboard aircraft between 1949 and 1985.[260] The criticality of the asset in this respect is the commercial airliner, which is of course the means of conveyance and the critical cog in the aviation system. The third variable then, vulnerability of the system can be manipulated or reduced through increased measures of security. Risk, in this case the chances of a terrorist attack or hijacking cannot be eliminated, but enhancing protection from those existing or potential threats can help reduce risk.[261]

Table 1 illustrates the pre and post 9/11 security measures aligned by security layer. The number of security measures within the Access layer has been increased two fold with the employment of observation teams and document checkers. However, improvements of existing passenger and employee access measures are more predominant in this layer. Information integration efforts have improved watch list screening databases, and more thorough screening procedures have been implemented for CAPPS selectees. Employee criminal background checks and access compliance inspections have also strengthened security measures within the Access layer.

The physical Screening layer carries over four pre 9/11 security measures, X-ray and metal detectors, canine patrols, and checked baggage screening, although the latter two measures have also been increased or improved. Screener supervisory oversight has been increased, and checkpoint measures have been implemented to reduce person throughput, while also increasing the throughput of screened objects (footwear, jackets, etc.). One item not listed but critical nonetheless is the training of the security screeners. Screener training has been increased to a minimum of forty hours of classroom training

---

[260] Peter St. John, *Air Piracy, Airport Security, and International Terrorism* (New York: Quorum Books, 1991), 210-213.

and 60 hours of on-the-job instruction.[262]   These marked increases coupled with standardized procedures and required recurrent training are significant improvements to the checkpoint screening system.

PRE 9/11	POST 9/11
ACCESS	
No Fly List	Integrated No Fly/Automatic Selectee List
CAPS (Select=Checked Luggage Search)	CAPPS (Select=Checked Lug & Persons Search)
	Behavior Detection Teams
	Travel Document Checks
Background Check - Employment History	Background Check - Criminal History
Access Control - Limited	Access Control - Compliance Inspections
PHYSICAL SCREENING	
	Only Ticketed Passengers
	Increased Prohibited Items List
Metal Detector	Metal Detector
X-Ray Carry Ons	X-Ray Carry Ons
	Outer Garments and Shoes X-rayed
	Explosive Trace Detection-Select Carry Ons
	Federal Security Manager
Canine Patrols	Canine Patrol - Increased
Checked Baggage Screening - Limited	Checked Baggage Screening - 100%
DIRECT ACTION	
	Hardened Cockpit Doors
FAMS - International	FAMS
	Armed Law Enforcement
	Federal Flight Deck Officers
	NORAD RADAR Improvements
	Temporary Flight Restrictions
	Fighter CAPS
	Crew Training - Self Defense
	Passenger Tolerance

Table 1.   Pre and Post 9/11 Security Measures

The third layer, Direct Action, illustrates a significant number of security measure initiatives to reduce system vulnerability.   These measures represent the last chance "glove save" effort because if employed, a hijack or terrorist event has or is taking place.

---

[261] United States General Accounting Office, *Aviation Security: Efforts to Measure Effectiveness and Address Challenges* (Washington D.C.: GAO, 2003), 12.

[262] United States, 107th Congress, <u>Aviation and Transportation Security Act of 2001, Pub. L. 107-71,</u> (Washington D.C.:2001).

If a terrorist hijacker was successful at bypassing the first and second security layers, it doubtful another 9/11 scenario could be reduced given the number of protective measure on board the aircraft, from crew to passenger.

Table 1 illustrates the number of security measure improvements put into place since 9/11. Whether in terms initiating new procedures, using new technology or increasing and improving previous security measures, the efforts have collectively more than doubled the number of security measures contained within the redundant security layers. In terms of layers of protection, there is also one additional layer that while not a primary focus of this thesis deserves mention, the Critical Infrastructure protection layer. This area is addressed by documents such as The National Infrastructure Protection Plan, which sets goals and objectives to secure the nations critical infrastructures, which the aviation transportation system is a part. In terms of aviation security, this "fourth" layer represents the last possible effort to dissuade a hijack, not necessarily by measures of security or interdiction, but more so by ensuring the aviation system is resilient, and can recover and restore service in an effort to mitigate the impact of an attack.

While many security measures have been implemented since 9/11, the transparency of the measure is an additional facet that warrants examination. The deployment of National Guardsmen to every airport to perform complete body searches of every traveler prior to entering an airport threshold would surely dissuade a would be terrorist from attempting to smuggle explosives on their persons. While these heavy-handed measures may dissuade and deter, they of course would not pass civil liberty scrutiny. Security measures that are transparent, meaning less visible to the traveler and do not impede the traveling public yet still add a measure of security, strike the optimum balance.

The Access layer only has two measures that are transparent, No-Fly lists and Behavior Detection Teams. For the Integrated No-Fly list however, transparency depends on list accuracy.

POST 9/11	Transparancy
ACESS	
Integrated No Fly/Automatic Selectee List	Yes
CAPPS (Select=Checked Lug & Persons Search)	No
Behavior Detection Teams	Yes
Travel Document Checks	No
PHYSICAL SCREENING	
Only Ticketed Passengers	No
Increased Prohibited Items List	No
Metal Detector	No
X-Ray Carry Ons	No
Outer Garments and Shoes X-rayed	No
Explosive Trace Detection-Select Carry Ons	No
Federal Security Manager	Yes
Canine Patrol - Increased	No
Checked Baggage Screening - 100%	Yes
DIRECT ACTION	
Hardened Cockpit Doors	Yes
FAMS	Yes
Armed Law Enforcement	Yes
Federal Flight Deck Officers	Yes
NORAD RADAR Improvements	Yes
Temporary Flight Restrictions	No
Fighter CAPS	Yes
Crew Training - Self Defense	Yes
Passenger Tolerance	N/A

Table 2.   Security Measure Transparency

Within the Physical Screening layer, the majority of measures are not transparent to the passenger as expected by the nature of the layer itself. This is the only layer that can interdict a concealed and prohibited carry-on object and as a result is the most intrusive. Finally, all of the measures in the Direct Action layer are transparent with the exception of Temporary Flight Restrictions. TFRs have tended to hamper general aviation by impeding or rerouting routes of flight. In total, 50% of the post 9/11 implemented measures discussed can be non-apparent to most aviation travelers. This is an important and successful aspect to highlight. When implementing new security measures, the more unobtrusive a measure is while still providing or adding security, the more acceptable the measure will be to the traveling public.

There is no doubt that, by comparing the current aviation security system to the pre-9/11 security measures, improvements have been made solely in the sheer number of measures in place within the different security layers. The Access layer's six security measures first mitigate ill-intentioned passengers and employees from gaining access to aircraft. The Physical Screening layer's system of nine screening measures interdicts the carry-on of dangerous items onboard commercial aircraft. The increase in the number of security measures alone, reduce the vulnerability of the system. Additional measures, some transparent to the traveler, reinforce multiple layers by adding security redundancy within each layer. As a result, an integrated system of layers cannot be breached by the defeat of a single security feature; each layer is a backup for the others, so that impermeability of individual layers is not required.[263]

1. Measures of Protection

Complete, impermeable layers are of course the desired effect of a layered security system. But by the very nature that the system is layered implies that layers or security measures within a layer can fail or have imperfections. The new measures imparted after 9/11 are no exception.

a. Access

The No-Fly lists are the most effective security measure to stop persons with questionable backgrounds or intent from boarding aircraft.[264] However as previously alluded to, difficulties have risen in applying the new expanded No-Fly list. Innocent passengers have been stopped from boarding aircraft because their names were similar to names on the No-Fly list, such as Senator Ted Kennedy.[265] A Former FBI agent stated that the No-Fly list had become a cover your rear end document as the list

---

[263] Transportation Research Board, *Deterrence, Protection and Preparation: The New Transportation Security Imperative, Special Report 270* (Washington D.C.: TRB, 2002), 16.

[264] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

[265] William J. Krouse and Bart Elias, *Terrorist Watchlist Checks and Air Passenger Prescreening*, (Washington D.C.: CRS, 2006), 4.

had expanded considerably.[266]   The airlines, still responsible for vetting passengers against the watchlists have no other amplifying information such as a birth date.[267]   A Terrorist Screening Center representative did state that the Watch List is continually being scrutinized.[268]   Constantly maintaining and overhauling a list containing thousands of names may continue to provide discrepancies. Those discrepancies may continue to cause false positives to occur, but it does point to the fact that person who's name matches those on the list are being stopped at the outer layer of security. TSA was also mandated to implement its next generation computer automated screening program that would allow TSA to take over the screening of passenger names against the No-Fly lists. Secure Flight which began development in 2004 after the failed CAPPS II program, is not expected to begin operational testing until the end of 2008, and is not anticipated to be fully operational until 2010.[269]

Once secure area access inspections were instituted, initial compliance reports were favorable, however, access control violations do still occur. In March 2007, an airline worker was arrested for using his airline identification to board an aircraft carrying a duffel bag containing thirteen handguns, an assault rifle and eight pounds of marijuana.[270]   However, two Federal Air Marshals were also onboard the aircraft.[271] TSA has instituted is surge operations, which deploy security inspectors and additional TSA to randomly increase security efforts at a select airport and to inspect current operations.[272]   One area focused on is employee screening and secure area access. The

---

[266] Steve Kroft, *Unlikely Terrorists on No Fly List,* CBS News Online, Available from http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml (accessed 23 Oct 2007).

[267]Ibid.

[268] Ibid.

[269] Kip Hawley, *Testimony Before the Subcommittee on Homeland Security, Committee on Appropriations,* United States House of Representatives, 13 Feb 2007.

[270] Jim Ellis, "TSA: Little Danger on Plane With Guns," ABC News, Available from http://abcnews.go.com/US/wireStory?id=2934874 (accessed 23 Oct 2007).

[271] Ibid.

[272] Transportation Security Administration, "TSA Ramps Up Employee Screening at Houston Airports," TSA Website, Available from http://www.tsa.gov/press/releases/2007/press_release_06082007.shtm (accessed 23 Oct 2007).

randomness of these actions imparts an unpredictable and unforeseen security measure on the employee, thus hopefully inducing security compliance.

b. *Physical Screening*

The federalizing of airport screeners was viewed as a significant and important measure to improve the quality of the screener workforce. Therefore it is interesting to note given the push for federalized screeners, that the Aviation and Transportation Security Act also allowed the opportunity for airports to maintain a private security screener workforce. Privatized security screening programs are currently being conducted at nine U.S. airports around the country, one of the largest being San Francisco Airport.[273] TSA however, is still required to oversee screening operations, and the companies can only employ persons who meet the same requirements as federal screeners and receive the same pay and benefits.[274] An additional stipulation is that the screening company must be owned and controlled by a citizen of the United States.

In the rush to meet the Federalized Screener deadlines set forth by the Aviation and Transportation Security Act, many of the screeners and airport workers were hired without background investigations, many with criminal records and over eighty with felony convictions.[275] In 2003, passengers filed more than 6,700 complaints against TSA employees for stealing cash, jewelry, and computers.[276] More than 1,200 of the original 55,000 screeners that made up the new federal screener force were terminated due to a criminal background.[277] These initial start up woes have been corrected however by use of the implemented background and criminal history checks.

---

[273] Transportation Security Administration, "Air Security TSA Strives to be Nimble: Ban on Complacency," TSA Website Available from http://www.tsa.gov/press/happenings/tsa_nimble.shtm (accessed 23 Oct 2007).

[274] United States, 107th Congress, Aviation and Transportation Security Act of 2001, Pub. L. 107-71, (Washington D.C.:2001).

[275] Mike Ahlers, "Report: felons hired in rush to fill screener jobs," CNN.Com, Available from http://www.cnn.com/2004/US/02/05/tsa.felons.screeners/index.html (accessed 23 Oct 2007).

[276] Marla Felcher, "Before and After the September 11 Attacks, *US Aviation Security*, Available from http://understandinggov.org/reports/ (accessed 13 Sep 2007), 9.

[277] Mike Ahlers, "Report: felons hired in rush to fill screener jobs," CNN.Com, Available from http://www.cnn.com/2004/US/02/05/tsa.felons.screeners/index.html (accessed 23 Oct 2007).

Screener problems persist in training as well as operational execution. Screener recurrent training, or refresher training, is one of the pillars of the new training regimen and is required for screeners three hours a week.[278] But due to manning shortages, some airports cannot afford to let screeners accomplish recurrent training without detracting from screener manning at checkpoints. As a result, some airport screeners are only receiving on average, three hours of recurrent training a month.[279]

Screener checkpoint weaknesses continue to be highlighted as well. A recent Government Accountability Office report cited that investigators were able to successfully smuggle improvised explosive devices and improvised incendiary devices past security checkpoints at nineteen different airports.[280] It is important to note, however, that most of the screeners executed their duties in accordance with TSA procedures and utilized screening technology correctly.[281] The test highlighted an exploitation of a weakness in policy and TSA procedure as opposed to a fault in screener performance.

c. *Direct Action*

The massive stand up of the Federal Air Marshal force following 9/11 encountered similar problems to the mass federal screener hire. TSA received more than 200,000 air marshal applications.[282] As a result, many agents were hired and flying while still awaiting completions of their required Top-Secret security investigation.[283] Like the screeners, the initial growth problems were remedied, but as a relatively new agency, management problems continue. The upper management echelon at the Federal

---

[278] Norman J. Rabkin, *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts* (Washington, D.C.: GAO, 2004), 11.

[279] Ibid.

[280] Gregory D. Kutz and John W. Kooney, *Aviation Security: Vulnerabilities Exposed Through Covert Testing of TSA's Passenger Screening Process* (Washington D.C.: GAO, 2007), 7.

[281] Ibid.

[282] United States 109th Congress, *Plane Clothes: Lack of Anonymity at The Federal Air Marshal Service Compromises Aviation and National Security* (Washington D.C.: GPO, 2006).

[283] United States General Accounting Office, *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed* (Washington D.C.: GAO, 2006), 7.

Air Marshal Service has limited aviation security experience sometimes resulting in less than always optimum management decisions regarding FAM operations.[284] For example, discreet Air Marshal movement procedures through airports and checkpoints have yet to be addressed, as current methods are cumbersome enough to compromise Air Marshal anonymity.[285]

As the new security measures and layers operate and continue to be improved, faults will be identified and most likely corrected. Implementation of all of the aforementioned new measures without imperfection is untenable. In the span of less than six years, the security aspect of the aviation transportation system has been completely overhauled. Layers and measures have been added to create additional proverbial concentric rings of protection around the target of interest, the commercial airliner. In the aftermath of the causal terrorist act, perhaps another warranted measure of progress is a comparison of the current measures to the 9/11 Commission recommendations.

B.   READDRESSING THE 9/11 DEFICIENCIES

The 9/11 Commission made three major recommendations to enhance or rectify the aviation security deficiencies in 2001, implement a strategic plan for the transportation sector, improve the use of No-Fly lists, improve the capability to detect explosives on persons and improve screener performance.[286]

The Transportation Sector-Specific Plan, which supports the National Infrastructure Protection Plan addresses the requirement for a strategic transportation plan. The transportation plan encompasses six transportation nodes, one of which is the aviation sector. The aviation annex plan identifies roles and missions of government agencies involved in securing the aviation system as recommended by the 9/11

---

[284] United States 109th Congress, *Plane Clothes: Lack of Anonymity at The Federal Air Marshal Service Compromises Aviation and National Security* (Washington D.C.: GPO, 2006).

[285] Ibid.

[286] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004).

Commission, as well as outlining the goals to achieve a secure, resilient airline system.[287] This recommendation has been met.

The 9/11 Commission also recommended that the improved use of No-Fly and Automatic selectee lists should not be delayed while waiting for a system that can replace CAPPS, and that TSA should perform the screening functions using the larger set of federal government watchlists.[288] This recommendation has been met in part, as integrated No-Fly and Automatic Selectee lists have been implemented for prepassenger screening. TSA's role in performing that function however has still not occurred, although TSA does manage the distribution of the watchlists to the airlines. TSA will take over the watchlist function once Secure Flight is complete. As previously mentioned, Secure Flight is still in the development phase but is nearing the testing stage.

The Third Commission recommendation for aviation security was to improve the ability to detect explosives on passengers, and that each person selected for additional screening should be screened for explosives.[289] This recommendation has not been fulfilled and the capability to detect explosives being carried on a person is has not been fully deployed. Testing of some technologies has been accomplished however. In 2006 TSA installed ninety-seven Explosive Trace Portals at thirty-seven airports which blow puffs of air on passengers as they pass through the portal.[290] The puffs of air dislodge explosive traces from travelers to facilitate detection. However, problems were identified with the technology, which effectively stopped further deployment.[291] Other technologies being developed are backscatter and millimeter wave body imaging technologies, which have not been fielded.

---

[287] United States Department of Homeland Security, *Transportation Sector-Specific Plan Aviation Model Annex* (Washington D.C.: DHS, 2007).

[288] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 393.

[289] Ibid.

[290] Cathleen A. Berrick, *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, But Key Challenges Remain* (Washington D.C.: GAO, 2007), 12.

[291] Ibid.

The second portion of the third Commission recommendation was for TSA to conduct a human factors study in an effort to improve screener performance.[292] This recommendation was achieved. TSA did accomplish a comprehensive Passenger Screener Performance Improvement Study, which focused on human factors, and the findings were used to implement improvements to increase screener performance.[293] In 2006, TSA implemented a performance management system, which now compensates screeners based upon technical proficiency, training and development, customer service skills, teamwork, professionalism, and leadership.[294] TSA also implemented a career progression program to provide advancement opportunities and pay advancement in an effort to provide incentive and to retain experienced individuals.[295]

With the exception of meeting the recommendation to detect explosives on individuals and taking over the No-Fly list screening, TSA has met the 9/11 recommendations mentioned above. Both of the aforementioned unfulfilled requirements are being addressed however with ongoing testing of pilot technologies. Improving or maintaining screener performance will most likely continue to be an ongoing performance issue. Due to monotony and routine, there is always the risk that after checking so many people and bags, screeners will tend to grow somewhat complacent.[296]

C. WHERE TO FOCUS EFFORTS

Given the aviation security measures put into effect, where should efforts be focused now? Look out, look forward and look around. Efforts must look out beyond the outermost layer. The outer layer discussed in this thesis was the Access layer pertaining to domestic aviation and passenger No-Fly lists. Looking further outward, however, No-Fly lists on international flights either inbound or outbound are vetted in a

---

[292] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 393.

[293] Asa Hutchinson, *Testimony before the Commerce, Science and Transportation Committee,* 16 Aug 2004.

[294] Kip Hawley, *Testimony before the United States Senate Committee on Commerce, Science and Transportation,* 4 Apr 2006.

[295] Ibid.

[296] Jin-Tai Choi, Aviation Terrorism, (New York: St. Martin's Press, 1994) 7.

similar fashion as domestic flights by Customs and Border Protection. This is where the next security layer begins, international cooperation. This layer is addressed in the International Outreach Plan, supporting plan to the National Strategy for Aviation Security. And while intelligence and information sharing efforts have been strengthened since 9/11, international cooperation and comparative security efforts need to be maintained if we are to attempt to interdict the threat before they can even reach the Access layer. Establishing and implementing the International Outreach Plan adds another defensive layer. This layer can superimpose all of our domestic layers upon international airports, if the same domestic standards can be applied abroad.

Security efforts must also continue to look forward. Efforts must be proactive. A security plan built solely on reactive security measures will only build a hodge-podge of non-integrated efforts. The 9/11 Commission noted this same conclusion, characterizing the security system in place on 9/11, "Most of the aviation security system's features had developed in response to specific incidents, rather than in anticipation."[297] To accomplish this however, security must stay ahead of the threat. Red Teaming can help achieve this goal as long as they are allowed to exploit aviation security weaknesses with innovative and unrestricted measures, and their efforts are looked at with support as opposed to adversarial. Terrorists analyze defenses.[298] Red Teams can do the same and highlight weaknesses to force the aviation security system to continually evolve. It is the difference between active improvement and reassessment versus stagnate procedures.

Besides looking out to stop the threat at the outermost layer, and looking forward to preempt the next aviation threat, aviation security efforts must continue to look around the entire security system of layers and measures as a whole. One area, layer, or measure cannot become the next focal point at the expense of the deterioration of the other

---

[297] National Commission on Terrorist Attacks Upon the United States, *The Aviation System and the 9/11 Attacks, Staff Statement No.3* (Washington D.C.: 2004), 8.

[298] National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington D.C.: 2004), 383.

measures and layers. A strong base level of security needs to be evenly applied so as not to create gaps by over-focusing on one area.[299] The whole aviation security system must remain a focal point of continuous improvement.

D. CONCLUSION

The Aviation Transportation System has continued to persevere against multiple hijack and terrorist incidents. With each incident, security improvements became the highest priority. Both security legislation and security measures addressed security deficiencies in an effort to improve aviation security, or at least address the security gaps from the previous aviation incident. The initial efforts laid the foundation for future security initiatives, employing the use of metal detectors, X-ray machines and armed sky marshals. Government official were charged to improve and increase security with varying degrees of success, but security vulnerabilities continued to exist, and continued to be exploited. Following each major incident, given the distance of time and the perception of a lessened threat, the priority of aviation security usually stagnated or dwindled, overshadowed by both economic cost and traveler convenience. Aviation security was systemically hindered by saddling the airlines with the responsibility and cost of security, coupled with the conflicting Federal Aviation Administration missions. It unfortunately took a monumental and tragic event to change these two barriers.

September 11 marked a turning point for aviation security. Never have so many security enhancements been implemented, from legal, to policy, to procedural, to technological. Almost every aspect of the aviation security system was overhauled. The Aviation and Transportation Security Act that was passed following 9/11 erected and reorganized organizations solely responsible for transportation security. The dual competing missions of the Federal Aviation Administration have finally been severed, alleviating the Federal Aviation Administration of the responsibility to secure and safeguard the system. While the Transportation Security Administration certainly weighs

---

[299] Bruce Schnier, "Interview with Kip Hawley," Bruce Schnier Website, Available at http://www.schneier.com/interview-hawley.html (accessed 10 Oct 2007).

each new security measure against passenger throughput and inconvenience, security is the priority, and it no longer competes on equal ground against commercial aviation interests.

A national aviation security strategy has also been developed to guide current and future security initiatives. A national strategy mitigates the pre-9/11 reactive security measure approach in an effort to preempt future security threats or vulnerabilities. The strategy also emphasizes a combined effort approach by enlisting the aid of not only federal, but also state and local governments that may be involved in, or respond to another aviation related hijack or terrorist incident.

Following 9/11, security layers were redefined and reinforced and a multitude of security measures have been added to provide redundant and tertiary measures of security. With the exception of a few major airports, the federal security screener initiative has alleviated the commercial, cost driven security screening companies from commercial aviation. Security screening policies and measures are now in the hands of the federal government in an effort to bring standardization and regulation to the screening workforce. Advanced technologies are being developed to refine passenger no-fly list matching, TSA officers are being trained in behavior observation techniques and screening procedures are being continually adjusted and fine tuned based on operational feedback, recent threats or undercover agent exposed vulnerabilities. Onboard the aircraft, security measures have not only included structural enhancements to cockpit doors or armed undercover federal marshals, but it has also permeated to the passengers and crew. Aircrew training that once emphasized crew compliance in response to an onboard hijack event has been replaced with overt action in an attempt to regain control of the aircraft. And if the passenger response to shoe bomber Richard Reid in 2001 is an indicator of post 9/11 passenger reactions, then passenger compliance has also been replace with overt action. The closer the potential aviation terrorist gets to his goal of gaining control of an aircraft and passengers, the more drastic the response measures will be.

Department of Defense fighters are now armed and trained to shoot down civilian airliners should the situation and need arise. An unthinkable security measure prior to

9/11, it is a last chance measure to protect U.S. critical infrastructure and avert a 9/11 reenactment. NORAD fighters have resumed alert postures at an increased number of bases around the country, but the inbound Russian bomber scenario has been replaced with the rogue airliner. The nation has also been moved to address critical infrastructure protection, should armed intervention from either U.S. fighters, or onboard armed officers fail.

Aviation security has been enhanced since 9/11, and the vulnerability of the system reduced by the application of so many additional barriers. Many of the security measures are not transparent to the every day traveler. The most notable overt layer is the physical screening layer, which has actually been in place since the 1970's. The transparency of this layer diminishes considerably in the face of newly implemented procedures for passengers passing through this layer. This layer also seems to gain the most attention when security procedures go awry.

While there may have been some setbacks in implementation, the new and refined security measures remain in place. No system is perfect, and security breaches in the future will most likely continue to occur. The government investigative teams that smuggled improvised explosive devices past security screeners earlier this year reinforced this fact. The media highlighted the failure, and will continue to highlight future failures. The aspect that has failed to be captured, however, is that each successive breach of security by teams from the Government Accountability Office or from TSA's red teams, can only strengthen the security system as a whole. Each successive breach will allow TSA the opportunity to improve a found weakness in policy, procedure, personnel or technology. These cannot be viewed as setbacks, but instead as waypoints for future security measures to meet and surpass. Media reports of security breaches also create an additional benefit, the attention garnered keeps aviation security at the forefront of public concern. This is perhaps the most difficult feat to accomplish.

Aviation security in the past has been cyclic in nature. After each aviation incident, security weaknesses are identified, and improvements are promised or developed with some degree of implementation. Over time, however, as security violations lessen, and the perception of the threat diminishes, security wanes or fails.

Building additional security layers and measures is fairly easy, especially in the wake of a monumental terrorist attack. What will be necessary now, and arguably more difficult to attain, is the perseverance to maintain the newly established security efforts as we move further away from September 11, 2001.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Ahlers, Mike. "Report: felons hired in rush to fill screener jobs." CNN.Com, Available from http://www.cnn.com/2004/US/02/05/tsa.felons.screeners/index.html (accessed Oct 2007).

Aircraft Owners and Pilots Association. "Senate to consider enhanced TFR enforcement over weapons storage facilities." AOPA Online. Available from http://www.aopa.org/whatsnew/newsitems/2002/02-3-138x.html (accessed Dec 2006).

Aircraft Owners and Pilots Association. "Serious security — Air Force says it will shoot Super Bowl TFR violators." AOPA Online. Available from http://www.aopa.org/whatsnew/newsitems/2006/060203superbowl.html (accessed Dec 2006).

Anderson, John Ward and Karen De Young. "Plot to Bomb U.S.-Bound Jets Is Foiled." *Washington Post*, 11 Aug 2006. Available from http://www.washingtonpost.com/wp-dyn/content/article/2006/08/10/AR2006081000152.html (accessed May 2007).

Berrick, Cathleen A. *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, But Key Challenges Remain.* Washington D.C.: Government Accountability Office, 2007.

Bryan, Richard H. *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation.* Congress No. 106, Session No. 2. 6 Apr 2000.

Bush, George W. *The Department of Homeland Security: Administration Homeland Security Actions Since September 11.* The White House. Available from http://www.whitehouse.gov/deptofhomeland/sect8.html (accessed Oct 2007).

Bush, George W. *The National Strategy for Aviation Security.* Washington D.C., 2007. Available from http://www.whitehouse.gov/homeland/nstrategy_asecurity.pdf (accessed Aug 2007).

Bush, George W. *The National Strategy for the Physical Protection of Critical Infrastructures and Key Assets.* Washington D.C., 2003.

CBS News. "Bulletproof Cockpit Doors a Reality." CBS News Online. Available from http://www.cbsnews.com/stories/2003/04/04/attack/main547827.shtml (accessed Oct 2007).

Choi, Jin-Tai. *Aviation Terrorism*. New York: St. Martin's Press, 1994.

CNN. "TWA Flight 800 The Crash and Investigation." CNN Online. Available from http://www.cnn.com/US/9707/twa.800/ (accessed Sep 2007).

CNN. "U.S. deaths in Iraq, war on terror surpass 9/11 toll." CNN Online. Available from http://edition.cnn.com/2006/WORLD/meast/09/03/death.toll/ (accessed Sep 2007).

Commission on Aviation Security and Terrorism. *Findings and Recommendations.* Washington D.C., 1990. Available from http://www.globalsecurity.org/security/library/congress/1990_cr/s900511-terror.htm (accessed Sep 2007).

Dillingham, Gerald. *Testimony before the Subcommittee on Aviation of the Committee on Commerce, Science and Transportation*. Congress No. 106, Session No. 2. 6 Apr 2000.

Dugan, Laura, Gary Lafree, Alex R. Piquero. 2005. "Testing A Rational Choice Model of Airline Hijackings." *Criminology,* Vol. 43, No. 4.

Elias, Bart, and William J. Krouse. *Terrorist Watchlist Checks and Air Passenger Screening.* Washington D.C.: Congressional Research Service, 2006.

Elias, Bart, William Krouse and Ed Rappaport. *Homeland Security: Air Passenger Prescreening and Counterterrorism.* Washington D.C.: Congressional Research Service, 2005.

Elias, Bartholomew. *Air Cargo Security.* Washington D.C.: Congressional Research Service, 2003.

Ellis, Jim. "TSA: Little Danger on Plane With Guns." ABC News. Available from http://abcnews.go.com/US/wireStory?id=2934874 (accessed Oct 2007).

Evans, Alona E. "Aircraft Hijacking: What Is Being Done." *The American Journal of International Law* Vol. 67, No.4 (1973): 644.

Farah, Douglas. *Blood From Stones.* New York: Broadway Books, 2004.

Federal Aviation Administration. *U.S. Certified Air Carriers 2006*. Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/addresses/ (accessed Sep 2007).

Federal Aviation Administration, *Primary and Non-Primary Commercial Service Airports.* Available from http://www.faa.gov/airports_airtraffic/airports/planning_capacity/passenger_allcargo_stats/passenger/index.cfm?year=2005 (accessed Sep 2007).

Federal Aviation Reauthorization Act of 1996, 49 USC 40101. 9 Oct 1996.

Felcher, Marla. "U.S. Aviation Security: Before and After the September 11 Attacks." Understanding Government. Available from http://understanding gov.org/reports/ (accessed Sep 2007).

Frank, Thomas. "Airport Security arsenal adds behavior detection." USA Today, 25 Sep 2007. Available from http://www.usatoday.com/travel/flights/2007-09-25-behavior-detection_N.htm?csp=34 (accessed Oct 2007).

Frittelli, John. *Transportation Security: Issues for the 109th Congress.* Washington, D.C.: Congressional Research Service, 2005).

Gathrite, Alan. "No-fly list ensnares innocent travelers." *San Francisco Chronicle,* 8 Jun 2003. Available from http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2003/06/08/MN253740.DTL (accessed Sep 2007).

Hartwick, Thomas S. *Testimony before the Subcommittee on Aviation, Committee on Transportation and Infrastructure*. Congress No. 106, Session No. 2. 16 Mar 2000.

Hawley, Kip. *Testimony Before the Subcommittee on Homeland Security, Committee on Appropriation.* United States House of Representatives. 13 Feb 2007.

Kip Hawley. *Testimony before the United States Senate Committee on Commerce, Science and Transportation*. 4 Apr 2006.

Hebert, Adam J. "Noble Eagle Without End." *Air Force Magazine* 88, no.2 (2005). Available from http://www.afa.org/magazine/feb2005/0205eagle.asp (accessed Oct 2007).

Holden, Robert T. "The Contagiousness of Aircraft Hijacking." *The American Journal of Sociology* (1986): 878-879.

Hutchinson, Asa. *Testimony before the Commerce, Science and Transportation Committee.* 16 Aug 2004.

Jean, Grace. "Focus on Checked Bag Screening has Detracted from Aviation Security." *National Defense* 91, 640 (2007).

Kaplan, Eben. 2006. "Targets for Terrorists: Post-9/11 Aviation Security." Council on Foreign Relations. Available from http://www.cfr.org/publication/11397/targets_for_terrorists.html (accessed May 2007).

Kroft, Steve. *Unlikely Terrorists on No Fly List.* CBS News Online. Available from http://www.cbsnews.com/stories/2006/10/05/60minutes/main2066624.shtml (accessed Oct 2007).

Krouse, William J., and Bart Elias. *Terrorist Watchlist Checks and Air Passenger Prescreening.* Washington D.C.: Congressional Research Service, 2006.

Kutz, Gregory D., and John W. Kooney. *Aviation Security: Vulnerabilites Exposed Through Covert Testing of TSA's Passenger Screening Process.* Washington D.C.: Government Accountability Office, 2007.

Landes, William M. "An Economic Study of U.S. Aircraft Hijacking, 1961-1976." *Journal of Law and Economics* Vol. 21, No. 1 (1978): 1.

Longley, Robert. "Air Passengers Must Remove Coats For Security Screening." About.Com: US Gov Info / Resources. Available from http://usgovinfo.about.com/od/defenseandsecurity/a/coatsoff.htm (accessed Oct 2007).

McClure, George. "Has Airport Security Improved Since 9/11?" IEE-USA Today's Engineer Online. Available from http://www.todaysengineer.org/2005/Jun/security.asp (accessed Oct 2007).

Military.com. "CG Assumes National Capitol Region Intercept Mission." Available from http://www.military.com/features/0,15240,114999,00.html (accessed Oct 2007).

MSNBC. "U.S. air passengers face increased air security." MSNBC Online. Available from http://www.msnbc.msn.com/id/14282396/ (accessed Sep 2007).

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* Washington D.C., 2004.

National Commission on Terrorist Attacks Upon the United States. *The Aviation System and the 9/11 Attacks, Staff Statement No.3.* Washington D.C., 2004.

National Commission on Terrorist Attacks Upon the United States. *The Aviation System and the 9/11 Attacks, Staff Statement No.17.* Washington D.C., 2004.

North American Aerospace Defense Command. *About NORAD.* Available from
http://www.norad.mil/about/CONR.html (accessed Oct 2007).

O'Brien, Kevin A. "France," in *Europe Confronts Terrorism*. Edited by Karen Von
Hippel. New York: Palgrave Macmillan, 2005.

Peterman, David Randall. *Transportation Security: Issues for the 109th Congress.*
Washington D.C.: Congressional Research Service, 2006.

Poole, Robert W., Jr. "Airport Security: Time for a New Model." Reason Foundation.
Available from http://www.reason.org/airportssecurity (accessed May 2007).

Rabkin, Norman J. *Aviation Security: Improvement Still Needed in Federal Aviation
Security Efforts.* Washington, D.C.: General Accounting Office, 2004.

Rapoport, David. "The Four Waves of Modern Terrorism." In *Attacking Terrorism:
Elements of A Grand Strategy*, edited by Audrey Kurth Kronin and James Ludes,
Washington DC: Georgetown University Press, 2004.

Rosenzweig, Paul and Ha Nguyen. "CAPPS II Should Be Tested and Deployed." The
Heritage Foundation. Available from
http://www.heritage.org/Research/HomelandSecurity/BG1683.cfm (accessed Sep
2007).

Rumerman, Judy. "Aviation Security." U.S. Centennial Commission of Flight. Available
from
http://www.centennialofflight.gov/essay/Government_Role/security/POL18.htm
(accessed Aug 2007).

Schneier, Bruce. Beyond Fear: Thinking Sensibly About Security in an Uncertain World.
New York: Copernicus Books, 2003.

Schnier, Bruce. "Interview with Kip Hawley." Bruce Schnier Website. Available at
http://www.schneier.com/interview-hawley.html (accessed Oct 2007).

Shubber, Sami. "Aircraft Hijacking under the Hague Convention 1970: A New Regime?"
The International and Comparative Law Quarterly Vol. 22, No. 4. (1973): 708.

Stefani, Alexis M. *Testimony before the Subcommittee on Aviation of the Committee on
Commerce, Science and Transportation*. Congress No. 106, Session No. 2. 6 Apr
2000.

St. John, Peter. Air Piracy, Airport Security, and International Terrorism. New York:
Quorum Books, 1991.

Strohm, Chris. 2005. "TSA Chief Says aviation attacks still pose greatest risk." Government Executive.com. Available from http://www.govexec.com/dailyfed/0205/021505c1.htm (accessed May 2007).

Subcommittee on Aviation of the Committee on Transportation and Infrastructure. *Hearing on Deployment and Use of Security Technology.* Congress No. 107, Session No 1, 11 Oct 2001. Available from http://www.globalsecurity.org/security/library/congress/2001_h/011011-memo.htm (accessed Sep 2007).

Szyliowicz, Joseph S. "Aviation Security: Promise or Reality?" In *Homeland Security and Terrorism,* edited by Russell Howard, James Forest and Joanne Moore, 118. New York: McGraw-Hill, 2006.

The International Air Cargo Association. *The TIACA Manifesto.* Available from http://www.tiaca.org/content/chapter1.asp (accessed Sep 2007).

Transportation Research Board. *Deterrence, Protection and Preparation: The New Transportation Security Imperative, Special Report 270*. Washington D.C.: TRB, 2002).

Transportation Security Administration. "3-1-1 for Carry-Ons." TSA Website, http://www.tsa.gov/311/index.shtm (accessed Oct 2007).

Transportation Security Administration. "Air Security TSA Strives to be Nimble: Ban on Complacency." TSA Website. Available from http://www.tsa.gov/press/happenings/tsa_nimble.shtm (accessed Oct 2007).

Transportation Security Administration. "Permitted and Prohibited Items." TSA Website. http://www.tsa.gov/travelers/airtravel/prohibited/permitted-prohibited-items.shtm#3 (accessed Oct 2007).

Transportation Security Administration. "TSA Continues to Extend Security Beyond the Checkpoint, Assuming Document Checking Responsibility at Airports from Coast to Coast." TSA Website. Available at http://www.tsa.gov/press/happenings/document_checking.shtm (accessed Oct 2007).

Transportation Security Administration. "TSA Provides Another Layer of Security to Airport Employee Hiring." TSA Website. Available from http://www.tsa.gov/press/happenings/sida.shtm (accessed Oct 2007).

Transportation Security Administration. "TSA Ramps Up Employee Screening at Houston Airports." TSA Website. Available from http://www.tsa.gov/press/releases/2007/press_release_06082007.shtm (accessed Oct 2007).

United States 107th Congress. Aviation and Transportation Security Act of 2001, Pub. L. 107-71. Washington D.C.: 2001. Available from http://www.tsa.gov/assets/pdf/Aviation_and_Transportation_Security_Act_ATSA_Public_Law_107_1771.pdf (accessed Sep 2007).

United States 109th Congress. *Plane Clothes: Lack of Anonymity at The Federal Air Marshal Service Compromises Aviation and National Security*. Washington D.C.: GPO, 2006.

United States Bureau of Transportation Statistics. *Domestic Airline Travel in October.* Available from http://www.bts.gov/press_releases/2006/bts002_06/html/bts002_06.html#table_01 (accessed Sep 2007).

United States Bureau of Transportation Statistics. *Domestic Flights: Air Revenue Ton Miles.* Available from http://www.bts.gov/press_releases/2006/bts002_06/html/bts002_06.html#table_01 (accessed Sep 2007).

United States Bureau of Transportation Statistics. *Employment Statistics.* Available from http://www.bts.gov/programs/airline_information/number_of_employees/ (accessed Sep 2007).

United States Bureau of Transportation Statistics. *Motor Vehicle Fatalities, Vehicle-Miles, and Associated Rates by Highway Functional System.* Available from http://www.bts.gov/publications/national_transportation_statistics/html/table_02_18.html (accessed May 2007).

United States Bureau of Transportation Statistics. *Prohibited Items Intercepted At Airport Screening Checkpoints.* Available from http://www.bts.gov/publications/national_transportation_statistics/2006/html/table_02_16b.html (accessed May 2007).

United States Bureau of Transportation Statistics. *Top 50 Airports by Passengers Enplaned On Large U.S. Carriers: 1995, 2004 and 2005*. Available from http://www.bts.gov/publications/state_transportation_statistics/state_transportation_statistics_2006/html/table_04_06.html (accessed Sep 2007).

United States Bureau of Transportation Statistics. *U.S. Air Carrier Aircraft Departures, Enplaned Revenue Passengers, and Enplaned Revenue Tons.* Available from http://www.bts.gov/publications/national_transportation_statistics/html/table_01_34.html (accessed May 2007).

United States Department of Homeland Security. *Air Domain Surveillance and Intelligence Integration Plan.* Washington, D.C.: 2007. Available from http://www.dhs.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf (accessed Aug 2007).

United States Department of Homeland Security. *Aviation Operational Threat Response Plan.* Washington, D.C.: 2007. Available from http://www.dhs.gov/xlibrary/assets/hspd16_opthreatrespplan.pdf (accessed Aug 2007).

United States Department of Homeland Security. *Aviation Transportation System Security Plan.* Washington, D.C.: 2007. Available from http://www.dhs.gov/xlibrary/assets/hspd16_transsystemsecurityplan.pdf (accessed Aug 2007).

United States Department of Homeland Security. *Transportation Sector-Specific Plan Aviation Model Annex.* Washington D.C.: DHS, 2007.

United States Department of Justice. *Fact Sheet: The Terrorist Screening Center.* Washington, D.C.: 2003. Available from http://www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm (accessed Sep 2007).

United States Department of State. *Significant Terrorist Incidents, 1961-2003: A Brief Chronology.* Available from http://www.state.gov/r/pa/ho/pubs/fs/5902.htm (accessed Aug 2007).

United States Department of Transportation. "Airports to Remain Closed, Mineta Says." Available from http://usinfo.state.gov/is/Archive_Index/Airports_to_Remain_Closed_Mineta_Says.html (accessed Sep 2007).

United States Department of Transportation. *A Chronology of Dates Significant in the Background, History and Development of the Department of Transportation.* Available from http://dotlibrary.dot.gov/Historian/chronology.htm (accessed Sep 2007).

United States General Accountability Office. *Aviation Security: Risk, Experience, and Customer Concerns Drive Changes to Airline Passenger Screening Procedures, but Evaluation and Documentation of Proposed Changes Could Be Improved.* Washington, D.C.: GAO, 2007.

United States General Accounting Office. *Aviation Security: Development of New Security Technology Has Not Met Expectations.* Washington, D.C.: GAO, 1989.

United States General Accounting Office. *Aviation Security: Efforts to Measure Effectiveness and Address Challenges.* Washington D.C.: GAO, 2003.

United States General Accounting Office. *Aviation Security: Federal Air Marshal Service Is Addressing Challenges of Its Expanded Mission and Workforce, but Additional Actions Needed.* Washington D.C.: GAO, 2006.

United States General Accounting Office. *Aviation Security: Further Steps Needed to Strengthen the Security of Commercial Airport Perimeters and Access Controls.* Washington D.C.: GAO, 2004.

United States General Accounting Office. *Aviation Security: Improvement Still Needed in Federal Aviation Security Efforts.* Washington D.C.: GAO, 2004.

United States General Accounting Office. *Aviation Security: Urgent Issues Need to be Addressed.* Washington, D.C.: GAO, 1996.

United States General Accounting Office. *Proactive Management of FAA's Security Program Needed.* Washington, D.C.: GAO, 1989.

United States Government Accountability Office. *Aviation Security: DHS Has Made Progress in Securing the Commercial Aviation System, but Key Challenges Remain.* Washington D.C.: GAO, 2007.

United States Government Accountability Office. *Aviation Security: Efforts to Measure Effectiveness and Address Challenges.* Washington D.C.:GAO, 2003.

United States Government Accountability Office. *General Aviation Security: Increased Federal Oversight Is Needed, but Continued Partnership with the Private Sector is Critical to Long-Term Success.* Washington, D.C.: GAO, 2004.

Woerth, Duane. *Testimony before the Subcommittee on Economic Security, Infrastructure Protection and Cybersecurity of the Committee on Homeland Security.* Congress No. 109, Session No. 1, 16 May 2005.

White House Commission on Aviation Safety and Security. *Final Report to President Clinton.* Washington D.C., 1997.

Zielbauer, Paul and John Sullivan. "After the Attacks: Airport Security; F.A.A. Announces Stricter Rules; Knives No Longer Allowed." *The New York Times,* 13 Sep 2001. Available from http://query.nytimes.com/gst/fullpage.html?res=9C07E6DC1038F930A2575AC0A9679C8B63 (accessed Sep 2007).

INITIAL DISTRIBUTION LIST

1.	Defense Technical Information Center
	Ft. Belvoir, Virginia

2.	Dudley Knox Library
	Naval Postgraduate School
	Monterey, California