NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

IMPROVING THE SECURITY OF THE U.S. AERONAUTICAL DOMAIN: ADOPTING AN INTELLIGENCE-LED, RISK-BASED STRATEGY AND PARTNERSHIP

by

David S. Williams

December 2010

Thesis Co-Advisors
Nadav Morag
Paul J. Smith

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE	*Form Approved OMB No. 0704-0188*

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** December 2010	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Improving the Security of the U.S. Aeronautical Domain: Adopting an Intelligence-Led, Risk-Based Strategy and Partnership	**5. FUNDING NUMBERS**
6. AUTHOR(S) David Williams	
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. IRB Protocol number: N/A.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	**12b. DISTRIBUTION CODE** A

13. ABSTRACT

Nine years after the 9/11 attacks—and despite the passage of federal legislation, the creation of a U.S. Department of Homeland Security and the appropriation of billions of dollars for this nation's security—the National Aeronautical Domain (NAD) is still vulnerable to exploitation and attack. Indeed, as has been evidenced time and again since September 11, 2001, ideologically-driven actors remain committed to exploiting the residual weaknesses of the U.S. aviation security apparatus.

This thesis examines three critical areas within the U.S. aviation security system and concludes that, in order to effectively and efficiently reduce the nation's exposure to aviation-based acts of terrorism, both federal and local levels of collaboration in the following areas is urgently required: 1) improved sharing of threat intelligence information; 2) identification and uniform utilization of a specific risk-assessment methodology; and; adaptation of an intelligence-led policing management model within the aviation security field. In order to achieve the strategic goal of protecting the United States through its aeronautical domain, each of the subject areas referenced is discussed as an interdisciplinary process. Finally, the aviation-related security procedures of three allied nations are examined to determine if other democratically governed countries have achieved success in the same areas.

14. SUBJECT TERMS airport security, aviation security, megacommunities, intelligence, intelligence sharing, risk assessment methodology, RAM, partnership, National Aeronautical Domain, NAD	**15. NUMBER OF PAGES** 149
	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

IMPROVING THE SECURITY OF THE U.S. AERONAUTICAL DOMAIN: ADOPTING AN INTELLIGENCE-LED, RISK-BASED STRATEGY AND PARTNERSHIP

David S. Williams
Assistant Director of Public Safety and Technology, Houston Airport System, Texas
B.S., University of Houston-Downtown, 1994

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 2010

Author: David S. Williams

Approved by: Nadav Morag
Thesis Co-Advisor

Paul J. Smith
Thesis Co-Advisor

Harold A. Trinkunas, PhD
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Nine years after the 9/11 attacks—and despite the passage of federal legislation, the creation of a U.S. Department of Homeland Security and the appropriation of billions of dollars for this nation's security—the National Aeronautical Domain (NAD) is still vulnerable to exploitation and attack. Indeed, as has been evidenced time and again since September 11, 2001, ideologically-driven actors remain committed to exploiting the residual weaknesses of the U.S. aviation security apparatus.

This thesis examines three critical areas within the U.S. aviation security system and concludes that, in order to effectively and efficiently reduce the nation's exposure to aviation-based acts of terrorism, both federal and local levels of collaboration in the following areas is urgently required: 1) improved sharing of threat intelligence information; 2) identification and uniform utilization of a specific risk-assessment methodology; and; adaptation of an intelligence-led policing management model within the aviation security field. In order to achieve the strategic goal of protecting the United States through its aeronautical domain, each of the subject areas referenced is discussed as an interdisciplinary process. Finally, the aviation-related security procedures of three allied nations are examined to determine if other democratically governed countries have achieved success in the same areas.

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

LIST OF ACRONYMS AND ABBREVIATIONS

AOA	Aircraft Operations Area
ASC	Airport Security Coordinator
ASP	Airport Security Program
ATVRA	Asset, Threat, Vulnerability and Risk Assessment
BAA	British Airports Authority
BCAA	British Civil Aviation Authority
CARVER	Criticality, Accessibility, Recoverability, Vulnerability, Effect, and Recognizability
CASA	Australian Civil Aviation Security Authority
CBP	Customs and Border Protection
CCTV	Closed Captioned Television
CFR	Code of Federal Regulations
CHRC	Criminal History Records Check
CI/KR	Critical Infrastructure and Key Resource
CIA	Central Intelligence Agency
CompStat	Computer Statistics
CONTEST	Counter-Terrorism Strategy (United Kingdom)
COP	Community Oriented Policing
CPTED	Crime Prevention Through Environmental Design
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DOI	Department of Infrastructure (Australia)
DOJ	Department of Justice
E-R2-C Grid	Eliminate-Reduce-Raise-Create Grid
ETH	Eilat International Airports
FAA	Federal Aviation Administration
FAM	Federal Air Marshal Service
FBI	Federal Bureau of Investigation
GAO	U.S. General Accounting Office
GWOT	Global War on Terror

HSDN	Homeland Secure Data Network
HSPD	Homeland Security Presidential Directive
HUMINT	Human Intelligence
IAA	Israel Airports Authority
IC	Intelligence Community
ICE	Immigration and Customs Enforcement
ILP	Intelligence Led Policing
IMINT	Imagery Intelligence
IRTPA	Intelligence Reform and Terrorism Prevention Act of 2004
ISA	Israel Security Agency
MASINT	Measurement and Signatures Intelligence
MATRA	Multi-Agency Threat and Risk Assessment (United Kingdom and Australia)
MSHARPP	Mission, Symbolism, History, Accessibility, Recognizability, Population, and Proximity
MSRAM	Maritime Security Risk Assessment
NAD	National Aeronautical Domain
NIPP	National Infrastructure Protection Plan
NSAS	National Strategy for Aviation Security
NSPD	National Security Presidential Directive
OSINT	Open Source Intelligence
OSO	TSA Office of Security Operations
PDD	Presidential Decision Directive
RAM	Risk Assessment Methodology
RMAT	Risk Management Assessment Tool
SIDA	Security Identification Display Area
SIGINT	Signals Intelligence
SO18	Aviation Security Operational Command Unit (United Kingdom)
STU	Secure Terminal Unit
TLV	Ben Gurion International Airport
TSA	Transportation Security Administration
TSCI/KRP	Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan

UK	United Kingdom of Great Britain and Northern Ireland
US	United States
USC	United States Code of Federal Regulations
USCAP	United States Commercial Aviation Partnership
USIC	United States Intelligence Community

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

But for the grace of God and the support of many people, the amazing journey I have taken at the Naval Postgraduate School (NPS) would not have been possible. Consequently, while this list is by no means exhaustive, I have to take a moment to thank those to whom I am most grateful.

First and foremost, I have to thank my childhood sweetheart, mother of my children and wife of over 25-years, Missy, for your love, encouragement, and support throughout this endeavor. As always, you have been a kind, patient, and understanding partner and friend—one without whom my success in this program would have been impossible. I am forever indebted to you not only for your support of me while at NPS but also for maintaining a fantastic lifestyle for our family throughout the duration of this program of study. I love you with all of my heart.

To our children, Amanda and Clayton, you have always been—and will remain—God’s inestimable gift to both your mother and me. As I have worked my way through the rigors of the NPS program, I want you both to know not only how proud I am of who you have become as smart, responsible, and patriotic adults, but how indebted I am to you for your long hours of discussion and debate with me on the topics of law, politics, religion, sociology, and terrorism—it was great fun for me. Along with my new son-in-law, Jonathan, a much welcomed addition to our family, I have truly learned a great deal from each of you and simply continue to marvel at your character, spirit and intellect on an individual basis. You are three amazing people, and in your honor, I say: “Hook’em, Texas Longhorns!” and “Gig’em, Texas Aggies!” Thanks for all of your help, I love all three of you.

To my mom and dad, Jeannie and Carl, thanks for your support and understanding for all of the missed family get-togethers over the past year and a half. I have sincerely missed our time together with everyone congregated out on your back porch—eating, drinking, and laughing—but I am ready to make-up for lost time. Someone please light the big pit! I love you both.

To my former bosses at the Houston Airport System, Frank Haley and Rick Vacar, thanks for your invaluable support over the course of the NPS program—your initial endorsement and sustained support were vital. Additionally, I want to acknowledge my co-workers in the Public Safety Division—Phyllis, Ron, Mark, Cheryl, Mark, Larry, Jennifer, Felipe, Robert, Brandon, and Betti—whose words of encouragement and management of our operation in my absence made this educational pursuit at NPS logistically possible. I am sincerely grateful to all of you for your help.

To the entire faculty and staff at NPS, thank you for the educational experience of a lifetime. I have always wanted to pursue a graduate education, but never in my wildest dreams did I believe I would be able to participate in such an esteemed program. Because of you, I remain "Wowed!" at the world-class caliber of professors and professional staff associated with the NPS Center for Homeland Defense and Security. I am extremely grateful for both the opportunity and the education you have made available to me. Also, to my NPS thesis advisors—Nadav Morag and Paul Smith—thanks for your patience, insight and counsel both in and out of the classroom. You both possess the type of knowledge, skills, and experiences that naturally command respect, and it was a real honor for me to work with both of you over the course of this master's program.

Finally, to the NPS cohort of 0903/0904, I wish to thank each of you from the bottom of my heart for your great friendship, keen intellect and undying sense of humor. Because of all of you together, I have learned more and laughed harder in the past year and a half than I have my entire life. You are all real experts in your respective fields of service and are true patriots for our nation. Indeed, it has been my high honor and distinct privilege to have lived, associated, and learned with each of you throughout the course of the NPS program. May God bless and keep each of you safe in your future pursuits.

I. INTRODUCTION

In the aftermath of the September 11, 2001, attacks—in addition to a catastrophic loss of human life—the U.S. civil aeronautical industry suffered an unprecedented disruption of air service to the National Aeronautical Domain (NAD), and the nation's economy was projected to lose an estimated half a trillion dollars by the end of 2003 as a proximate result of these tragedies (Looney, 2002, p. 1). As evidenced by these terrorist actions, then, ensuring the adequate defense of the NAD is vital to the physical, psychological and economic security interests of the United States. However, some nine years after the 9/11 attacks—and despite the passage of federal legislation, the creation of a U.S. Department of Homeland Security and the appropriation of billions of dollars for this nation's security—the NAD is still vulnerable to exploitation and attack.

A. PROBLEM STATEMENT—BACKGROUND

As far back as 1990, *The 1989 President's Commission on Aviation Security and Terrorism* (Commission) noted the federal government's fundamental failure to gather and disseminate threat assessment information[1] to local aviation security partners (White House, 1990). In fact, some seven years later, *The 1996 President's Commission on Aviation Safety and Security* again acknowledged that threat assessment information is often passed by the Central Intelligence Agency or Federal Bureau of Investigation to the Federal Aviation Administration (now the Department of Homeland Security (DHS), Transportation Security Administration), but it is then "sanitized" to avoid revealing source information (White House, 1997). As a result of this practice, and with no formal

[1] This thesis will recognize a distinction between the terms "intelligence information" and "threat assessment information," the latter of which is typically a derivative of raw intelligence information. For example, the details of specific intelligence information may or may not be disseminated due to either classification issues or the fact that operational security for an active case investigation may necessitate restricting the widespread dissemination of the same, such as to protect the confidentiality of either the identity of a human source or the specific method by which information was collected. Threat assessment information, however, evolves from specific intelligence information, inclusive of that developed from the confidential sources cited above, and is oftentimes more generally focused on the potential threat streams and modalities from which a hazard may emanate in any given mission space.

access to any other agency within the U.S. Intelligence Community (USIC),[2] local aviation security managers are oftentimes just told what countermeasures to implement by the TSA but not why they are expending the time, money and scarce resources. Consequently, without specific information and collaboration, local aviation security groups are effectively denied a meaningful opportunity to help formulate more effective countermeasures to threats directed toward the NAD. This culture has not significantly changed within the USIC over the past two decades, despite the events of 9/11. In addition, more recently, this supposition is further supported by the Office of the Director of National Intelligence's (ODNI) 2008 report entitled, *United States Intelligence Community Information Sharing Strategy* (pp. 3, 5).

Accordingly, while the collection, analysis and integration of threat information may be occurring at the DHS-Transportation Security Administration (TSA) headquarters' level, empirical evidence indicates that the dissemination of the same is still neither consistent nor timely at the regional level throughout the NAD.[3] Finally, in resolving the critical problems of information sharing and the subsequent implementation of effective countermeasures within the air domain, no substantive efforts have been made to adapt methodologies, such as intelligence-led policing or other similar organizational models, into the NAD.

The problem of securing the NAD is further exacerbated by the fact that, as a critical subsector of the Transportation Industry identified within *Homeland Security Presidential Directive -7* (HSPD-7), there is currently no standard methodology for local

[2] According to the Office of the Director of National Intelligence, the U.S. Intelligence Community is composed of 16 federal agencies, specifically the: Central Intelligence Agency, Defense Intelligence Agency, Department of Energy, Department of Homeland Security, Department of State, Department of Treasury, Drug Enforcement Agency, Federal Bureau of Investigation, National Geospatial Intelligence Agency, National Reconnaissance Office, National Security Agency, U.S. Air Force, U.S. Army, U.S. Coast Guard, U.S. Marine Corps, U.S. Navy (Office of the Director of National Intelligence, 2010).

[3] This supposition is predicated upon this researcher's experience as a consumer, as well as the recurring complaints of many other major U.S. airport operators; it is not suggesting any willful malfeasance, but rather is identifying a significant homeland security policy issue that needs to be addressed if a true federal, state and local partnership is to exist in the defense of the NAD. In fact, in further support of this hypothesis, this researcher completed a survey related to this matter using 20 of the busiest U.S. airports as a sample population. The results of this survey, which was conducted in August 2009 in the course and scope of this author's regular duties, reveals that 19 of the 20 aviation security managers surveyed do not believe they receive adequate threat assessment information from DHS-TSA; the twentieth airport's security manager was unavailable and did not respond to the survey.

aviation security managers to utilize in conducting vulnerability risk assessments at the nation’s commercial aviation facilities (White House, 2003a). As such, coupled with the problems associated with a lack of information sharing, the NAD remains vulnerable to exploitation and attack by the nation’s enemies.

B. RESEARCH QUESTIONS

1. Primary Questions

- To what extent, if any, may a form of intelligence-led policing be adapted to better secure the National Aeronautical Domain?
- What is an effective and consistent threat appraisal methodology that could be utilized by U.S. aviation security managers in discerning current security posture, estimating future infrastructure requirements, and ultimately gauging the viability of countermeasures deployed in response to received threat assessment information within the National Aeronautical Domain?

2. Secondary Question

- Which effective policies and procedures could be adapted from the successful aviation security models of Israel, Great Britain and Australia?

C. LITERATURE REVIEW

Consistent with the overarching intent of the 2007 *National Strategy for Aviation Security* (DHS, 2007b), the specific purpose of this literature review is to examine the existing body of scholarly work related to the improvement of the security of the National Aeronautical Domain. The assimilation, analysis, dissemination, and incorporation of threat assessment information into aviation security field operations is often broadly cited as a necessary step in better defending the NAD but little has actually been written regarding the substantial implementation of this process for local aviation security practitioners across the nation. Moreover, there is no practical guide or operational model instructing the local security manager how to institute an effective aviation-sector defensive plan that merges the disciplines of the intelligence process together with the risk assessment/management process. Accordingly, in order to achieve the goal of developing a cogent national aviation security doctrine that fuses both the intelligence and risk management processes, three principal sub-categories of literature must be examined, namely: 1) a review of the U.S. Intelligence Community and processes; 2) an evaluation of applicable security risk assessment methodologies appropriate for use within the NAD and 3) an exploration of homeland security organizational models that might better achieve the critical objective of denying future adversaries' access to the NAD.

1. U.S. Intelligence Community and Processes

In a civilian environment and long before the tragedy that befell the nation on September 11, 2001, members of the U.S. aviation security community understood the necessity for the timely intelligence preparation of the aviation security operating environment in order to appropriately plan and defend against potential adversaries to the NAD. Indeed, this point was formally proffered in the *1989 President's Commission on Aviation Security and Terrorism* (President's Commission)[4]when that investigative body noted the federal government's fundamental failure to gather, assess and disseminate threat assessment information to local security partners in a timely and appropriate manner (White House, 1990). As a consequence of this finding, the Federal Aviation Administration, the TSA's predecessor for aviation security matters, created the position of a federal security manager to serve as the "conduit for aviation-related intelligence" from the federal government to the local security manager (White House, 1990). Furthermore, in order to promote federal-local collaboration, section 3.23 of the *President's Commission Final Report* also made the recommendation to "give properly cleared airline and airport security personnel access to the classified information they need to know" (White House, 1997). This proposal was submitted, according to the same report, because threat assessment information was being "sanitized" to the point of being irrelevant for the local authorities who are actually responsible for providing the majority of security countermeasures across the NAD.

[4] This Commission was created in the aftermath of the 1988 bombing of Pan American Flight 103 over Lockerbie, Scotland.

Similarly, Chapter 13 of the *9/11 Commission Report* determined that the IC had failed to properly share threat assessment information across the full spectrum of domestic security agencies in advance of the 9/11 attacks (subsection 13.3). Indeed, this revelation was specifically cited in that investigative body's retrospective recommendation entitled, *Unity of Effort in Information Sharing* (subsection 13.3). In this section of the *9/11 Commission Report*, the commissioners strongly repudiate the IC's traditional Cold War era assumptions that information should be shared only on a "need to know" basis; rather, the *9/11 Commission Report* authors cite a new standard of threat assessment information dissemination that should be adopted at all levels of government and referred to the concept as a culture that must recognize a "need to share" (subsection 13.3). A plethora of other IC reports, programs and laws then emanated from the *9/11 Commission Report* recommendations related to the overall topic of the U.S. intelligence process. Notably among the changes borne from the *9/11 Commission Report's* work is the enactment of the *Intelligence Reform and Terrorism Prevention Act of 2004* (IRTPA).[5]

The IRTPA serves as the legal instrument by which the IC is to be restructured, transformed and improved—for the benefit of organizations at all levels of government. Recognizing the disparate and autonomous nature of IC's agencies, the IRTPA established a director of national intelligence (hereafter the "DNI") to oversee all IC agencies and operations, inclusive of the U.S. Central Intelligence Agency. Principally amongst the IRTPA's Congressional mandates, then, of which there are many, the DNI has been commissioned to "promote intelligence information sharing within the IC" (Title I, Subtitle A, Sec. 1011). Furthermore, the IRTPA's Title IV, Subtitle A (Sec. 4011) requires the Secretary of Homeland Security to "develop and implement a National Strategy for Transportation Security and transportation modal security plans," many of which are specifically related to the security of the NAD.

[5] The Intelligence Reform and Terrorism Prevention Act of 2004 was adopted by Congress on December 6, 2004.

National Security Presidential Directive-47/Homeland Security Presidential Directive-16 (NSPD-47/HSPD-16)[6] mandated the further refinement and development of U.S. aviation security policy (White House, 2006). From the seven plans that sprung from NSPD-47/HSPD-16, the *Air Domain Surveillance and Intelligence Integration Plan*[7] is most notable for this portion of the literature review (DHS, 2007a). Herein, the U.S. Department of Homeland Security provides an overview of the importance of threat intelligence sharing within the NAD and broadly defines its strategy to effect "air domain awareness" to all aviation security partners across the NAD. Indeed, this plan recognizes the essential use of threat assessment information as a "critical enabler" in aviation security operations for "operational decision-makers" within the domain (DHS, 2007a, p. 1). But the relative value of threat assessment information is diminished, and a viable protective plan cannot be developed and implemented, unless aviation security practitioners understand exactly which critical assets are vulnerable to exploitation and attack.

2. Security Risk Management and Methodologies

Further complicating matters, beyond the basic assessments and standard countermeasures now mandated by the TSA, is the fact that a few U.S. airport security authorities have instituted a comprehensive, regimented and continuous risk management program that seeks to root out and address vulnerabilities in a proactive and recurring fashion. In fact, historically, most U.S. airport authorities simply establish the minimum TSA-mandated baseline protective measures and then adjust their security posture thereafter based upon known threats if and when they are identified. Consequently, a survey of the sub-literature associated with risk assessment methodologies applicable to the NAD is also within the scope of this research.

[6] The NSPD-47/HSPD-16 was issued by President George W. Bush in June 2006, and directed the Department of Homeland Security, to develop a comprehensive U.S. aviation security policy.

[7] The *Air Domain Surveillance and Intelligence Integration Plan* was published on March 26, 2007 as a supplement to the *National Strategy for Aviation Security* ordered by NSPD-47/HSPD-16.

Presidential Decision Directive-29 (PDD-29) was signed in 1994 by President Bill Clinton and ordered the Joint Security Commission[8] to develop and implement, among other plans, a risk assessment methodology more relevant for the federal government and its industry partners for the post-Cold War era (White House, 1994). From Chapter 1 of this PDD, a five-step risk management procedure was identified that sought to mitigate risk in a variety of applications by providing "a rational, cost-effective and enduring framework" for security decision-makers in both assessing risk and applying appropriate counterterrorism measures. The Central Intelligence Agency's (CIA) Office of Security later refined this risk management model and labeled it "Analytical Risk Management" (Joint Security Commission, 2004). More recently, a 2001 U.S. General Accounting Office report, *Homeland Security: Key Elements of a Risk Management Approach*, buttresses or corroborates the Joint Security Commission's findings relative to the essential elements of a sound risk management program, and stresses that rather than value alone, the "criticality" of an asset must be also included in a security manager's decision-making process (GAO, 2001a, p. 1).

Superseding the *May 1998 Presidential Decision Directive/N.S.C.-63* concerning "critical infrastructure protection," *Homeland Security Presidential Directive-7* (HSPD-7) was signed by President George W. Bush in December 2003 (White House, 2003). HSPD-7 established a mandate for federal agencies to identify and prioritize U.S. critical infrastructure sectors and develop plans for each sector's protection against future attack. This Presidential Directive resulted in the development of the *National Infrastructure Protection Plan* (NIPP). Emanating from the NIPP for the transportation sector, the Department of Homeland Security developed the *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan* (TSCI /KRP). The TSCI /KRP, which is inclusive of the U.S. Aviation Sub-Sector, establishes "a systems-based risk management strategy" to improve the overall security posture of the NAD (DHS, 2007c).

[8] The "Joint Security Commission" was composed of the Deputy Secretary of Defense and the Director of the Central Intelligence Agency, and their designees or commissioners, "to provide coherent security policy development, security policy evaluation and security policy oversight to the Defense and Intelligence Communities" (Joint Security Commission, 2004). The risk assessment models developed by this Committee were reportedly later adopted by both government and industry alike, but if so, the methodology has not been widely publicized within the current TSA-regulated aviation industry and the local level.

However, while very useful, it is important to note that the TSCI/KRP does not include either tactical or operational planning elements, save and except a short notation under the document's Appendix A that mandates local airport operators' responsibility to adopt "baseline measures" as promulgated by the TSA. Otherwise, the TSCI/KRP generally refers to the seven overarching federal programs linked to TSA's *National Strategy for Aviation Security,*[9] none of which details a specific risk-assessment/management methodology. As such, a brief survey of risk assessment methodologies is included herein for review.

Several risk assessment methodologies (RAM) exist that are appropriate for the local security manager's use within the NAD. For example, Sandia National Laboratories, in conjunction with the U.S. Department of Energy Nuclear Regulatory Commission, has developed a variety of systematic RAMs applicable to most critical infrastructure/key resource (CI/KR) sectors to assess high-risk facilities and operations relative to four specific criterion: 1) discernment of various threats to both physical and cyber assets; 2) analyses of the vulnerabilities of the structure(s) or other assets to be defended; 3) determination of the likely results of a successful attack; and 4) determination of the most viable countermeasures to be deployed to mitigate risk. Similarly, the NI-2 Center for Infrastructure Expertise[10] endorses the criticality, accessibility, recoverability, vulnerability, effect, and recognizability methodology (CARVER), and its variations, as a prudent means of conducting target analysis and risk assessment (NI2 Center for Infrastructure Expertise, 2009). Finally, the U.S. Department of Defense (DoD) Joint Chiefs of Staff Joint *Publication 3-07.2 Antiterrorism,*[11] specifies the use of the mission, symbolism, history, accessibility, recognizability, population and

[9] The TSA's National Strategy for Aviation Security is composed of seven aviation-specific plans, namely: the *Aviation Transportation System Security Plan* (2007); *Aviation Operational Threat Response Plan* (2007); *Aviation Transportation System Recovery Plan* (2007); *Air Domain Surveillance and Intelligence Integration Plan* (2007); *International Aviation Threat Reduction Plan* (2007); *Domestic Outreach Plan* (2007); and finally, the *International Outreach Plan* (2007).

[10] NI2 is a National Institute of Standards and Technology grant-funded group.

[11] *Joint Publication 2-07.2: Antiterrorism* is a 2006 publication by the U.S. Joint Chiefs of Staff that provides detailed guidelines for military commanders on issues relative to force protection and risk assessment/management. The publication specifically endorses both the CARVER and MSHARPP risk assessment methodologies (DOD, 2006).

proximity methodology (MSHARPP) as another robust means to analyze likely targets and develop appropriate countermeasures (DoD, 2006). In summary, although not actively promoted by TSA, the local aviation security manager possesses access to a wide variety of bonafide resources related RAM; however, no particular functional structure has been instituted within the NAD to combine threat assessment information and RAM within the context of a predefined organizational model.

3. Homeland Security Organizational Models

Assuming that a local U.S. aviation security manager can achieve success in both receiving additional, enhanced and more timely threat assessment information, and also assuming that the same security manager is willing to institute a continuous risk management program, which type of organizational model should exist that would effectively tie or fuse these two functions together? The process of developing and maintaining a multi-layered, defense-in-depth security posture within the environmental dynamics of a major U.S. aviation facility is problematic. Consequently, an all-inclusive security management organizational methodology must also be adopted if success is to be achieved in better securing national aviation assets. Since U.S. aviation security managers have never embraced any type of an established security management construct, consideration should be given to management models developed in American policing. Intelligence-led policing (ILP), CompStat and community oriented policing (COP) are examples of police management organizational models that may be adapted for use within the air domain.

Ratcliffe (2008) states that ILP is a police management approach that has evolved from CompStat and COP strategies, but “holds out the promise of a more objective basis for deciding priorities and resources allocation . . . [by] using an analysis-driven approach to decision-making” (p. 4). Carter (2004) explains that threat assessment information ought to form “part of the fabric of decision making” for organizational leaders, and denotes further that the concept of intelligence-led policing “is explained from an operational perspective, illustrating its interrelationship with community policing and

CompStat."[12] In summary, Carter draws a conclusion throughout his publication that both CompStat and ILP share many common elements that may be useful for aviation security managers, such as: 1) both management strategies focus on prevention, a key element of aviation security operations; 2) each policing style requires the collection of data, analysis of that data, as well as a nimble organizational response capability; and 3) both ILP and CompStat are influenced by operational needs with respect to reducing vulnerability to crime.

Similarly, the U.S. Department of Justice's (DOJ) Office of Community Oriented Policing defines community oriented policing as ". . . a philosophy that promotes organizational strategies, which support the systematic use of partnerships and problem-solving techniques, to proactively address the immediate conditions that give rise to public safety issues such as crime, social disorder, and fear of crime" (DOJ, 2008). COP, in other words, presumes that an efficient crime control model may be achieved by the police partnering with the community, identifying the root causes of crime ("the problems") and addressing them together as a community. To achieve this goal, a COP model requires police officers to become general practitioners in their field, as opposed to specialists operating in just one sub-category of law enforcement service.

4. Summary

While the historical issues and evolution of the U.S. intelligence process is a topic rich in subject matter, none of the literature surveyed denotes specifically how the problem of a "failure to share" information is to be overcome in any sector, much less within the NAD. The issues relative to defending the NAD are thus compounded by a lack of timely threat assessment information dissemination throughout the U.S. aviation sector. As a consequence of the gap in information flow from the IC to the local aviation security practitioner, then, regional security actors are left to formulate protective plans

[12] The term "CompStat" refers to "computer statistics," which is a program originally developed at the New York Police Department that utilizes statistical information to inform police commanders about issues related to criminal activity.

based principally upon the speculation of various threat streams[13] vis-à-vis any risk/vulnerability assessments that may have been conducted for the facility and personnel to be protected. Given the fact that no particular aviation security doctrine has been established combining the aviation intelligence process with the risk assessment/management process, additional research is merited to determine if a particular homeland security organizational model, such as ILP, CompStat or COP, may achieve the desired results of merging the disciplines of intelligence and RAM with the ultimate goal of hardening the NAD against future adversaries. If this can be achieved, however, perhaps a foundation for aviation security doctrine may be established throughout the NAD.

D. HYPOTHESIS

The intent of an effective national aviation security program is to reduce risk by detecting, deterring, delaying and denying potential adversaries' access to security-sensitive segments of the NAD. In order to accomplish this goal, two indispensible elements must be received, fused and acted upon, specifically: 1) the timely receipt of credible threat assessment information must obtained by U.S. aviation security managers; and 2) a well-developed understanding of a target's assets, vulnerabilities and contingent risks must be assessed by NAD security managers so that appropriate countermeasures may be then be deployed. In sum, tailoring aviation security strategies to both threat information and risk assessments, based upon local circumstances, will provide the most successful model for securing the NAD from evolving future threats, but currently no national operational security doctrine has been developed that formally inculcates an intelligence-driven, risk-based security strategy within the U.S. civil aviation infrastructure. Accordingly, the development and unified adoption of such a doctrine across the air domain would substantially improve U.S. aviation security.

[13] The term "threat streams" is defined by this researcher as a potential route, direction or manner from which terrorism-related acts may emanate.

E. SIGNIFICANCE OF RESEARCH

This research will principally benefit U.S. aviation security practitioners at the local level by providing a substantive policy option relative to better securing the National Aeronautical Domain. This will be accomplished by identifying and combining viable, "smart practices"[14] for the aviation security manager within the realms of both intelligence policy and risk management/assessment strategy. Furthermore, considering the fact that no literature exists that specifically establishes a foundation for aviation security doctrine, this work product will also provide an organizational model for future homeland security professionals to build upon as the threat streams to the U.S. Air Domain evolve over the next several decades. Finally, this research may also benefit both the local and national policy maker, who has toiled with great effort since the published findings of the *9/11 Commission Report*, to formally merge the threat intelligence process with the risk assessment/management process within the NAD.

F. METHODOLOGY

The policy options analysis methodology will be utilized for this thesis project. Accordingly, this research will identify and explain the various elements and problems relative to securing the NAD, particularly at the nation's largest aviation facilities: FAA Category X airports[15]. A review of potential policy options will then be examined, inclusive of potential enhancements that may be realized from various organizational models, technological resources, as well as other successful international aviation security programs. The viability of these alternatives will then be compared and contrasted against conventional security strategies currently in effect. Finally, a recommendation will be made to adopt a policy option that best addresses the problem of

[14] A "smart practice" is "something clever that the researcher must analyze, characterize in words, and appraise as to its applicability to the local situation" (Bardach, n.d.).

[15] FAA Category X airports are those that represent the nation's largest and busiest airports as measured by overall passenger traffic and are therefore considered potentially attractive targets for criminal/terrorist activity (GAO, 1998).

better securing national aviation resources within the context of the evaluation criteria deemed vital for success in this endeavor. Hence, the three policy options cited below are outlined for consideration in this research plan.

1. Policy Options

a. Increase the Frequency of the TSA Risk Assessment Process

Some improvements to the U.S. civil aviation security infrastructure have been realized since 9/11. For example, federalization of the screening workforce, standardization of the passenger/baggage screening processes and implementation of a broad-based triennial threat assessment of Category X airport facilities by TSA have all been incorporated within the NAD. Since large commercial aviation facilities are typically under a perpetual state of construction, reconfiguration and expansion, however, a slight modification and improvement to the national aviation security posture may be realized if the triennial threat assessment currently mandated for Category X airports were required on an annual basis.

b. Improve the Dissemination Element of the Intelligence Cycle[16] Within the NAD

Homeland security intelligence processes have improved since 9/11, but instituting federal policies and procedures to further refine the dissemination element of the intelligence cycle may help ensure a more timely, regular and detailed distribution of threat assessment information to aviation security operators. This option might include the selective sharing of classified threat assessment information regarding emerging threats within the NAD, which may ultimately assist the local aviation security manager at Category X facilities in better understanding and responding to the overall threat picture within the aviation domain.

[16] According to Johnson and Wirtz (2008), *Intelligence and National Security: The Secret World of Spies*, the U.S. intelligence cycle consists of five steps: planning and direction, collection, processing, analysis and production and dissemination (p. 49).

c. Institute an Intelligence-Driven, Risk-Based Security Doctrine

Introduce federal legislation and or policies to mandate the improved sharing and utilization of threat assessment information, along with the incorporation of a standardized risk-based management methodology, into all U.S. aviation security programs at Category X airports across the nation. This option would necessarily also include a mandate for each local aviation security operator to institute an appropriate organizational model to analyze and respond to threat assessment information vis-à-vis specific risk appraisal and reduction criteria.

2. Hierarchy of Criteria for Judging Success/Failure

a. Legality

Refers to the legal permissibility of state and federal statutes with regard to instituting recommended changes.

b. Effectiveness

The total projected benefit to be yielded upon implementation of any proposed changes.

c. Political Acceptability

Relates to the acceptability of any proposed changes by local, state and federal legislative and executive bodies; also to the American public as a whole.

d. Level of Effort

The total amount of energy or exertion required by the managing body to implement any recommended changes.

e. Cost

Refers to the monetary expense associated with implementing recommended changes.

3. Policy Options Matrix

Table 1. Policy Option Matrix

Policy	Cost	Legality	Political Acceptability	Level of Effort	Effectiveness
A	Low	Yes	Poor	Minimal	Minimal
B	Low to Med	Yes	Med	Med	Med
C	Med to High	Yes	High	Med to High	High

THIS PAGE INTENTIONALLY LEFT BLANK

II. U.S. AVIATION SECURITY: AN OVERVIEW

A. SIZE AND SCOPE OF THE U.S. NATIONAL AERONAUTICAL SYSTEM

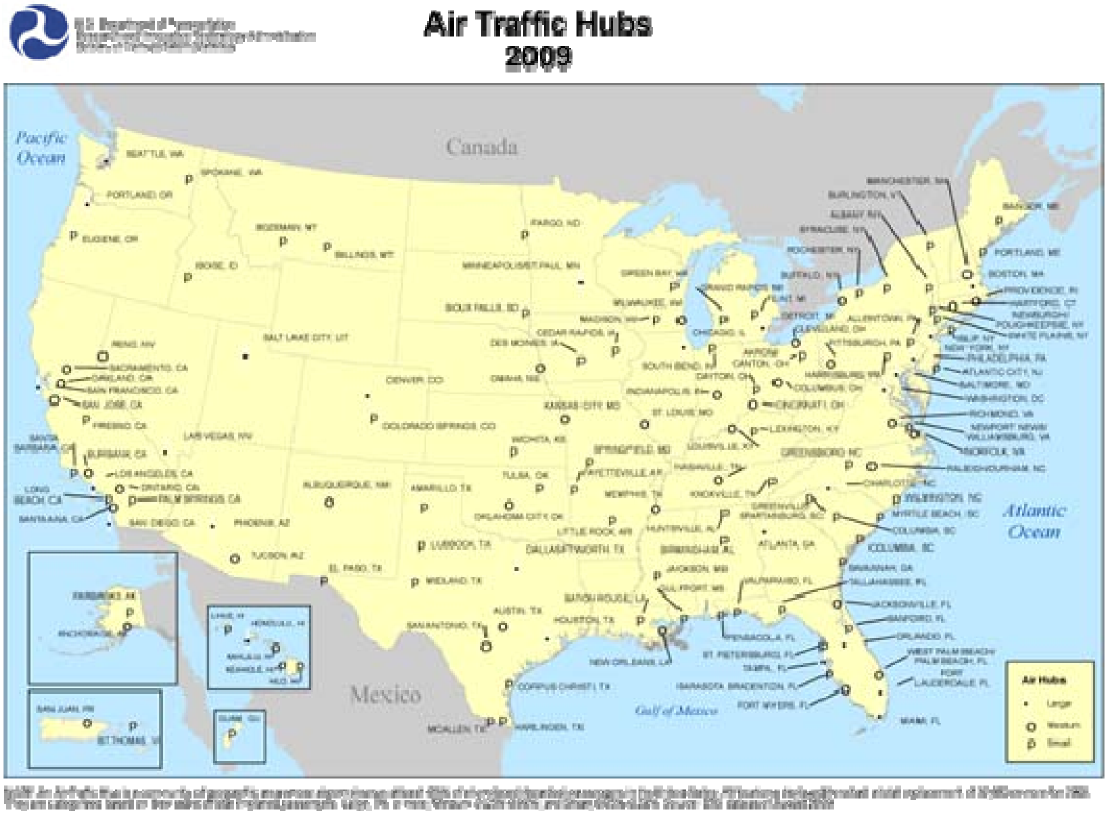

Figure 1. Air Traffic Hubs 2009 (From U.S. Department of Transportation, 2009)

The National Aeronautical Domain (NAD) is composed of a total of 18,345 civil aeronautical landing areas,[17] and of this number, 413 are classified as "primary commercial service" aviation facilities (Wells, 2000, p. 46). Of these primary commercial service facilities, several principal categories of commercial airports are further identified and sub-divided by operational type, to wit: 1) Large-hub primary airports; 2) Medium-hub primary airports; 3) Small-hub primary airports, and 4) No-hub primary airports

[17] Wells & Young define civil aeronautical landing areas as all "airports, heliports, STOLports [short take-off and landing]" within the U.S., inclusive of approximately 13,000 private-use airports (2004, p. 526).

(Wells & Young, 2004, p. 13). U.S. Code (U.S.C) Title 49 § 47102 defines Large-hub primary airports as those with annual enplanement populations of at least one percent of the total annual passenger enplanements accounted for within the United States. For aviation security purposes, the FAA and TSA also commonly know and refer to large hub aviation facilities as “Category X” airports. Similarly, medium-hub airports are defined by 49 U.S.C § 47102 as commercial service airports that facilitate the movement of at least 0.25 percent but less than one percent of the annual total passenger boardings within the United States. For aviation security purposes, these facilities are commonly known and referred to as “Category I” airports. Small hub airports are those commercial aviation facilities that enplane at least 0.05 percent but less than 0.25 percent of passenger boardings annually (U.S.C 49 § 47102). Non-hub commercial service airports are defined by 49 U.S.C § 47102 as those with less than 0.05 percent of total U.S. passenger boardings per year.

For federal aviation security purposes, the U.S. General Accounting Office (GAO) cites the existence of 27 Category X, and 55 Category I, airports in the United States (GAO Report GAO-07-299, 2007). Other categories of airports within the small- and no-hub classifications are recognized by the FAA and TSA as well, such as Categories II, III and IV varieties. However, not all of these aviation facilities are capable of accommodating either large annual passenger populations or large commercial aircraft.[18]This factor is a significant consideration in air domain threat analysis due to both aircraft fuel and passenger load capacities. Accordingly, as compared to Category X facilities, since Category I, II, III, and IV airports are much smaller in both physical size and overall passenger enplanement capacity they will not be included within the scope of this research.

Within the framework of the nation’s commercial aviation infrastructure, the U.S. Department of Transportation’s Bureau of Transportation Statistics (DOT) reports that a total of 618,113,048 passengers traveled on domestic flights during calendar year 2009 (DOT, 2010). Based upon a 365-day year, this statistic equates to approximately 1.7

[18] For the purposes of this research, large, commercial aircraft are considered Boeing 747, 757, 767, and 777 varieties. This list is only a representative sample, however.

million passengers per day transiting through America's primary commercial service airport complexes. Wells & Young (2004) cite that approximately 70 percent of this total passenger traffic is funneled through Category X airport facilities (p. 15). Therefore, the overwhelming mass of all aviation passenger traffic is enplaned through relatively few very large facilities, a significant fact when considering network theory[19] in the allocation of security resources across the NAD.

The following graphical representation outlines the percentage of U.S. aviation facilities within each of the aforementioned airport classifications. Consequently, as reflected in the below-referenced chart, Category X and Category I commercial aviation facilities represent only about 18 percent of the nation's largest and busiest airport facilities in terms of geographic size, passenger enplanement levels, as well as total aircraft landings and departures. In order to devote the majority of attention and scare resources to the most critical segment of the U.S. air domain, then, the focus of the security strategy presented in this research project will center upon the geographically large and vastly populated, yet relatively small number of Category X airports within the U.S. NAD.

[19] In his book *Critical Infrastructure Protection in Homeland Security*, Ted Lewis at the U.S. Naval Postgraduate School defines network theory as the study of "a collection of nodes and links that connect pairs of nodes" and "provides a formal foundation for a scientific study of critical infrastructure protection" (Lewis, 2006, p. 77).

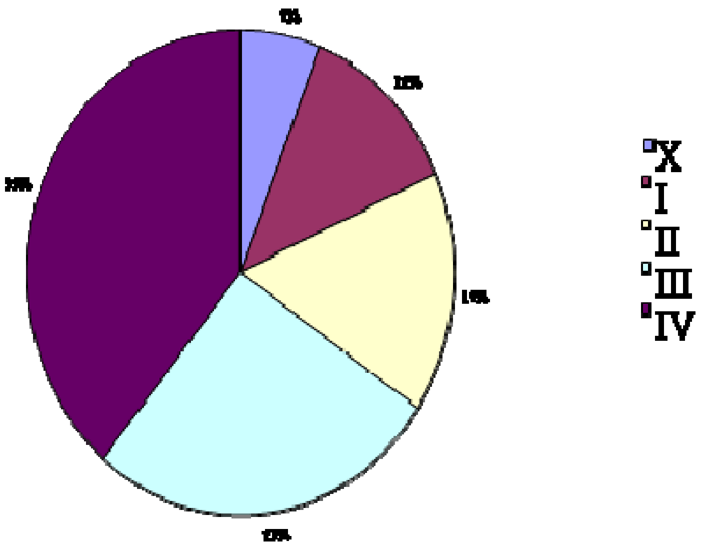

Figure 2. Commercial Airports by Airport Security Category as of April 2006 (From GAO, 2007)

B. POST-9/11 EVOLUTION OF U.S. AVIATION SECURITY

Ensuring the adequate defense of the NAD is vital to both the physical and economic security interests of the United States. As a critical component of the national transportation infrastructure, the collective and sustained efforts of all levels of government must come to bear upon the deterrence, detection, denial and delay of future adversaries to the NAD. This fact is particularly true today in the aftermath of the September 11, 2001 (9/11) tragedy—a disaster that left almost 3000 innocent people dead, national symbols of strength and wealth destroyed and damaged, along with the unprecedented closure of the U.S. civil aviation transportation system.[20] With this horrific act as the impetus, the nation's leaders immediately recognized that the enemies that attacked America on 9/11 continued to plot against U.S. national interests with the

[20] Based upon the 9/11 Commission testimony of Secretary of Transportation Norman Y. Mineta on May 23, 2003, the NAD had never been ordered completely closed to civil aviation assets in the history of aviation (Mineta, 2003).

intention of replicating the same type of catastrophic physiological and psychological damages, death and destruction that the world witnessed on 9/11.

Indeed, the long-term, post-9/11 commitment of al-Qaeda to attack America by exploiting the aviation domain has been evidenced in the following cases, specifically:

- The December 22, 2001 attempt by al Qaeda operative Richard Reid in his failed attempt to detonate an explosive device concealed in his shoe while in flight aboard American Airlines Flight 63, a transatlantic flight from France to the United States;
- The 2006 al Qaeda plot against commercial airliners uncovered and thwarted by British counter-terrorism agencies in Operation OVERT,[21] and
- The December 25, 2009 attempt by al-Qaeda operative Umar Farouk Abdulmutallab in his failed attempt to detonate an explosive device concealed in his undergarments while in flight aboard Northwest Airlines Flight 253, a transatlantic flight from the Netherlands to the United States.

Understanding that America had been thrust into an international conflict with a committed, ideologically-driven enemy using unconventional weapons and tactics the likes of which had never before been witnessed, shortly after September 11, 2001, the President and U.S. Congress immediately responded by launching the Global War on Terror (GWOT). This reaction, in addition to the global deployment of military and law enforcement assets, also resulted in the creation of a myriad of investigative bodies, legislative reforms and realignment of homeland security and defense resources. For the national aviation sector, chief among these earliest counterterrorism plans were the *Aviation Transportation Security Act of 2001*[22] and the creation of both the Transportation Security Administration (TSA)[23] and U.S. 9/11 Commission.[24] The U.S.

[21] Operation OVERT was announced on August 10, 2006 by British Home Secretary Dr. John Reid. In his public statement, Home Secretary Reid revealed that British counter-terrorism agencies had detected and disrupted an al- Qaeda plot to attack transatlantic airliners en route from the United Kingdom to the United States where flights to New York, Washington, D.C., and California were to be destroyed in flight by al-Qaeda operatives who had smuggled liquid explosives on-board (Reid, 2006).

[22] This was created by the President and Congress by Public Law 107-71 on November 19, 2001.

[23] This act also transferred the responsibility of aviation security from the Federal Aviation Administration to the newly created TSA.

[24] This was created the President and Congress by Public Law 107-306 on November 27, 2002.

Department of Homeland Security (DHS)[25] was subsequently created and assumed, among many other duties, operational responsibility and oversight for the nation's aviation security through the newly formed TSA.

C. SECURITY WORKGROUPS WITHIN THE U.S. AVIATION DOMAIN

Although a more in-depth analysis of both U.S. airport security operators' and TSA's Office of Security Operations (TSA-OSO) security responsibilities will be included later in this chapter, the following summary provides an overview of the various other law enforcement and security workgroups that operate at U.S. Category X airports. Accordingly, U.S. airport security operators liaison with, and oftentimes support, the following agencies:

1. Local Law Enforcement

49 U.S.C § 1542.217 requires U.S. airport security operators to provide uniformed police officers in the number and manner adequate to support its aviation security program. This support may be provided either by a proprietary law enforcement service (police officers employed and commissioned by the airport authority itself) or via a contractual agreement with an outside police agency with the local airport security operator. Both law enforcement support models are common within the NAD; but as the regulated party, it should be noted that the local airport security operator ultimately retains the responsibility and regulatory liability from TSA for any infractions or violations committed by local law enforcement personnel vis-à-vis any of the requirements stipulated by the federal code as it relates to law enforcement support and response.

2. Federal Bureau of Investigation (FBI)

Since major aviation facilities represent targets of high-value for various terrorist factions, most Category X airports host a contingent of FBI special agents known and

[25] This was created by the President and Congress by Public Law 107-296 on November 25, 2002. This act also transitioned the administration and oversight of the TSA into DHS.

referred to as “airport liaison agents.” This federal law enforcement presence is due principally to the FBI’s primary role in investigating acts of terrorism pursuant to the mandates of the 28 U.S.C § 533.

3. Department of Homeland Security (DHS)

The DHS maintains several components of its organization in Category X airports across the nation. For example, while the Federal Air Marshal’s Service (FAMS) provide some airport security services on an ad-hoc basis, the crux of the FAMS mission lies in providing covert, armed personnel aboard commercial aircraft in flight to interdict acts of air piracy and hostage-taking. Since Category X airports are also typically international ports of entry as prescribed by U.S. Customs and Immigration law, the U.S. Customs and Border Protection Service (CBP) provides federal inspection services for international travelers, baggage and products presented for admission into the U.S. from foreign destinations. CBP’s sister agency, the Immigration and Customs Enforcement Service (ICE), provides the federal law enforcement support necessary for CBP in investigating suspected violations of customs and immigration law. More specifically, ICE’s mission includes the interdiction of human, narcotics, currency, arms and other forms of international trafficking schemes. On a daily basis, however, local airport security operators interact with the TSA-OSO in the proactive security of the NAD.

D. DIVISION OF AVIATION SECURITY RESPONSIBILITIES: TSA-OSO PRINCIPAL ROLES

Among the many sub-components that now compose the federal transportation security apparatus, the TSA’s-OSO for the aviation sector has subsequently been commissioned to perform very limited operational security duties within the NAD as well as disseminate specific threat assessment information to authorized individuals at the nation’s airports. More specifically, the TSA field office personnel deployed at the local level are assigned three primary tasks by law, that is: 1) to screen passengers and baggage for prohibited items;[26] 2) to ensure regulatory oversight and implementation of federally-mandated rules at local airport facilities; and 3) to ensure dissemination of threat assessment information and provide conditional assessments of the same to aviation security policy stakeholders (U.S. Congress, 2002). Unfortunately, TSA is currently only fulfilling responsibilities one and two, a fact which will be addressed later in Chapters III and IV of this thesis. Nevertheless, as the federal statutes relate to the TSA's crucial mission functions, Public Law 107-71 provides the following specific mandates for TSA pursuant to Title I of the Act:

> § 114. (f): (1) receive, assess, and distribute intelligence information related to transportation security;
>
> (2) assess threats to transportation security;
>
> (4) make other plans related to transportation security, including coordinating countermeasures with appropriate departments, agencies, and instrumentalities of the United States Government;
>
> (7) enforce security-related regulations and requirements.

These basic TSA duties and responsibilities have been further supplemented since their initial adoption by the promulgation of seven different aviation security plans that were ordered by Presidential Directive 47/Homeland Security Presidential Directive 16 (NSPD 47/HSPD 16). Together these plans constitute the *National Strategy for Aviation Security* (DHS, 2007b). Of particular importance within the *National Strategy for Aviation Security* (NSAS), in 2007 the Secretary of Homeland Security stated, in relevant part, that ". . . public and private sectors must work together to improve national security by: sharing threat information . . ." (DHS, 2007b, p. 13). Furthermore, the *Air Domain Surveillance and Intelligence Integration Plan*, one of the seven appendant strategies referenced above, specifically cites the intent of this particular measure is the coordination of "requirements, priorities, and implementation of national air surveillance resources and the means to share this information with appropriate stakeholders" (DHS, 2007a, p. 1).

[26] Although the initial identification of prohibited weapons in passenger and baggage screening is a principal function of TSA at local airports, the retention and disposal of these identified weapons, and the arrest(s) of suspects, etc., is generally the responsibility of local airport authorities.

In sum, TSA, specifically TSA's Office of Security Operations, is responsible for: 1) working with airport operators/authorities to develop baseline security measures at all legally recognized U.S. airport facilities; 2) provide both specific threat assessment information as well as overall NAD threat assessments to stakeholders, and 3) regulate individuals and entities at airport facilities subject to the regulatory control and oversight of TSA as mandated by the U.S. Code of Federal Regulations. When coupled with the U.S. Office of the Director of National Intelligence's (ODNI) 2008 report entitled *Information Sharing Strategy*, the main theme of which is moving the Intelligence Community[27] (IC) from a culture of "need to know" into a culture of "responsibility to provide," two clear legal and operational expectations emerge: 1) that the TSA Office of Security Operations is expected to partner with local airport operators to develop coherent baseline aviation security measures; and 2) the TSA Office of Security Operations is responsible for the regular and timely dissemination of both national threat assessment information as well as more specific threat assessment information to local airport operators. Without a doubt, both of these components are critically necessary if commercial airport operators are to develop and maintain effective aviation security programs. This type of collaboration is especially necessary for local aviation security program managers who seek to be proactive and extend protective plans beyond that which is minimally required by the current static, federally mandated baseline measures.[28]

[27] The IC is a federation of executive branch agencies and organizations that work separately and together to conduct intelligence activities necessary for the conduct of foreign relations and the protection of the national security of the United States (ODNI, 2008).

[28] This simply means that local airport authorities may wish to voluntarily enhance their airport's security posture above and beyond what the federal government has mandated as minimum standard, but are unable to do so effectively because of the lack of threat assessment information forthcoming from federal intelligence resources.

E. DIVISION OF AVIATION SECURITY RESPONSIBILITIES: LOCAL OPERATOR'S[29] ROLES

In the United States, most of the large commercial airport facilities are owned by either governmental entities or "quasi-governmental bodies" (Wells, 2000, p. 46). Irrespective of an airport's status of legal ownership, however, the body or group that manages the facility is known and commonly referred to as an "airport operator." 49 C.F.R. § 1542 governs the specific TSA-mandated aviation security requirements of a U.S. airport operator. Cited in relevant part for this thesis, the aviation security requirements of a U.S. airport operator, pursuant to 49 C.F.R. § 1542, are to:

- Develop and maintain a TSA-approved Airport Security Plan (ASP)[30] that identifies the baseline[31] security measures that the airport operator will incorporate at the facility (§ 1542.101);
- Identify one individual to act as the Airport Security Coordinator (ASC) to serve as the immediate contact for security-related activities and communications with TSA (§ 1542.3);
- Provide detection and physical security measures of the "secured area," i.e., the most security-sensitive area(s) at an airport where aircraft fueling and enplanement/deplanement of passenger operations are conducted (§ 1542.201);
- Provide detection and physical security measures for the "Aircraft Operations Areas" (AOA), i.e., the areas that encompass the taxiway and runway systems where aircraft operate (§ 1542.203);
- Provide detection and physical security measures for the "Security Identification Display Area" (SIDA), i.e., the area of an airport where aircraft fueling and loading/unloading of cargo operations are conducted (§ 1542.205);

[29] TSA defines "airport operator" as a person that operates an airport serving an aircraft operator of a foreign air carrier required to have a security program under part 1544 or 1546 of this chapter (49 C.F.R. Part 1540, et. seq.).

[30] The ASP represents a formal written agreement between the TSA and the airport operator and specifically outlines what the airport operator must do, as a minimum standard, to ensure aviation security. The ASP does not prohibit an airport operator from instituting additional security measures on its own, however. Additionally, the ASP document is not as comprehensive as most asset, threat, vulnerability and risk-assessment studies.

[31] "Baseline" security measures are those recurring functions and actions that local airport operators must undertake to ensure aviation security. Many of these functions are standardized and mandated by TSA headquarters personnel. Failure to fulfill these minimum standards may result in the airport operator's civil liability.

- Implement and maintain an Access Control System to ensure unauthorized access to security-sensitive areas of an airport complex remain secure (§ 1542.207);
- Provide a fingerprint-based criminal history records check (CHRC) for individuals seeking unescorted access to secure areas of an airport (§ 1542.209);
- Provide an identification or credentialing system for all employees who seek unescorted access to security-sensitive areas of an airport (§ 1542.211);
- Provide security training for security personnel (§ 1542.213);
- Provide law enforcement officers in a sufficient number and manner to support the ASP (§1542.215);
- Develop, maintain and implement upon TSA's demand, a contingency plan to counter threats to aviation security that may arise (§ 1542.301);
- Establish procedures to evaluate bomb threats, threats of sabotage, aircraft piracy, and other unlawful interference to civil aviation operations (§ 1542.307).

F. CHAPTER SUMMARY

As demonstrated by the legal citations referenced above, the actual physical deployment of most aviation security resources at airport facilities across the NAD is the principal responsibility of the local airport security operator. This point is made not to diminish the critical role of the TSA in the aviation security mission, but rather to demonstrate that:

- Apart from baggage and passenger screening responsibilities, U.S. airport operators actually control and maintain the bulk of the personnel, technology and physical infrastructure resources necessary to effectively maintain the security of the NAD;
- That individual airport operators retain the legal responsibility to provide aviation security countermeasures across the NAD; and
- Considering the foregoing, there is a critical need for the local security operator to receive timely, regular and accurate threat assessment information from the U.S. Intelligence Community, inclusive of classified information, in order for security assets to be managed and deployed most effectively *beyond* the TSA-mandated baseline measures found in a commercial airport's ASP.

As already referenced in this chapter, the TSA-OSO has focused the preponderance of its time and resources on both screening operations and regulatory compliance of local airport security operators, leaving the threat assessment element of its statutory mandate nearly untouched. As a consequence, while screening and regulatory compliance mandates are fundamentally necessary to the overall security of the NAD, so too is the dissemination of threat assessment information component of TSA’s mission. This supposition is especially true if local airport security operators are to remain proactive, flexible and adaptive in countering emerging threat streams within the NAD.

III. U.S. INTELLIGENCE COMMUNITY AND CIVIL AVIATION SECURITY

> By the word 'information' we denote all the knowledge which we have of the enemy and his country; therefore, the foundation of all our ideas and actions. (Clausewitz, 1832)

A. INTRODUCTION: WHY IS AVIATION THREAT ASSESSMENT INFORMATION NECESSARY FOR LOCAL SECURITY MANAGERS?

In his quote from over 177 years ago, General Karl von Clausewitz expresses the strategic understanding that threat assessment information is critically necessary in forming the basis of all operational planning when fighting a determined adversary. Likewise, in the war on terrorism that began in 2001 with the exploitation of commercial aviation assets, the current mission of the U.S. civil aviation sector is to defend against another catastrophic terrorist attack on the U.S. homeland from the exploitation of this same sector of the nation's critical infrastructure. Success in this type of a defense can only be achieved by formulating effective aviation security programs that reduce risk by detecting, deterring, delaying, and denying potential adversaries' access to security-sensitive segments of the NAD.

To accomplish this goal, the timely receipt of threat assessment information represents a fundamental component to understanding and subsequently mitigating threat streams because the development, deployment and efficacy of potential countermeasures are contingent upon information received and utilized at the field level of execution. In other words, threat assessment information aides in both the specific and general identification of the types of techniques, tactics and procedures against which security managers may need to defend, especially in the field of critical infrastructure protection. This "need to know," then, is relevant for regional actors[32] at both the federal and local levels who are charged with protective services responsibilities.

[32] "Regional security actors" (also "regional actors") is defined by this researcher as the local Federal Security Director appointed by DHS-TSA as well as the lawfully designated Airport Security Coordinator appointed by a particular airport authority.

In his book *Intelligence: From Secrets to Policy,* Dr. Mark Lowenthal notes that the principal reason intelligence agencies exist is to collect, produce and disseminate threat assessment information and "to keep track of threats, forces, events, and developments that are capable of endangering the nation's existence" (2009, p. 2). While non-state actors such as al-Qaeda probably pose little threat to endangering the existence of the U.S., another successful attack directed against America's critical infrastructure utilizing commercial aviation resources could, nonetheless, produce a disastrous effect not just upon the aviation sector, but upon the populace of the U.S.—physically, psychologically and economically. Thus, the continuous receipt and utilization of threat assessment information by security managers is necessary to help prevent and or mitigate the overall threats, vulnerabilities and consequences of terrorism emanating from within, or otherwise directed toward, the U.S. aviation sector.

B. INTELLIGENCE: DEFINED

But specifically, what is the difference between "intelligence" and "information"? Lowenthal (2009) establishes this distinction as "information is anything that can be known, regardless of how it is discovered. Intelligence refers to information that meets the stated or understood needs of policy makers and has been collected, processed, and narrowed to meet those needs" (p. 1). Consequently, in order to produce threat assessment information that can exploited, the U.S. Intelligence Community (USIC) engages in a specific cyclical process as represented in the graph below.[33]

As graphically demonstrated by the FBI's intelligence cycle below (see figure 3), the U.S. cycle of intelligence flows in a specific, continuous manner in the following

[33] This thesis' co-advisor, Mr. Paul Smith, a retired intelligence professional from the UK's MI-5 (British Security Service), endorses an intelligence cycle with only four components: 1) requirements, 2) collections, 3) analysis, and 4) action. According to Smith, this is because the "dissemination" of a report, as denoted in the U.S. version of the intelligence cycle cited hereinabove, should not necessarily become the outcome of requirements. Smith notes that dissemination of a report "may" be an outcome, but so could the deployment of a surveillance team or other action in the field, not just a written report. However, since research for this thesis project reflects the model graphically represented herein as that which is predominant within the U.S. at the time of this writing, the U.S. model is used with this important notation included for the reader's clarification and future consideration (Smith, 2010).

order: 1) requirements; 2) planning and direction; 3) collection; 4) processing and exploitation; 5) analysis and production; and 6) dissemination. Each segment of the process is explained as such:

According to Lowenthal (2009), the requirements and planning and direction phases of the intelligence process, phases one and two, respectively, are typically influenced by policy makers who determine "those policy issues or areas to which intelligence is expected to make a contribution" (p. 55). In the case of U.S. civil aviation, for example, policy-makers and strategists alike may wish to identify particular threats to the aeronautical domain. For instance, the identification of:

- Which groups or individuals represent a threat to U.S. civil aviation,
- The specific targets within aviation's critical infrastructure area, and or
- The intent and current/future capabilities of the potential adversaries identified.

In phase three of the process, collection, Lowenthal (2009) notes that general information, not intelligence, is gathered by one or more methods at this point (p. 55). Carter (2009, p. 63) cites those various methods of intelligence collection as:

- Human intelligence (HUMINT), which is the use of human beings to solicit and collect information;
- Signals intelligence (SIGINT), which is a generic term for the electronic interception of information being transmitted/received (for example, from an electronic signal generated by a telephone/radio/email/etc.);
- Imagery intelligence (IMINT), which is that information derived from photography, infrared image capture, satellites, radars, etc.;
- Measurement and signatures intelligence (MASINT), which is the "analysis of electronic emanations from equipment and seeks to detect information patterns in a different part of the electronic spectrum not previously captured by other methods";
- Open source intelligence (OSINT), which is the analysis of information available to the general public.

The FBI's intelligence cycle phase four is identified as processing and exploitation. In this segment, collected information begins the transformation of becoming intelligence after, according to Carter (2009), four considerations are made:

1. Evaluation of the raw data is made by intelligence analysts with regard to source reliability and information validity;
2. Evaluation of the method of data collection is conducted;
3. Integration/collation of new data with existing information has been completed; and
4. De-confliction, with pre-existing information suggesting contrary results or expectations, has been reconciled (pp. 64–65).

The fifth phase, analysis and production, is the center of the intelligence process. At this stage, the analytic process is begun in earnest by analysts utilizing both quantitative as well as qualitative research methodologies to develop previously collected segments of information into intelligence products.

Dissemination represents the sixth and final phase of the FBI's intelligence cycle before it repeats itself. Futhermore, according to Lowenthal (2009), is the process of transferring finished intelligence products "from the producers to the consumers" (p. 62). Carter (2009) concludes his discussion of the dissemination phase by noting that the post-9/11 philosophy of sharing information is supposed to be "radically different" in that now intelligence information is supposed to be shared as widely as possible with those who need it in hopes to "prevent threats from reaching fruition" (p. 69).

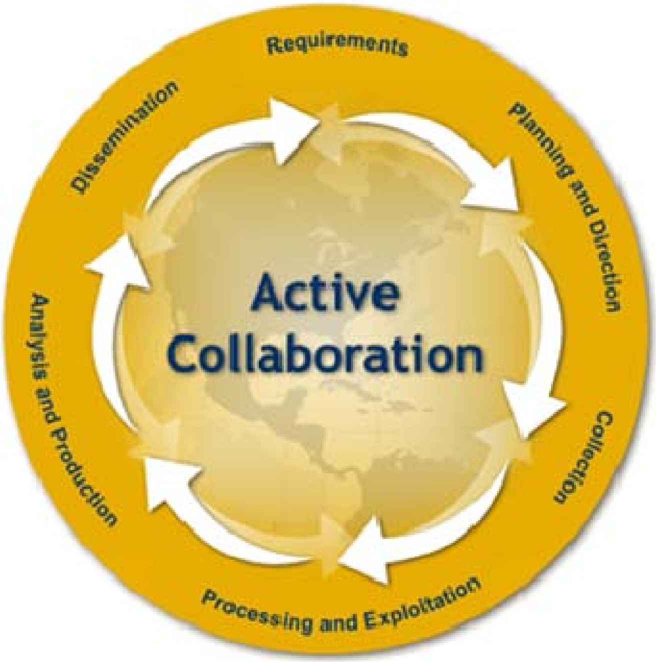

Figure 3. The Intelligence Cycle (From FBI, 2010)

C. AVIATION INTELLIGENCE

> To maximize Air Domain awareness, we must transform, and integrate capabilities that collect, analyze, and disseminate surveillance, intelligence and information to create an operational picture that is tailorable to the needs of users across the United States government, as well as at State, local, and tribal levels . . . (DHS, 2007a, p. 17)

In his February 2005 article in *The Journal of Airport and Airline Security*, aviation security author Robert T. Raffel buttresses the DHS *2007 National Strategy for Aviation Security* by suggesting that there are three primary threat assessment information sources for local aviation security managers: 1) open source information; 2) local law enforcement; and 3) classified DHS-TSA threat assessment information. Considered in their totality, these information resources provide, according to Raffel: 1) trend analysis; 2) situational awareness; and 3) vulnerability/risk-assessment capabilities. However, while open source information and local law enforcement resources may be beneficial for supplemental informational purposes, the focus of this thesis chapter is centered upon the importance of local dissemination of national threat assessment information that is collected, processed and analyzed at the federal level. This is because the U.S. Intelligence Community receives information from global resources that are critical to all segments of the NAD as identified by Raffel's elements of analysis, awareness, and assessment from a much broader perspective. As such, if threat assessment information were shared more regularly with local security partners, then pragmatic changes and supplements to any one particular airport's security plan may be augmented accordingly, thus providing a more tailored, more proactive approach to aviation security nation-wide. Otherwise while adjustments to a regional airport's security posture may be made based upon locally-generated information, a potentially serious gap may occur if international and national resources are not collated and disseminated by the U.S. federal government. In conclusion, the potential viability of an aviation security program is contingent upon two indispensible elements: 1) the accurate and efficient use of anti-terrorism resources as suggested by the trends, tactics and procedures identified in USIC intelligence products as well as locally-generated intelligence information; and 2) the acquisition and deployment of those resources against pre-identified risks as indicated by a comprehensive ATVRA.

Figure 4 demonstrates the flow and potential usefulness of intelligence products within the air domain at the local level. Flowing from the right to left in the graph below, Raffel notes that open source information, threat assessment information from the TSA and local law enforcement may all flow through the airport security operator and ultimately produce meaningful results for improving an overall state of aviation security, to wit: 1) trend analysis; 2) situational awareness; and 3) vulnerability and risk assessment information. The practical field application of threat assessment and vulnerability/risk assessment information is outlined in more detail in the next chapter regarding risk management methodologies.

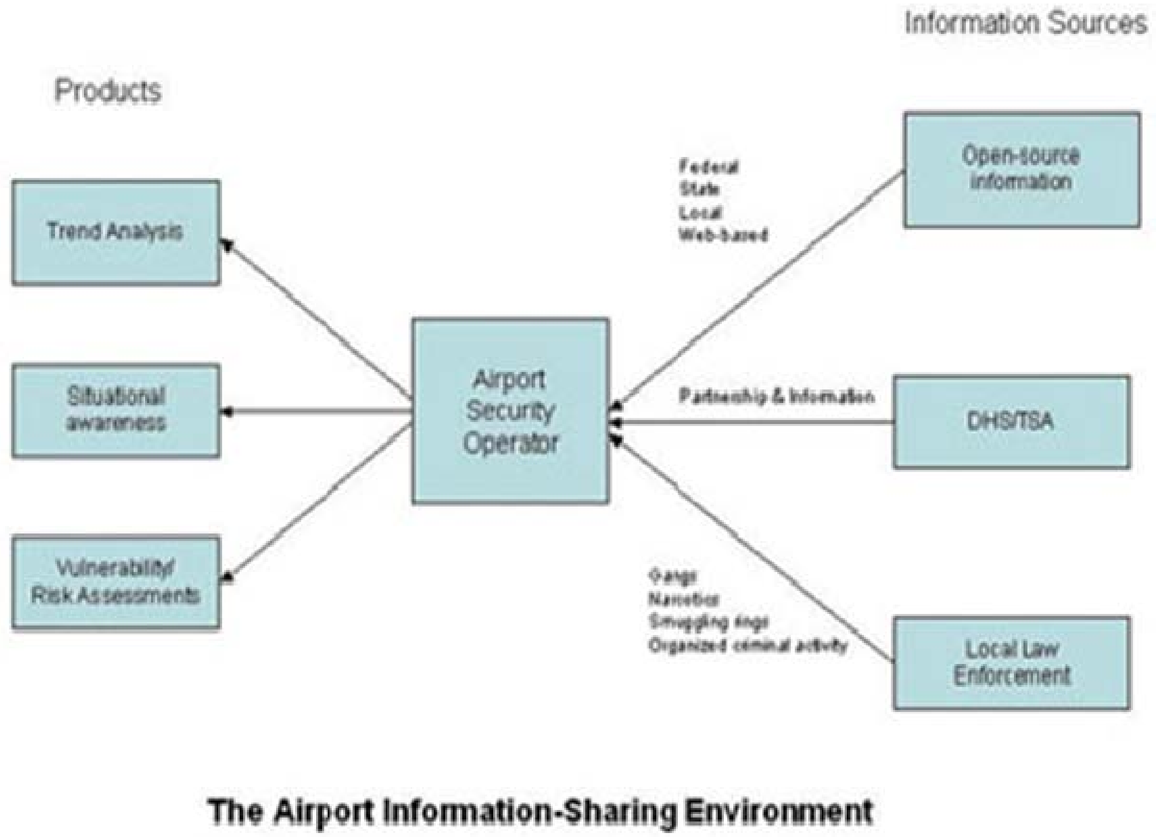

Figure 4. The Airport Information Sharing Environment (From Raffel, 2007)

D. AVIATION INTELLIGENCE AND STRATEGIC PLANNING

How does intelligence-based threat assessment information actually inform and influence operational decision-making within the National Aeronautical Domain?

While the nature of, and need for, intelligence-based threat assessment information within the aviation domain may not be dissimilar from that which is necessary in other critical infrastructure domains, such as in the rail and maritime industries, the commercial aviation environment is unique in many ways. First, as outlined in Chapter II of this thesis, the repeated attempts of terrorist operatives to penetrate attacks within the NAD remains evident. As a known high-value target environment, then, both the criticality and utility of efficiently, effectively and consistently sharing threat assessment information across the full spectrum of aviation security organizations at the local and federal levels is made apparent.

The focus of our adversaries on air transportation is explained, at least in part, by the potential lethality of an another attack within the NAD in terms of the high number of human causalities that could reasonably be expected, as well as by the tremendous overall negative impact upon the U.S. economy if successfully executed. Second, although most transportation centers share the commonality of condensing large concentrations of people together in one location, the air domain presents a particularly enticing target environment for terrorist organizations. This is especially true because transient populations within these centers remain extremely high during normal hours of operation, which accounts for about 16 hours out of a day, seven days per week, year around. Third, in order to accommodate large transient populations, particularly at Category X aviation facilities, a perpetual state of major construction is typically seen at airport facilities across the nation. Therefore, since airports represent a unique, dynamic and ever-changing physical environment with large numbers of people typically present—and is a threat environment that continues to be the focal point of our nation's enemies—a consistent flow of threat assessment information is necessary for security operators so that protective plans may be updated as necessary. For these reasons, this is true perhaps even more so in the aviation environment than in either the rail or maritime sectors noted hereinabove.

Accordingly, the immediate, mid- and long-term development of strategic security plans—inclusive of operational/maintenance budgets and field plans, capital infrastructure development and protection, and security policy development—may be greatly informed by the use of threat assessment information. This is true in three distinct areas of aviation security, specifically:

1. In planning new facilities;
2. In planning the expansion and reconfiguration of existing facilities; and,
3. In managing an active operational security plan for an existing facility that is currently occupied and in use.

For instance, in the aviation domain where large capital building projects are oftentimes programmed and planned several years prior to construction and utilization, security managers could provide more meaningful input into the security design phase of a project by better understanding emerging terrorist trends, tactics, techniques, and procedures. In these cases, if threat assessment information were available that identified certain emerging threat patterns, tactics and techniques, then the original design of a facility could be constructed to diminish exposure to those threat vectors. Through and by utilization of a crime prevention concept known as "crime prevention through environmental design (CPTED), perimeters, for example, could be protected by decorative ponds, manmade streams, the placement of trees, etc. as effective barriers to from a point critical to protect; parking lots and curbsides that could be chosen as ideal points for the detonation of explosive devices could be strategically placed to mitigate those weaknesses by increasing stand-off distances, and terminal buildings could be constructed out of less glass to diminish the effects of sharding[34] at areas vulnerable to improvised explosive attacks, load bearing walls and beams could be reinforced to withstand the impact of certain levels of bomb blast overpressures.

Similarly, in retrofitting the physical configuration of an existing aviation facility, for example a terminal building built in the 1960s, at a time in history when bomb incident prevention plans were not yet required for most domestic buildings in the U.S., an aviation security manager could be more effective. For example, an appropriately informed security manager informed by threat assessment information may "harden"[35] an existing facility against attack, or otherwise make more informed decisions regarding the acquisition and deployment of physical and human countermeasures in order to layer the protective resources throughout a high-value target and area. Moreover, threat assessment information may be of great utility for determining the type, quantity and placement of

[34] "Sharding" is a term commonly used to refer to pieces of glass, steel, and concrete, among other materials, that have been broken apart into small fragments and propelled forcibly through the air by the overpressures created by a bomb blast. In this context, in addition to the physical trauma potentially imparted to human beings as a proximate result of bomb blast overpressures, "shards" of material represent the very dangerous secondary consequences of a bomb blast to humans when detonated adjacent to physical a structure. This is similar to shrapnel propelled from a detonated grenade, for example.

[35] In this context, "harden" means to reinforce against the vulnerability to attack or otherwise diminish the ultimate consequences of the same.

anti-terrorism countermeasures, such as bollards, fencing materials, the implementation of technology as guard force multipliers, and so on. Suffice to say, then, threat assessment information is absolutely critical if one is to make informed decisions regarding the acquisition and implementation of physical countermeasures, technology and policy development for guard force operations.

As argued above, the notion of incorporating strategic, risk-based planning into local aviation security programs is even more critical in a post-9/11 environment where U.S. commercial aviation assets are still considered high-value targets. Moreover, while strategic planning based upon threat assessment information is necessary in order to more efficiently acquire and deploy an aviation security organization's resources on an ad-hoc basis as threat information is received, another fundamental element of the security planning process is necessarily coupled with the risk assessment process of the facility to be guarded, which is more of long-term approach to security planning and budgeting.

More specifically, in developing and managing an effective aviation security program, beyond deploying security resources in a totally random and potentially ineffective piecemeal fashion, a comprehensive asset, threat, vulnerability and risk-analysis (ATVRA) of the facility to be protected should be conducted utilizing a standardized risk assessment methodology—one that should be identified by DHS and implemented throughout U.S. aviation. Simply stated, in order to better explain how intelligence-based threat assessment information may help solve problems relative to threats within the aviation domain, in conjunction with intelligence-based threat assessment information, the use of a comprehensive ATVRA aides in the following topic areas to reduce overall contingent risk. The following is an example of how and why threat assessment information must be incorporated in risk-based planning to improve the U.S. aviation domain's overall security posture:

Given any Category X aviation facility in the U.S., the designated local security manager should utilize a standardized process to complete the following tasks:

1. Identify all assets necessary to ensure a continuity of business operations so that security managers know specifically what may need to be protected. Examples may include, but are not limited to: terminal

buildings, roadway systems, runways, and support facilities, such as central plants. Other critical on-site infrastructure may include such topic areas such as: electrical, water, natural gas, and aviation fuel pipelines and supply feeds.

2. Through a review of all available intelligence-based threat assessment information, security managers possess a situational awareness of the potential threat streams against which a facility should be defended. Consider, as an example only, if threat assessment information were received that indicates al-Qaeda possesses a long-term interest in exploiting the fuel farms and supply lines to an airport storage facility's 10-million gallon reserve of highly volatile jet fuel (Jet-A). The security manager would: a) identify this fuel storage facility as a critical asset, and b) know and understand that it constitutes a potential target for terrorist operatives;

3. By conducting a review and comparison of all assets as well all the known/suspected quantum of threats that may be directed toward a Category X aviation facility, security managers may make more informed decision which threats may be most likely to be target, and thus understand what the vulnerability/likelihood of occurrence is for the types of attacks/hazards. Take for example again the fuel storage facility scenario referenced above, the security manager may also be informed now as to the potential capabilities, tactics, techniques, and procedures that may be employed by al-Qaeda. Understanding this perspective, to the extent available anyway, then facilitates a security manager's understanding as to: a) the priority to which the fuel the storage system should be ranked on a security projects list, and b) providing some insight as to which types of countermeasures must be acquired and deployed to best defend the target area;

4. The overall risk to the facility studied is then better understood because the contingent, real, or residual risk is identified after the less likely threats/attack scenarios are eliminated from the threat picture. As such, a relative weight may then be assigned to each vulnerability mitigated to determine the amount of overall risk reduction achieved with any given countermeasure deployed;

5. Once contingent risk is identified from the most probable, specific threats considered, then protective resources/countermeasures may be designed, developed, implemented, or otherwise acquired to mitigate the known contingent risk based upon the efficacy of each measure instituted as described hereinabove.

Accordingly, threat assessment information utilized in the completion of an ATVRA allows site-specific vulnerabilities to be identified and subsequently addressed with a tailored approach for aviation facilities dependent upon the physical, environmental, financial, and human resources available to each facility’s security manager. The critical element of intentionally coupling threat assessment information with the ATVRA process into the aviation security planning program will be considered in detail in Chapter IV of this thesis.

The critical point emphasized and demonstrated in this segment of this research project, however, is the vital role that intelligence-based threat assessment information should play in the protection of U.S. aviation airport facilities. Currently, the process identified hereinabove has not been institutionalized by the DHS-TSA across the aeronautical domain, thus leaving U.S. commercial aviation more vulnerable to exploitation and attack than is necessary and reasonable, despite DHS-TSA’s stated intent to approach U.S. aviation security in a collaborative, layered and intelligence-led manner.

E. INTELLIGENCE RESPONSIBILITIES WITHIN THE AERONAUTICAL DOMAIN

> Ultimately, the backbone of protecting the United States from threats in the Air Domain is an active, layered security and defense. Air Domain awareness, achieved through persistent situational knowledge provided to operational decision-makers, is a critical enabler in achieving this capability. (DHS, 2007a, p. 5)

As alluded to in the *Air Domain and Intelligence Integration Plan* cited above, the potential success of an effective anti-terrorism plan is contingent upon thwarting the element of strategic surprise enjoyed by an adversary (DHS, 2007a, p. 5). In fact, Johnson and Wirtz (2008) state that “providing warning against surprise is central to both official and public perceptions of the fundamental role of intelligence services” (pp. 28–29). Accordingly, if the element of surprise is mitigated, an attack may either be frustrated by the deployment of effective countermeasures, or at least the ultimate consequences of the attack may be altogether diminished to a reasonable level.

As referenced in Chapters I and II of this thesis, the USIC member legally responsible for providing threat assessment information to local aviation security managers is the TSA Office of Intelligence and Warning. Facilitating the dissemination of classified and restricted materials is oftentimes impeded, however, due to two issues:

1) technological constraints; and 2) a lack of trained intelligence analysts deployed forward across the aeronautical domain and attached to TSA field offices to advise and brief Category X security practitioners at the local level. More specifically, relative to technology, local security managers are oftentimes unable to procure classified/law enforcement sensitive intelligence products that may supplement the quantum of knowledge available from open sources materials because the necessary equipment to legally and securely transmit and or receive classified and law enforcement sensitive intelligence products has not been acquired by the local security manager.[36]

This is not to suggest that when exigent circumstances exist emergency provisions could not be made by the "owner"[37] of the information to convey critical details. But for the local aviation security manager in the day-to-day planning and future deployment of protective resources based upon an intelligence-led/risk-based model security model, the continuous flow of open source, law enforcement sensitive, and classified information is necessary in order to maintain a broad-based situational knowledge of terrorist events and trends within the air domain. To that end, local aviation security managers, as operational decision-makers, should give serious consideration to acquiring secure communications equipment, with the sponsorship of the local TSA field office, for both emergency as well as routine planning and operational use. As such, local security managers should recognize that they possess an affirmative duty to work with their local TSA field offices in acquiring not only classified security clearances and access to intelligence networks such as the DHS's Homeland Secure Data Network,[38] but secure telephones and facsimile equipment as well, in order to facilitate the timely and lawful transmission of threat assessment information from the broader USIC.

[36] Note, however, that the acquisition of a secure telephone to transmit SECRET level information, commonly referred to as a Secure Terminal Unit (STU Phone) is a National Security Agency regulated product, and as such, the local security operator must have a DHS-TSA sponsor to acquire such technology. Accordingly, this type of technology may not unilaterally be purchased by a unit local government.

[37] The term "owner" of classified threat assessment information is a reference to the individual or agency from which the information originates, by whom the subsequent dissemination of which is oftentimes controlled, or restricted.

[38] According to GAO Report 04-375, the Homeland Secure Data Network is administered by DHS and is intended to be the technological means by which the federal government shares sensitive and classified homeland security information with state and local partners (GAO, 2004b, p. 50).

The second impediment, related specifically to the lack of trained intelligence personnel deployed forward in the field to advise and brief local security managers regarding intelligence-based threat assessment information, continues to be problematic regarding the dissemination/sharing of intelligence information across the domain. Simply put, for whatever internal reasons that may exist, DHS-TSA simply has not made intelligence analysts available to, and actively engaged with, local aviation security mangers across the U.S. This fact is buttressed by the survey heretofore referenced in Chapter I of this thesis, wherein 19 of the U.S.'s 27 Category X airport security managers opined that DHS-TSA had not achieved success in this topic area. Moreover, what is confounding about this persistent problem, is that the DHS, and vicariously the TSA, is a designated member of the USIC and is the legally responsible party for disseminating intelligence information across the aeronautical domain to local stakeholders.[39] The TSA possesses the legal authority to sponsor federal security clearances for local security managers; and finally, many local security counterparts wish to buttress their security operations with input from the intelligence community providing general guidance, hence the repeated calls for more intelligence sharing from many domains—inclusive of many outside of aviation—in conjunction with the similar findings of the U.S. 9/11 Commission. But, again, despite DHS-TSA's legal authority and responsibility in this matter, as well as the aviation community's repeated requests for intelligence-based threat assessment information, positive results have not been forthcoming.

Intentionally deviating from the USIC and DHS-TSA information-sharing problems discussed herein, in a bottoms-up intelligence collection strategy for regional aviation security operators, local security managers may also help ensure the protection of facilities by acquiring technologies related to intelligence information generated at the operational level. This is particularly true in situations at the local level where the execution of an attack scenario may be commenced, having gone previously undetected and pre-empted by intelligence and law enforcement entities outside of the air domain. In

[39] Recall, for example, that the topic of legal responsibility for sharing intelligence information across the aeronautical domain rests with the TSA. See Chapter I and II for a review of this discussion and the legal references pertaining to this subject area.

these cases, in addition to human detection and intervention of an attack, technology may serve as a force multiplier by adding additional layers of defense by forewarning airport security organizations of approaching dangers.

In this regard, local security operators may develop and deploy trip wires,[40] even virtual trip wires, around their most sensitive facilities in order to develop local indication and warning systems at the field level of operation. For example, license plate reader technology deployed along a local roadway may provide early warning of a pre-identified motor vehicle-borne threat travelling inbound toward an airport facility. Similarly, closed captioned television units placed strategically throughout an airport complex may provide situational awareness of the perimeter, as well as the internal and external environs of the terminal complex. Moreover, a combination of technologies integrated together may provide an even more robust, defense-in-depth/layered security posture for U.S. aviation facilities.

A more detailed discussion of the specific technological components noted above is beyond the scope of this research project, but they are nonetheless mentioned herein for three principal reasons:

1. To prompt the local aviation security manager to think about and consider their own responsibilities in regard to acquiring proprietary systems related to the generation of their own operational intelligence—and not simply relying totally upon the DHS-TSA to presumably provide all that is necessary relative to site protection intelligence; and
2. To draw a distinction between operational intelligence for indications and warnings at the local level and the real impetus of this chapter, which is to define and outline the structure and practical uses of USIC, DHS-TSA intelligence-based threat assessment information in the aeronautical domain; and
3. In addition to human sources of intelligence developed at the local level, to understand that from a bottoms-up approach to the nation's aviation security posture that the types of technological systems referenced herein may also provide opportunities, and indeed responsibilities upon local security operators, to collect—within the boundaries of the U.S.

[40] A "tripwire" is a wire or line that activates a weapon, trap, or camera, for example, when pulled (The Free Dictionary, 2010).While human intelligence sources may also be utilized as trip wires, in the context used here the reference relates to a technological collection platform that may serve as force multiplier in the early warning process in the event of an immediate threat to an aviation facility.

> Constitution—certain types of information from these system and pass the same upstream to the USIC via the DHS-TSA.

F. CHAPTER SUMMARY

This chapter has defined the term "intelligence," in the normal usage and context of the U.S. Intelligence Community, as information that has been collected, analyzed, processed, and disseminated for a particular requirement as determined necessary by a U.S. policy-maker. This chapter also discussed the U.S. intelligence process through and by use of the intelligence cycle. Most importantly, this chapter identified and explained in great detail the critical nature of threat assessment information within the aeronautical domain and the manner in which intelligence-based threat assessment information may be used to better protect the U.S. National Aeronautical Domain through the preparation, budgeting, and planning processes relative to the aviation security industry.

With this introduction into intelligence completed, detailed discussions regarding the formal role of intelligence into both the formal risk-assessment process and introduction of the intelligence-led policing concept within U.S. commercial aviation may now be conducted.

IV. RISK MANAGEMENT

> Almost every aspect of infrastructure protection is sorely lacking in foundational theory, scientific proof of effectiveness, and applied tools and techniques. Indeed, the very basic task of identifying what is critical, and measuring its vulnerability, is currently inadequate and poorly understood by the people whose responsibility is to implement the national strategy. (Lewis, 2006, p.60)

A. INTRODUCTION

> ***In addition to the receipt and dissemination of intelligence-based threat assessments and information, why is the discipline of risk management a necessary component in the strategic planning process for both the federal government and local aviation security managers?***

From the national government's perspective, the impetus to develop a strategy to protect the U.S. homeland's critical infrastructure predates the publication of the 2003 *National Strategy for the Physical Protection of Critical Infrastructures and Key Assets* and the 9/11 tragedy. This is evidenced by President Clinton's 1994 order, pursuant to *Presidential Decision Directive-29*, for the federal government to develop and implement a coherent risk assessment methodology for the U.S. in a post-Cold War period. In 1998, recognizing that ". . . future enemies whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States," President Clinton again addressed the issue of critical infrastructure protection by signing *Presidential Decision Directive-63*, which purpose was to "propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes . . . to develop security-related best practice standards" (White House, 1998). After the events of 9/11, the 9/11 Commission also issued a recommendation on the topic of risk management by acknowledging that "in a free-for-all over money [for the acquisition of homeland security assets] . . . resources must be allocated according to vulnerabilities" (2004, p. 396).

Furthermore, from a national viewpoint, the *Homeland Security Act of 2002* created the DHS and charged the department with, among other duties, a mandate to identify a system by which to identify and prioritize U.S. critical infrastructure assets and subsequently develop plans for each sector's protection. From this directive emanated the *National Infrastructure Protection Plan* (hereafter the "NIPP"), which includes by reference the *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan* (DHS, 2007c).

Unfortunately, however, none of these plans serve to inform the local aviation security manager specifically that risk assessment methodology (RAM) should be utilized in the risk management process within the air domain. In fact, there is still no one risk assessment methodology standard that has been instituted by DHS, despite President George Bush's subsequent 2003 requirements for a comprehensive risk management approach for critical infrastructure protection pursuant to *Homeland Security Presidential Directive -7* (HSPD-7), with the U.S. aviation domain being no exception to this rule.

This wicked problem[41] plagues the federal government from both an operational and resource allocation perspective, and equally afflicts the local security manager in strategic budgeting and operational planning. Lewis (2006) corroborates this point by noting, "Currently there is no standard; hence, it is impossible to compare vulnerabilities across jurisdictions or sectors. And yet DHS requires vulnerability analysis" (p. 7).

From a local aviation security managers' position, the practical or operational aspects of this problem are driven home by the repeated attempts of adversaries to exploit aviation assets in the United States. For example, on August 13, 2006 Secretary of Homeland Security Michael Chertoff ordered the NAD to elevate the security posture of the entire civil aviation infrastructure to DHS Level ORANGE contingency conditions

[41] According to Dr. Jeff Conklin, a "wicked problem" has four defining characteristics: 1) the problem is not fully understood until after the formulation of a solution; 2) stakeholders have radically different world views and different frames for understanding the problem; 3) constraints and resources to solve the problem change over time; and 4) the problem is never solved (Word IQ, 2010).

(Chertoff, August 13, 2006).[42] This order continues in effect at the time of this writing (August 2010), which serves to affirm a reasonable supposition that terrorists still consider U.S. civil aviation assets/facilities targets of high interest. As such, the efficient and effective management of aviation sector anti-terrorism countermeasures/security programs continues to be vitally important in order to mitigate risk. But before risks can be effectively reduced, local aviation security managers must know and understand specifically, or at least generally to the degree that threat assessment information may provide, which particular assets are at the greatest vulnerability of attack and need to be protected. The only way to determine vulnerability and contingent risk, then, is to conduct a comprehensive risk assessment and subsequently devise a risk management program to address identified weaknesses. This type of a security survey is especially important in large, public use aviation facilities.[43]

Moreover, unlike military air bases that may either close or otherwise choose to funnel the ingress of people and materiel to certain checkpoints points for inspection prior to entry during periods of heightened threat, U.S. civil aviation facilities may not typically restrict access in the same manner. To the contrary, a vast majority of U.S. civil aviation facilities are open and are in fact designed to facilitate ease of ingress/egress to public areas. Additionally, U.S. Category X airport facilities provide not only for the movement of people and commerce across the nation and world, but also act as power economic engines for the geographical regions in which they serve[44].

With limitations on security spending an inevitable business necessity in order to maintain financial solvency, as is true in most critical infrastructure sectors, the efficient

[42] DHS defines Level ORANGE as a "HIGH Risk of Terrorist Attacks" (DHS, 2010). Moreover, DHS Threat Level ORANGE imposes many additional aviation security requirements upon airport security operators during heightened periods of alert. For example, increased security visibility, screening, internal audits and the deployment of physical countermeasures are required for a commercial airport facility to remain in DHS-TSA regulatory compliance, all of which strain financial, physical and human resources.

[43] This is because Category X aviation facilities conduct hundreds of daily flight operations, employ thousands of workers at each location who have access to aircraft, and move millions of passengers every year. As such, these facilities are very large, very busy transportation centers and are inherently vulnerable to criminal exploitation/attack.

[44] Consider, for example, that the 2003 Economic Impact Study for the Houston Airport System's three airports in Houston, Texas reportedly supports over 151,000 jobs in the Houston metropolitan area and contributes approximately $24 billion annually to the local economy (Houston Airport System, 2010).

utilization of security resources,[45] then, becomes a matter of strict prioritization based upon the specific airport's contingent risks vis-à-vis its assets, threats and vulnerabilities—all of which are subject to change based upon the intent, adaptability and capabilities of adversaries. Lewis (2006) acknowledges the vital importance of critical infrastructure protection and risk management, and its inextricable nexus to threat assessment information, by stating that "the lack of information sharing causes inefficiencies and vulnerabilities in the war against terrorism," and that the struggle to secure our nation's critical infrastructure against today's ideologically driven adversaries ". . . is particularly vulnerable to asymmetric[46] attacks" (pp. 49–50).

B. THE CONCEPT OF RISK MANAGEMENT AND ANALYSIS

GAO report 02-150T defines risk management as "a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions to reduce risk and mitigate the consequences of an attack" (2001, p. 3). While security experts generally agree that there is no 100 percent guarantee that all threats to a facility can be completely mitigated, Jenkins (1998) notes that the process of risk analysis is a means by which to identify organizational threats and vulnerabilities and "identifies the probable consequences or risks associated with the vulnerabilities and provides the basis for establishing a cost-effective security program" (p. 1). Furthermore, Jenkins (1998) reveals that the process of risk management "implement[s] and maintain[s] countermeasures that reduce the effects of risk to an acceptable level" (p. 1). Finally, when considering the various elements of threat analysis, security practitioners should be mindful to consider both manmade as well as natural threats to infrastructure, the latter of which relates to weather events such as hurricanes, tornadoes, earthquakes, and any other type of unwanted event that may compromise the operational functionality of a particular site to be protected.

[45] "Security resources" include, but are not limited to: people, technology, machinery, physical infrastructure, etc.

[46] Lewis defines asymmetric warfare as "the art of force multiplication using nontraditional techniques such as converting jumbo jets into bombs, using the public broadcast media to spread propaganda and gain public support for a cause, and creating terror and mass destruction or economic disaster through forced attacks on infrastructure that millions of people depend on" (2006, p. 18).

Yacov Haimes outlines the risk assessment process in his June 2002 article in the *Journal of Infrastructure Systems*. With respect to the assessment function, according to Haimes, the security professional must attempt to answer the following three questions in order to begin to understand risk in any given environment: 1) what can go wrong? 2) what is the likelihood that it could go wrong? and 3) what are the consequences? Similarly, Sandia National Laboratory's Risk Assessment Program represents the components of risk as: threat (likelihood of attack), consequence of adversary success, and likelihood of adversary success (protection system effectiveness). Intelligence-based threat assessments would be of great utility to the security practitioner at this phase of the risk assessment process because they may serve to better inform the assessors of: 1) The likelihood of attack based upon the suspected motives of an adversary; and 2) The likelihood of a successful attack based upon the suspected capabilities of an adversary.

The aforementioned elements of the risk assessment process are represented in Figure 5.

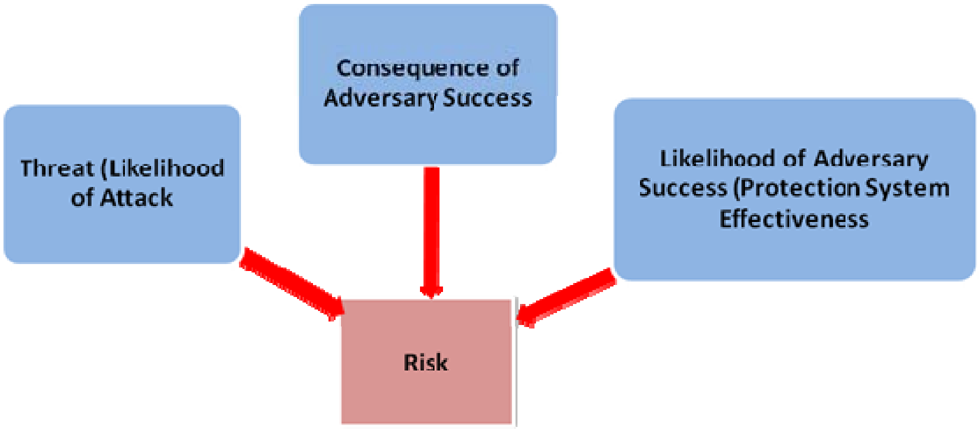
Consequence of Adversary Success
Threat (Likelihood of Attack
Likelihood of Adversary Success (Protection System Effectiveness
Risk

Figure 5. Components of Risk (From Sandia National Laboratories, 2009)

Once the questions relative to assessment are answered, Haimes (2002) asserts that the risk management process may be formulated by asking three additional questions, namely:

1. What can be done and what options are available?
2. What are the trade-offs in terms of all costs, benefits, and risks?
3. What are the impacts of current management decisions on future options?

In GAO report 07-386T (GAO, 2007), the federal government divides the process of risk management into five distinct phases:

1. Setting strategic goals and objectives while determining constraints;
2. Assessing the risks;
3. Evaluating the alternatives for addressing these risks;
4. Selecting the appropriate alternatives; and
5. Implementing the alternatives and monitoring the progress made and the results achieved. In weighing costs and benefits to manage risk.

However, Lewis (2006, p. 103) submits that the "80:20% rule"[47] should also be applied, meaning simply that since financial resources to protect everything cannot typically be appropriated, as a rule of thumb, 80 percent of financial resources should be spent on roughly 20 percent of the most sensitive components of a critical infrastructure site that are identified by the formal risk assessment process.

Finally, in a March 2008 article published in the *Journal of Homeland Security*, Pat Jones and Yolanda Edmunds summarize the U.S. Navy's concept of risk analysis and management for naval facilities in the following steps:

1. Identify the broad set of attack types that could occur at Navy installations;
2. Review current Navy intelligence information to differentiate the likelihood of each type of attack;
3. Define the role of the functional capability set in preventing or mitigating each attack type;
4. Define levels of capability set implementation and performance;
5. Fuse threat, vulnerability, and criticality information to develop an overall risk characterization;

[47] The "80–20 rule" cited by Lewis (2006) may also be known as the "Pareto Theory." Developed by Italian economist Vilfredo Pareto in 1906, the theory may be extrapolated by security practitioners, as Lewis suggests, as a reminder to focus on the 20 percent of business activities or critical infrastructure most vital to a particular operation—in this case, commercial aviation security operations at Category X airport facilities (About.com, 2010).

6. Generate risk-based measures of effectiveness and cost measures for each functional capability set.

Similar to the Sandia National Laboratories risk assessment methodology (Sandia National Laboratories, 2009), Jones and Edmunds (2008) express the above-referenced steps as a linear equation, such that: **risk = threat x vulnerability x criticality [consequence]**.

C. RISK MANAGEMENT METHODOLOGIES

In his remarks delivered to the DHS Grants and Training National Conference in 2006, DHS Secretary Michael Chertoff stated, "We have to have a common approach, a coordinated approach across all phases of what we have to do to create homeland security" (Chertoff, 2006). Similarly, Baker (2005) declares, " To understand and correct exploitable susceptibilities of critical infrastructure facilities, infrastructure providers and regional planners need a common, repeatable, systematic methodology to understand the comparative risks and vulnerabilities and determine where to invest scare resources" (p. 1). Yet, despite the requirements of HSDP-7 to develop a consistent risk assessment methodology, along with the similar requirements of the NIPP, the latter of which only generally describes the risk assessment process, no one particular risk assessment methodology has been adopted by DHS for the aviation sector.

The fact that a common risk assessment methodology has yet to be identified and utilized within the aviation domain is not due to a lack of options. To be certain, a plethora of RAMs exist within the homeland security arena. As two examples, the U.S. military has utilized both the criticality, accessibility, recoverability, vulnerability, effect, and recognizability methodology (CARVER), as well as the mission, symbolism, history, accessibility, recognizability, population, and proximity methodology (MSHARPP) offensive target prioritization tools for many years. Both of these methodologies assist warfighters in identifying the attractiveness of potential battlefield targets, but again are offensive target prioritization tools for military planners. As such, while assessing a target's relative value may be useful for a security manger in determining which sites or facilities should be given first priority in the strategic planning process, at least from an adversary's perspective, these particular tools do little to aid in the risk assessment process from a defensive standpoint.[48]

Likewise, Sandia National Laboratories has developed various RAMs for U.S. critical infrastructure and key resources, to include assessment methodologies for: energy, water, and chemical facilities. The U.S. Coast Guard has adopted the maritime security risk assessment model (MSRAM) for use at our nation's seaports, but none of these methodologies have been adapted for use, and subsequently endorsed by TSA, for airport security operators whose task is to protect the physical infrastructure of U.S. civil aviation facilities.

In an attempt to address the RAM void within the aviation domain, however, the TSA's Aviation Security Impact Assessment Working Group has been field testing the U.S. Commercial Aviation Partnership's (USCAP) risk management assessment tool (RMAT). USCAP refers to this tool as an "econometric tool," meaning simply that it attempts to quantify the economic impact of proposed security measures within the aviation domain. However, according to Massachusetts Institute of Technology professor R. John Hansman in his 2006 remarks concerning RMAT's nomination for the Franz Edelman Award,[49] the tool ". . . does not include a threat mitigation analysis component (e.g., the benefit in a classical cost benefit [analysis])." As such, the RMAT simply endeavors to calculate the potential costs of security policies and procedures within the aviation domain (e.g., [fluctuation of] ticket prices, passenger enplanement numbers, etc.), but does not inform the security manager what the anticipated return on a particular security investment will be after deployment. Additionally, there is no evidence that RMAT does anything to identify assets, threats, or non-economic[50] risks and

[48] In this context, "defensive standpoint" questions, for example, who may attempt to attack a facility? How might they achieve a successful attack? What is the likelihood of the attack's success? What potential impact will an attack have on facility's operational functionality? And finally, what, if anything, can be done mitigate both the opportunity and or consequences of an attack?

[49] The Franz Edelman Award is an annual competition given for "the discipline of applying advanced methods to help make better decisions" (Operations Research: The Science of Better®, 2010).

[50] While most risk management strategies involve some level of economic consideration because of a potential for business interruption, what is meant here by "non-economic risks" is simply a juxtaposition between the financial and physical consequences of an attack.

vulnerabilities. There is, however, one particular asset-based RAM that does assess the overall security and operational risks of commercial aviation facilities that may, if formally adopted by DHS, provide consistent, repeatable and sustained results across the nation.

Alea Holdings, LLC. in Dallas, Texas has developed a RAM referred to as INTELOS Airport (INTELOS)[51] (Alea Holdings, L.L.C., 2010). This RAM software package utilizes a series of proprietary algorithms to assess and calculate the overall security, engineering, operational, and country risks for global aviation infrastructure assets. As such, the calculated outputs of this program include numerical, linguistic, and color coded reports related to:

1. A standardized overall risk grade for the facility assessed, inclusive of the protective elements currently deployed as countermeasures for the assets protected;
2. Specific recommendations to improve security as related to costing;
3. Specific budget allocation recommendations; and
4. Relates financial risk to a standardized grading system for use in budget presentations.

Finally, as an additional benefit, the INTELOS program utilizes and produces CARVER offensive targeting data as an alternative means of assessing the relative value an adversary may assign to various components of any given aviation facility, which, as previously noted herein, is valuable supplemental information for consideration and use by the aviation security manager in balancing and expending scare resources.

D. CONCLUSION

Managing risk is a fundamental element in adequately securing the U.S. National Aeronautical System from future attack. The first step in accomplishing this task begins

[51] In the interests of full disclosure, this researcher's employer, the Houston Airport System (HAS), and its subsidiary, the HAS Development Corporation, participated in the initial development of this RAM product by providing subject matter expertise and airport data to Alea Holdings, LLC. However, the INTELOS Airport program was developed, and is wholly owned and controlled, by Alea Holdings, LLC. Likewise, since this software is owned by a private-sector company, this author has no means by which to validate the algorithms utilized in the program; however, the preliminary results of the Intellos tool in Houston has provided promising results by yielding detailed information regarding the Houston Airport System's current security posture, security infrastructure and security budgeting requirements.

with DHS and its responsibility to adopt a standardized RAM within the aviation domain. By doing so, regardless of the RAM ultimately adopted by DHS, several specific benefits related to aviation security should be realized.

First, the adoption of one of the aviation RAM will provide a common base or understanding of threat assessment within the industry and allow regional security partners at the local and federal levels to evaluate threats, vulnerabilities, and contingent risks with a high degree of repeatability and relative accuracy—nationwide—so that effective security risk management plans may then be executed. Second, the unique strengths and vulnerabilities of particular airport facilities, once identified, may then be addressed with a tailored approach at each of the nation's airports dependent upon the physical, environmental, financial, and human resources available to each facility. Third, the federal government may then appropriate security funding on a more equitable and consistent basis across the nation's airport authorities. Fourth, the inevitable variations in the type, amount and frequency of the countermeasures deployed at each individual airport facility should result in a more random and unpredictable threat mitigation strategy across the nation, thus potentially forcing adversaries to either abandon a particular plan—such as in a multiple, simultaneous coordinated attack scenario—or otherwise expend appreciably more time and resources conducting pre-attack surveillance.[52] In short, at the very least, delaying an adversary's attack plan will provide security and law enforcement groups a greater opportunity to identify the plot prior to the execution of an actual attack. And finally, fifth, the financial and logistical burden to the U.S. government of providing one specific RAM to Category X airports across the nation, inclusive of the necessary training to teach the appropriate use of the RAM, would be minimal. This is true particularly given the enormous projected return on this investment in terms of increased security across the air domain, and ultimately, for the nation as a whole.

[52] The effective utilization of available resources to thwart potential attacks is related to, and consistent with, the generally accepted security philosophy of detecting, deterring, *delaying*, and denying adversaries to the NAD. As a result of delaying an attack, then, local security, intelligence resources and law enforcement will be provided with a greater opportunity (more time) to uncover and disrupt a terrorist plot prior to attack. Recall, for example, the UK's 2006 successful disruption of terrorist operatives in Operation OVERT.

E. BRIEF SUMMARY OF THESIS KEY POINTS THUS FAR

In this and the preceding chapters, this thesis has attempted to make the following points:

1. That the NAD is a vital resource to the United States for both mobility as well economic security reasons.
2. That the NAD is a large and complicated domain that terrorists still wish to attack and potentially utilize for another 9/11-style attack.
3. That intelligence-based threat assessment information is a necessary component in developing and sustaining a viable aviation security program across the nation.
4. That formalized risk assessments and risk management programs also constitute a critical component in developing and sustaining a viable aviation security program across the nation.

But the question now arises as to how all of these elements should be meshed together in an organizational and operational sense within the air domain. Chapter VI will explore this particular issue in more detail, but after Chapter V considers certain aspects of aviation security programs of other countries allied with the United States.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTERNATIONAL AVIATION SECURITY PERSPECTIVES

A. BACKGROUND

The use of commercial aircraft to perpetrate the terrorist attacks upon the United States on September 11, 2001, left not only this country, but the international aviation community as a whole, to struggle with security problems in a post-9/11 threat environment. Endeavoring to solve these problems in the United States a dialogue emerged that revealed three principal competing interests. Specifically, unrestricted by the barriers of U.S. law, politics or cost, how might a maximum level of aviation security be realized within the National Aeronautical Domain (NAD)? More to the point, the unique geopolitical circumstances of the U.S. notwithstanding, which policies, tactics and procedures currently in use by other countries might prove to be of utility if appropriately adapted within the criteria cited hereinabove?

This central question of national security interest continues to be asked almost nine years after the 9/11 tragedy. Consequently, the intent of this chapter is to discern whether or not the aviation security program of the United States may be enhanced by adopting some of the most effective techniques, tactics and procedures of three U.S.-allied countries that are also engaged in the critical work of improving the security posture of the international aviation community. Accordingly, this policy research will specifically analyze the aviation security models of the State of Israel, the Commonwealth of Australia, as well as the United Kingdom of Great Britain and Northern Ireland—all democratically administered governments—to ascertain and ultimately determine the viability of certain key elements of each government's aviation security model as they may relate to, and ultimately buttress, the current aviation security program of the United States.

Before this discussion begins, however, one may rightly question, "Why should we care what other countries do with regard to aviation security?" What is the "so what" for security practitioners, politicians and citizens alike in the U.S. to consider foreign perspectives relative to this issue? The answer is twofold.

First, as a matter of national security for the U.S., there is a practical interest in knowing whether other countries have instituted meaningful, consistent, and effective aviation security measures for those flights in-bound into the United States. Second, since this thesis considers potential security improvements to the U.S. NAD by such means as improved intelligence collection and dissemination, incorporation of a specific risk assessment methodology and enhanced security group organizational models, it may prove useful to determine if any foreign aviation security programs have already remedied any related problems. Therefore, if the U.S.-allied nations of Israel, the United Kingdom and Australia have achieved certain successes related to the same, then perhaps adaptations to these various foreign programs may add value in solving some of the ongoing security problems currently being experienced in the U.S. NAD.

B. PROBLEM

As evidenced by the U.K.'s 2006 liquid bomb threat, as well as the unsuccessful bombing of a U.S. airliner on Christmas Day in 2009,[53] the post-9/11 threat environment reveals that commercial aviation assets remain a high-value target for non-state sponsors of terrorism. However, rather than focusing on the identification and neutralization of potential actors at aviation facilities who may try to perpetrate these acts, the U.S. aviation security community continues to focus chiefly upon locating the weapons, or "things," that may represent a hazard to civil aviation assets.

C. SCOPE

The following table provides a brief overview of the commercial aviation environments of the United States, Israel, UK, and Australia.

[53] This is a reference to Delta Flight 253, a transcontinental flight from Amsterdam to Detroit, whereupon Nigerian national Umar Farouk Abdulmutallab attempted to detonate an explosive device just prior to landing in the U.S. Abdulmutallab smuggled the device on board the aircraft by concealing the explosives in the groin area of his trousers.

Table 2. Statistical and Regulatory Comparison of International Aviation Environments Surveyed

	U.S.	Israel	UK	Australia
Number of Major Airport Facilities	27	7	6	7
Annual Passenger Enplanements (in millions)	618	11.5	232	101
Regulatory Authority	Transportation Security Administration (TSA)	Israeli Airports Authority (IAA)	British Civil Aviation Authority (BAA)	Australian Civil Aviation Security Authority (CASA)

1. United States

As specifically noted in Chapter II of this thesis, and subsequently incorporated again herein by reference thereto, the U.S. NAD constitutes a very large, diverse and complicated array of primary commercial service aviation facilities. In short but relevant repetition, however, it is within this framework of the nation's commercial aviation infrastructure that the U.S. Department of Transportation (DOT), Bureau of Transportation Statistics reported a total of 618,113,048 passengers traveled on domestic flights during calendar year 2009 (DOT-Bureau of Transportation Statistics, 2010). Based upon a 365-day year, this statistic equates to approximately 1.7 million passengers per day transiting through America's primary commercial service airport complexes.

2. Israel

Israel's primary commercial service airports are managed by the national government through a public corporation known and identified as the Israel Airports Authority (IAA). This political subdivision[54] of the state was established in 1977 and exists as the legal entity by which Israel's airports are governed. Airports Council

[54] A "political subdivision" is defined as a local government created by the states to help fulfill their obligations. Political subdivisions include counties, cities, towns, villages, and special districts such as school districts, water districts, park districts, and airport districts (High Beam Research, 2010).

International[55](2010) notes that the IAA operates a total of seven airports across the country, specifically: Ben Gurion International Airport, Eilat International Airport, Haifa Airport, Herzlia Airport, Jerusalem/Atarot Airport, Rosh Mahanaim Airport, and Tel-Aviv/Sde-Dov Hoz Airport. Of these seven as noted, only two, Ben Gurion International and Eilat International Airports (ETH), provide passenger services for international travelers. Of these two international aviation facilities, Ben Gurion International Airport (TLV), located southeast of Tel Aviv and near the city of Lod, is by far the busiest Israeli aviation facility with respect to overall international passenger traffic. More particularly, the IAA database denotes that approximately 11.5 million passengers transited through TLV during calendar year 2008 (Israel Airports Authority, 2010).

3. The United Kingdom of Great Britain and Northern Ireland

Regulated by the British Civil Aviation Authority (CAA), the British Airports Authority (BAA) operates six commercial service airports in the U.K. These airport facilities are identified by BAA as: Heathrow, Stansted, Glasgow, Edinburgh, Aberdeen, and Southampton Airports; however, Heathrow, which is located in the London metropolitan area, is by far the busiest airport in the UK logging approximately 65.9 million passengers in calendar year 2009 alone (British Airports Authority, 2010). Finally, the CAA reports total U.K. passenger enplanements numbered approximately 218.126 million passengers during the same reporting period (British Civil Aviation Authority, 2010).

4. Commonwealth of Australia

Australia’s primary commercial service airports are regulated by the Australian Civil Aviation Safety Authority (CASA) along with the Australian Department of Infrastructure, Transport, Regional Development and Local Government (DOI). For aviation security matters, according to CASA, the DOI exercises sole regulatory responsibility for all security controlled airports in Australia. Similar to the airport

[55] Airports Council International is an aviation industry trade organization that represents the world’s airports in matters regarding business, safety, security, and other regulatory affairs (Airports Council International, 2010).

classification scheme of U.S. Category X airports, the CASA website also reports that the Australian government designates its large international aviation facilities as "major international" airports, of which there are seven, specifically: Adelaide, Brisbane, Cairns, Darwin, Melbourne, Perth, and Sydney (Australian Civil Aviation Safety Authority, 2010).

For calendar year 2009, the DOI reports that a total of approximately 23.4 million international passengers, or approximately 2.0 million per month, transited through Australia's major international airport complexes (Australian Department of Infrastructure, Transport, Regional Development and Regional Government, 2010). Overall, however, the DOI reports a total of approximately 101 million passengers utilized Australian commercial aviation services for the 2008–2009 reporting period, with Sydney and Melbourne Airports ranking first and second with 22.7 million passengers and 20.0 million passengers, respectively (Australian Department of Infrastructure, Transport, Regional Development and Regional Government, 2010).

D. FOREIGN SECURITY PERSPECTIVES

1. Israeli Aviation Security: Major Themes

In his 2003 *Homeland Security Studies and Analysis Institute* journal article entitled *Strategies for Countering Terrorism: Lessons from the Israeli Experience*, Dr. Jonathan B. Tucker, a senior fellow at the U.S. Institute of Peace in Washington, D.C., identifies the five basic principles of Israeli counterterrorism strategy, specifically:

1. Intelligence collection and analysis;
2. Military and paramilitary operations to disrupt terrorist infrastructure;
3. Commercial aviation security;
4. Defense against chemical and biological agents; and,
5. Efforts to strengthen the psychological endurance of the civilian population. (p. 2)

All five of these elements possess general utility within the international aviation security sphere; however, the fundamental Israeli perspectives on intelligence collection and analysis, as well as commercial aviation security, retain particular relevance for U.S. aviation security practitioners.

This is particularly true since Israeli counterterrorism strategy is characterized by an open flow of intelligence sharing within the aviation domain, which is then supplemented at state aviation facilities via the robust utilization of human observation and interaction of passengers by the IAA. In sum, the Israeli model of aviation security centers upon interdicting the *individuals* who intend to commit an act of terrorism within the aviation domain, and not in detection of *offensive weapons* that may be concealed and transported into aviation facilities or otherwise smuggled aboard aircraft.

a. Intelligence Collection and Analysis

Citing Israeli General Meir Dagan, Tucker (2003) posits that "The first priority [to combating terrorism] must be placed on intelligence, then on counterterrorism operations, and finally on defense and protection" (p. 3). According to the official website of the Israel Security Agency (ISA), the country's domestic intelligence service, which is also known as *Shin Bet,* works closely with the Israeli Defense Force, the Mossad, and the Israeli police to protect the state from threats of terror, espionage, sabotage, subversion, and the disclosure of state secrets (Israel Security Agency, 2010a). In order to accomplish this mission, the ISA utilizes "sophisticated technological resources" and methodologies in both human and technical collection to acquire threat assessment information (Israel Security Agency, 2010b). But, unlike the USA's intelligence community, the ISA concentrates its agency's efforts within the realm of human intelligence collection (Tucker, 2003, p. 3). Intelligence products published from the ISA are also shared with the IAA for the defense of Israeli aviation facilities.

Rafi Ron, a former chief of IAA security operations from 1996–2001, testified before the U.S. Congress that that in order for an attack on an aircraft to be launched two pre-conditions must be in existence: 1) "There has to be a person with hostile intentions," and 2) "A weapon must be used" (Ron, 2002). Within the text of this same testimony, Ron goes on to explain that explosive materials and devices have evolved to the extent that it is oftentimes difficult to screen both individuals and baggage for dangerous contraband with 100 percent success. According to Ron, this is due to the fact that these materials are easily concealed in an artful fashion and thus may be passed through technological screening devices undetected. As a consequence, the IAA, much like the ISA save and except for the duty to recruit human sources for intelligence operations, focuses the bulk of its aviation security resources on human observation and interaction, also known as human profiling, in conjunction with the use of threat assessment information to determine whether or not an individual is either a high- or low-risk passenger.

b. Human Observation and Interaction

Ron's February 27, 2002 Congressional statement characterizes the Israeli method of human assessment as a "systematic, real time" means of discerning the level of risk a given individual poses to aviation security. This model of human observation and interaction is based upon two general components. First, human interaction is predicated upon an individual's age, ethnicity, birthplace, and religion, amongst other unidentified factors, that are automatically factored into a risk profile of a passenger prior to reaching an airport ticketing counter (Tucker, 2003, p. 6). At this point in time, dependent upon the profile, an interview may be conducted with a potential high-risk passenger at this outer layer of the IAA's protective envelope inside the airport environment. Once at check-in, however, all passengers are interviewed with a series of questions, the specific purpose of which is to elicit information regarding the passenger's reason(s) for travel as well as the particular contents of their baggage. Changes in narrative and or behavior are observed and any anomalies are noted for further consideration and investigation.

Second, if cleared from the ticketing counter to proceed toward an aircraft loading area, all passengers are continuously observed throughout their ingress, or penetration, into the airport environment. Throughout this continuous observation process, Tucker (2003) notes that individuals are selectively engaged by security personnel for an interview at some point in time prior to actually boarding an aircraft (p.

6). These subsequent brief investigatory interviews are based upon anomalous behavioral traits that may be detected by the security staff. These interviews reportedly last “90 seconds” to as long as “20 minutes,” according to Ron’s Congressional statement, and are supplemented as necessary with baggage searches that may involve testing at the “forensic level” for passengers subsequently identified as threats to the aviation domain (2002).

2. UK Aviation Security: Major Themes

In 2002, the British government appointed the Right Honorable Sir John Wheeler[56] to conduct a review aviation security in the U.K. and report his findings. In 2003, Wheeler submitted his conclusions and recommendations in a work product entitled, *Report of Airport Security*. In 2005, Wheeler conducted similar research for the Commonwealth of Australia and subsequently produced a report entitled, *An Independent Review of Airport Security and Policing for the Government of Australia* (Wheeler Review). The Wheeler Review incorporates many of the same recommendations and conclusions as the former 2003 Report *on Airport Security*.

As such, in the 2005 *Wheeler Review*, the author notes that the “three essential security pillars [of] policy, operations and capability development” are critical to improved aviation security (Wheeler, 2005, p. 130). Accordingly, the U.K. has achieved a particularly high level of competence in the areas of integration and utilization of closed captioned television (CCTV) and interagency cooperation. The elements of interagency collaboration and cooperation are also evidenced by the U.K.’s development and use of the multi-agency threat and risk assessment (MATRA) methodology; the gold, silver, and bronze system of transit police command and control, as well as development of an overarching counter-terrorism strategy (CONTEST).

Before discussing the specific elements of each of these U.K. programs, however, it is helpful to understand that CONTEST is a national counterterrorism strategy in the U.K., the likes of which do not exist within any U.S. federal agency, inclusive of either

[56] The Right Honorable Sir John Wheeler is a British citizen and politician who served in the Cabinet of the UK Prime Minister, The Right Honorable Sir John Major (Debrett’s, 2010).

the FBI or DHS-TSA. As a U.K. national strategy, then, CONTEST is divided into four principal areas of concentration (U.K. Office of the Home Secretary, 2010):

1. Pursue: to stop terrorist attacks.
2. Prevent: to stop people becoming terrorists or supporting violent extremism.
3. Protect: to strengthen our protection against terrorist attack.
4. Prepare: where and attack cannot be stopped, to mitigate its impact.

a. CCTV

According to the U.K.'s Parliamentary Office of Science and Technology publication *Postnote*, CCTV is used for four principal reasons: 1) to monitoring public areas to identify suspicious events and subsequently direct security responses; 2) to record events for evidentiary purposes; 3) to engage in directed surveillance against suspected offenders; and 4) to serve as a deterrent against unwanted activities, particularly those involving criminal acts (United Kingdom Parliamentary Office of Science and Technology, 2002, p. 1). To accomplish these objectives, UK CCTV control rooms are designed with advanced digital technologies that alert operators to anomalous situations[57] within certain CCTV-monitored environments, as well as pre-identified vehicle registration numbers, thus improving overall efficiency by reducing the necessity of CCTV operators to constantly monitor all cameras integrated into a particular CCTV system. Furthermore, by properly training CCTV operators in the use and appropriate documentation of recorded events, CCTV operational personnel are able to help identify regular patterns in both passenger and vehicular traffic, as well as identify anomalies within high-risk areas vulnerable to exploitation and attack. As such, regular surveillance and documentation via CCTV monitoring assists U.K. security authorities in identifying, interceding into, and ultimately disrupting acts such as the pre-operational surveillance of an enemy prior to an attack.

[57] An "anomalous situation" may, for example, be a piece of luggage left unattended in the public area of an airport. As such, algorithms may be developed for use with CCTV equipment that may automatically sense and alarm at such events so that explosive detection teams and or bomb technicians may be dispatched to inspect and resolve the threat prior to a potential detonation.

b. Interagency Cooperation

Interagency cooperation and improved aviation security are characterized in the UK through both the MATRA threat assessment system as well as the counter-terrorism strategy CONTEST. Specific details on the MATRA system will be discussed at length later in this chapter. However, as this risk assessment system generally encourages collaboration, communication and coordination amongst aviation security personnel, the Rt. Hon. Sir John Wheeler is quoted in the 2005 review as stating: “The [MATRA] model encourages a culture of cooperation through sharing information, meetings, strong leadership, and linkages with other airport committees (where MATRA groups are meant to be strategic, other groups tend to be operational). It is, in short, an all-way communication process” (Wheeler, 2005, p. 124).

Interagency cooperation and communication is further characterized in the U.K. by the deployment of specialized police personnel within the aviation domain. Known and referred to as the Aviation Security Operational Command Unit (SO18), a component of the London Metropolitan Police Special Branch Division, officers assigned to this detail are highly-trained in counterterrorism policing tactics. Similar to the numerically smaller contingent of FBI Airport Liaison Agents in the U.S., officers attached to SO18 focus on working with both airport security operators as well as the U.K.’s intelligence resources to ensure the security of London’s airport facilities.

3. Commonwealth of Australia Aviation Security: Major Themes

As identified by the 2005 Wheeler Review, the system of aviation security in Australia is characterized by three principal themes that may be relevant to U.S. aviation security enhancements, specifically: 1) Airport Security Command Structure; 2) Intelligence Sharing; and 3) Threat Analysis (Wheeler, 2005). Each of these fundamental elements will be individually examined within the context of the Australian aviation security environment as identified in the 2005 Review.

a. Airport Security Command Structure

The 2005 Review identified “command and control” of aviation police and security forces at Australian airports as a substantial impediment to achieving an enhanced national security posture within the air domain (Wheeler). Moreover, the 2005 Review noted that there was neither consistency in unity of command, control, communications, nor central police leadership at any given Australian aviation facility (Wheeler). As a result, the 2005 Review recommends an inter-jurisdictional approach to forming Australian aviation police contingents. Specifically, the 2005 Review suggests placing a federal police commander at each major airport in Australia, and then rounding out that force with police officers from state and territorial police agencies. The exact compliment of each police force, according to the 2005 Review, is dependent upon the geographical size/location/transient population of the airport, along with other factors highlighted by the joint threat assessment analysis for each airport facility considered.

b. Intelligence Sharing

The 2005 Review notes that “intelligence [information] is the first line of defense against terrorism and crime at airports” (Wheeler, p. 52). Despite this fact, the 2005 Review also cites that cultural issues regarding threat assessment information dissemination has been hampered at Australian airports such that fact-based decisions, which are facilitated by intelligence products distributed to aviation security decision makers, are oftentimes unavailable (Wheeler). Accordingly, Australian aviation police and security practitioners are left to function in a reactionary mode as opposed to fielding a more proactive security posture. In sum, the 2005 Review concludes that threat assessment information “. . . should be shared rather than sequestered, used rather than filed away” with and by those individuals who possess both the authority and responsibility to ensure the security of Australian aviation facilities (Wheeler, p. 87).

The remedy to this dilemma in Australia has been to proffer a two-fold response: 1) alter legislation as necessary to facilitate the dissemination of threat assessment information to appropriately cleared airport security operators; and 2) to charge the Australian Security Intelligence Organization with the legal responsibility to pass intelligence products to airport security officials so that it may assess the information relative to the threat environment that then exists.

c. Threat Analysis

The system of threat analysis in the Australian Aeronautical Domain is adapted from the U.K.'s Multi-Agency Threat and Risk Assessment (MATRA) methodology. Developed and tested in the U.K. after the initial 2002 Wheeler Report on Airport Security, the MATRA methodology recognizes that size, location, physical composition, and other general characteristics of the threat environment for individual aviation facilities will present different threats, vulnerabilities and contingent risks for each location assessed. As such, MATRA promotes an interdisciplinary approach to conducting aviation threat assessments by enlisting the involvement of various police, security, and private stakeholders at each facility to compose a threat assessment team. Approaching the aviation threat assessment in this manner, according to the Wheeler 2005 Review, will encourage a jointly owned work product that can be supported by all parties.

There are four main components of the MATRA system. First, a general threat assessment is conducted that identifies all of the probable threat streams, along with the potential consequences of each, that are most likely to be encountered at an individual airport. Second, a vulnerability assessment is conducted to determine which particular assets at a given aviation facility may be at the greatest risk to the potential attack scenarios considered. Third, a comparison of the threats and vulnerabilities is conducted to discern the overall real or residual risks that exist within the facility assessed. And fourth, an action plan is developed by the joint committee to determine which countermeasures are necessary in order to sufficiently mitigate the residual risks identified.

Finally, the Australian MATRA system is monitored by the national government at individual airports across the Commonwealth. This is a significant difference from the current aviation security system in the U.S. where there is no federal mandate to incorporate a consistent, recurrent and systematic plan for assessing individual threat(s) and risk(s) at commercial-use aviation facilities.

E. DISCUSSION & RECOMMENDATIONS

While none of the foreign aviation security partners assessed in this research totally discard the appropriate use of advanced physical screening technologies within the air domain to locate weapons and other dangerous materials, it is apparent that Israel, the U.K. and Australia all tend to focus more proactively within two principal areas: 1) engaging in multi-agency collaboration and coordination amongst security partners; and 2) a prevailing focus on identifying dangerous people, not dangerous belongings. To achieve the ultimate goal of aviation security, then, these countries engage in the following key security activities:

- **Israel**: robust intelligence gathering and sharing of the same information with aviation security partners of travelers prior to their arrival at an airport facility; physical observation of airport travelers once they have arrived at an airport facility; and finally, face-to-face engagement of passengers through interviews prior to boarding a departing flight.
- **UK**: robust intelligence gathering and sharing of the same information with aviation security partners—those security partners being Special Branch police officers who have been specifically trained in the U.K.'s national counterterrorism doctrine—of travelers prior to their arrival at an airport facility, which in the case of the U.K. is characterized by the use of enhanced CCTV systems; command and control of police/security resources as noted through the gold, silver and bronze system,[58] along with the CONTEST national strategy; and finally, the incorporation of a joint threat assessment methodology (MATRA) for each commercial airport within the U.K.'s jurisdiction.
- **Australia**: robust intelligence gathering and sharing of the same information with aviation security partners of travelers prior to their arrival at an airport facility; utilization of a coordinated system of

[58] The reference to the "Gold, Silver and Bronze" system of managing UK police forces is made simply to demonstrate that the various components of the UK system of law enforcement work in concert with one another in a structure and coordinated manner, under a common antiterrorism doctrine, in order to better secure the United Kingdom. Considering that the U.S. hosts a plethora of policing agencies at all levels, the suggestion here is simply that U.S. law enforcement/aviation security organizations should consider adopting a similar coordinated approach to sharing information and resources to better secure the U.S. NAD.

police/security command and control at the federal, provincial and local levels. Finally, the incorporation of a joint threat assessment methodology (MATRA) for each commercial airport within Australia's jurisdiction.

Compared to the current overall system of aviation security, all of the practices outlined above possess a great deal of promise for the U.S. aviation security industry. Consequently, generally speaking, the U.S. should consider adoption of a more collaborative approach to aviation security with an overall shift in focus to identifying potentially dangerous people, not just weapons alone. More demonstrative of the notion of success with respect to the foreign security practices identified, however, is the recurring themes of police/security/intelligence service cooperation and coordination—themes that are evidenced in the works cited herein.

Moreover, while legal, logistical, political, and cost constraints may prohibit practices such as the Israeli method of interviewing all passengers prior to boarding, or the Australian practice of meshing all police/security forces at U.S. airport facilities, some modified form of these methodologies may be attainable domestically. For example, the U.K.'s use of digitally based CCTV surveillance may provide a force multiplying effect for U.S. aviation security operators that facilitates the Israeli methodology of enhanced human observation while only permitting engagement of passengers who demonstrate some behavioral anomaly indicative of a threat.

The recurring theme of intelligence gathering and sharing amongst the foreign partners examined herein is, in fact, a smart practice for U.S. practitioners and is further supported by the U.S. 9/11 Commission Report. Likewise, Australia's and the U.K.'s use of the MATRA system of consistent and recurrent threat assessments is promising and is widely discussed within U.S. aviation security circles, but unfortunately the specific practice of conducting comprehensive threat assessments at domestic aviation facilities within the U.S. has not come to fruition at this time. Overall, however, none of the practices outlined herein would be cost prohibitive to either the U.S. government or domestic airport security operators because, in large part, all of the practices outlined chiefly involve changes in governmental policy and culture, and do not entail the large capital outlay or investment of expensive infrastructure. One potential exception, however, may be in cases where the addition/rehabilitation of CCTV systems is necessary due to either a poor design/deployment strategy, or because the age and technological capability of the current equipment is inadequate.

F. CHAPTER SUMMARY

The terrorist attacks of September 11, 2001 have fueled a near decade-long debate regarding how best to ensure the future security of the U.S. National Aeronautical Domain. Traditionally within the U.S. aviation security sector, emphasis has been placed upon detecting offense weapons, such as firearms and explosive devices, by the use of screening technology. In a post-9/11 aviation threat environment, the U.S. government has generally maintained the same philosophical approach, specifically: utilize advanced technology to locate the physical implements, or tools, of terrorism prior to their introduction onto a commercial aircraft. Accordingly, with the advancement of explosive trace detection equipment, more sophisticated imaging technologies, as well as the deployment of additional explosive ordinance detection canine teams across the U.S., this trend has continued domestically with little variation.

Conversely, other countries faced with the same challenges to secure their respective aeronautical domains have instituted programs, policies, and technological infrastructure to supplement their post-9/11 security posture, but with one fundamental philosophical variance, that is: focus on locating, identifying and neutralizing dangerous people—not necessarily the weapons that might be utilized to facilitate an attack—prior to the dangerous person’s introduction onto a commercial aircraft. As such, this thesis chapter seeks to explore the theoretical and operational security focuses of three different democratically governed countries—Israel, the U.K. and Australia—to determine the potential efficacy of those countries’ respective aviation security methodologies for possible inclusion into the U.S. aviation security strategy.

In brief summary, while the major theme in U.S. aviation security continues to be a focus on the identification of dangerous weapons, which, to be sure, is an extremely important aspect of aviation security, Israel has maintained its long-established center of interest in profiling dangerous people prior to their arrival at aviation facilities.

Specifically, by the utilization of both intelligence resources and thereafter within the geographical footprint of the airport by physical observation and face-to-face interviews with travelers, Israeli aviation security forces have produced a long and impressive record of aviation security success. Likewise, Australia has implemented an enhanced aviation intelligence apparatus and threat assessment process that supplements an inter-jurisdictional police service to maintain its defense of national aviation resources. And finally, the UK has implemented the advanced use of digitally-based closed captioned television systems, supplemented by appropriate policies and interagency cooperation, to deter, identify, interdict, and, as necessary, respond to suspicious individuals within the aviation domain. To be sure, within certain legal as well as logistical limitations,[59] all of the security methodologies utilized by these foreign aviation security partners could prove useful within the U.S. aeronautical domain.

Further research in this area is certainly recommended, which is a point that will be noted within the conclusion chapter of this thesis.

[59] Note the introductory facts cited early in this chapter regarding variances in each country's aviation domain size, scope, and transient populations, all of which are factors that may ultimately inhibit the incorporation of the exact methodologies utilized in each country analyzed. Legal constraints may also impact implementation of these factors from country-to-country as well.

VI. CREATING AN INTELLIGENCE-LED, RISK-BASED AVIATION SECURITY MEGACOMMUNITY[60]

> Leadership and organizational structures must support and reward innovations in community partnership and problem solving. (Peed, 2008)

A. INTRODUCTION

Sir Robert Peel,[61] oftentimes referred to as the "father of modern policing," understood that effective partnerships with all facets of a community were necessary in order to ensure public safety. Similarly, in order to adequately defend the United States against future attacks within the homeland, particularly with in the aviation domain, the tasks of integrating intelligence-based threat assessment information with risk-based operational planning and decision-making will require great effort, coordination, and collaboration from the police, security groups, and the public alike. This will certainly not be an easy task, especially given the traditional law enforcement/security subcultures that rightly place a great deal of value into secrecy for operational security purposes. As such, a specific organizational construct should be adopted within the aviation security industry that facilitates and supports a logical migration into a more open, communicative, and participative environment. Accordingly, the commercial aviation industry must seek and implement remedies to these problems before another national catastrophe occurs.

The December 25, 2009 attack (12/25 attack) of a commercial aircraft in Detroit, Michigan demonstrates two critical issues: 1) that the U.S. Aeronautical Domain is still considered a high-value target for terrorist factions; and 2) that but for good fortune, the 12/25 attack referenced above would have been successful—especially given the missed

[60] A "megacommunity" is defined by Gerencser, Lee, Napolitano, and Kelly (2008) as "a collaborative socioeconomic environment in which business, government, and civil society interact according to their common interests, while maintaining their unique priorities" (p. 232).

[61] Sir Robert Peel (1788-1850) was a British politician and prime minister and is considered the "father of modern policing" because of reforms he instituted within England's police force in1829. These reforms are characterized, in part, by Peel's acknowledgement that the police and a state's citizens must form a community partnership in order to ensure public safety (Answers.com, 2010).

intelligence opportunities revealed in the post-event investigation.[62] As such, there is still much to be accomplished in order to better secure the national air transportation network. Since the reliance upon good luck is not a viable anti-terrorism strategy for the United States, the future physical and financial security of the U.S. Aeronautical Domain will rest largely upon the willingness and abilities of the actors within the sector to connect together for a common purpose. To this end, a significant paradigm shift in aviation security strategy must first occur with respect to intelligence sharing and critical infrastructure protection within the domain. More specifically, all of the stakeholders within the U.S. aviation industry must join together and engage each other as a community with a common cause—that cause being the continuous improvement and evolution of aviation security in advance of developing threat streams to the sector.

Accordingly, those working in and otherwise utilizing domestic air transportation services must become a community—an aviation security megacommunity—truly devoted to the protection of the people and the critical assets that constitute the American aviation transportation network. Thus, in order to achieve the goal of becoming an effective aviation security mega-group, many lessons in strategic community engagement should first be gleaned from the guiding principles established in an assortment of business management publications available today.

B. BORROWED PERCEPTIONS ON COMMUNITY ENGAGEMENT FROM THE BUSINESS SECTOR

In the publication *Megacommunities*, Gerencser, Lee, Napolitano, and Kelly (2008) note, "Megacommunities are not large communities of people; they are communities of organizations whose leaders and members have deliberately come together across national, organizational, and sectoral boundaries to reach the goals they cannot achieve alone" (p. 28). Furthermore, within these megacommunities described by the authors, Gerencser et al. (2008) also introduce the notion of "tri-sector" collaboration,

[62] See, for example, the *White House Review Summary Regarding the 12/25/2009 Attempted Terrorist Attack* wherein federal investigators found that sufficient threat assessment information existed within the Intelligence Community (IC) to thwart Umar Farouk Abdulmutallab's attack, yet the IC failed to share the information within the broader intelligence "megacommunity" such that the dots could be connected to ultimately prevent the attack (White House, 2010).

which is the understanding by leaders that three indispensible groups - composed of private, public and civil sectors -actually comprise the overall population that constitutes the "megacommunity" (pp. 194–197). As the idea of megacommunity engagement relates to air domain security, the general theory encompasses great utility because, as already noted in this research project, U.S. Category X airport facilities represent very large and diverse communal populations. Typically employing anywhere from 25,000–45,000 public and private sector workers at each facility[63], as well as transporting millions of passengers (civil sector representatives) annually at each of the nation's largest 27 commercial service airport complexes, Category X aviation facilities serve as a prime example of a potential security megacommunity—one rich in potential intelligence gathering/sharing capabilities due to the inherent overlap in vital interests, structure and convergence of the air transportation industry. The vital security interest of the domestic aviation industry is, or should be, the ultimate goal of providing for the safe, efficient, and unimpeded movement of people and commerce across the United States. Finally, if one considers that all Category X airports are linked into a national air service network, then the potential aviation security megacommunity's population grows exponentially . . . provided, of course, an effective strategy is utilized to first build the megacommunity's security system.

The strategic elements necessary to build a national aviation security megacommunity—one that seeks to collect and disseminate threat assessment information and protect the critical infrastructure that ultimately supports the industry—may be found in the work, *Blue Ocean Strategy* (Kim & Mauborgne, 2005). In this publication, Kim and Mauborgne (2005) note that there are three characteristics of a good strategy, specifically: 1) focus; 2) divergence; and 3) a Compelling Tag Line (p. 39). In the context of aviation, then, the term "focus" relates to centering the aviation megacommunity's attention on security-related matters, conveying the understanding that everyone is responsible for contributing to the security effort. The term "divergence" relates to a departure from the status quo and aviation's predominant reliance upon

[63] This estimation is predicated upon this researcher's personal knowledge of the Houston Airport System's credentialed employee population.

standard TSA baseline security measures to ensure air domain safety, and the emerging "tagline" should emanate from the national megacommunity's interdependence upon one another to produce a more proactive intelligence-led, risk-based security strategy. While the idea of actively gathering and sharing threat assessment information within aviation is not new, in practice the concept is only a good theory. In fact, some aviation security practitioners within the industry and law enforcement arenas would label the idea of widespread collaboration and threat assessment information sharing as foolish and unwise based upon, for example, the traditionally inflexible "need to know" standard of sharing intelligence information.

To the contrary, however, in their publication *The Starfish and the Spider*, Brafman and Becktrom (2006) postulate that rigid, orderly and hierarchal solutions oftentimes stifle creativity and innovation (p. 203).[64] Consequently, in today's asymmetrical aviation threat environment where terrorist organizations and individual perpetrators are more decentralized and creative, and in fact are leaderless in more and more instances, a more participative, evolutionary, and novel security strategy is necessary. Accordingly, including and leveraging the collective knowledge and ideas of all of the members within the aviation megacommunity, inclusive of non-traditional security partners such as ramp agents, ticket agents, janitorial staff, and airline mechanics in the protective services process, the National Aeronautical Domain as a whole will become safer and more resilient because these non-traditional partners may: 1) provide insight into vulnerabilities previously not considered by traditional security/police assessors; 2) provide insight into what types of countermeasures may be most effective in the protection of aviation critical infrastructure and key resources; and 3) by practicing inclusion, provide a forum by which to convey previously untapped intelligence sources for security/police groups whose principal responsibility is the protection of the air domain. This more organic, non-typical, decentralized approach to aviation security is exactly the type of strategy necessary in order to combat adversaries to the domain who

[64] As the limitations of rigid, hierarchal decision-making are considered in *The Starfish and the Spider*, one may draw an analogous reference to the 911 Commission Report's conclusion that the bureaucracy of the U.S. government failed "in imagination, policy, capabilities, and management" (*9/11 Commission Report*, 2004, p. 339).

are likewise creative, increasingly decentralized and innovative in their own regard. But establishing trust amongst those within the aeronautical industry, although a daunting and long-term task, will ultimately be a critical enabler in achieving an all-inclusive, robust and effective intelligence-led, risk-based national aviation security strategy.

Covey and Merrill (2006) denote in *The Speed of Trust* that "trust impacts us 24/7, 365 days a year. It undergirds and affects the quality of every relationship, every communication, every work project, every business venture, every effort in which we are engaged" (pp. 1–2). Unfortunately, however, even within the post-9/11 aviation security industry, the vital element of trust has neither been widely extended nor leveraged outside of the formal hierarchy of law enforcement and security circles in the pursuit of air domain security. While regrettable, this condition is understandable due to the inherent nature of distrust extant within most security/police subcultures toward anyone else outside of those closely associated fields of work; trust is also difficult to establish between air carriers who are, understandably, very protective of their corporate information within an intensely competitive, capitalistic marketplace.

Consequently, before a paradigm shift may occur to inculcate an intelligence-led, risk-based security strategy utilizing the strategic principles found in *Megacommunities* (Gerencser, et al., 2008), *Blue Ocean Strategy* (Kim & Mauborgne, 2005), or the flexible *Spider and the Starfish* (Brafman and Becktrom, 2006) -type organizations, change agents must begin extending "smart trust" (Covey & Merrill, 2006, p. 287). Smart trust, according Covey and Merrill, is an area of trust found on a "smart trust matrix" between distrust/suspicion and blind trust/gullibility (p. 288), and it is exactly this type of trust that must be extended to the hundreds-of-thousands aviation workers heretofore not actively engaged in the aviation security process nationwide. As such, aviation security groups across the nation, in partnership with the law enforcement and DHS elements extant within the sector, are in the best position to begin building a national security network—and in due course recruit other members into the aviation security megacommunity from both aviation business and private citizens. Within this paradigm shift of better communication, coordination, and collaboration, overcoming the traditional turf wars and trust issues inherent within the intelligence community may be overcome within the NAD by: 1) the identification of a specific inter-jurisdictional work plan, and 2) practicing the elements of trust and engagement previously cited herein.

As a consequence, an intelligence-led, risk-based strategy that endeavors to incorporate the elements of trust and community engagement are necessary to effectively evolve and thwart emerging threat streams to the air domain. Fortunately by reaching out to the millions of Americans working in and otherwise utilizing the national aviation transportation network, and with the inculcation of widespread trust within this megacommunity, a flexible, adaptive, and more robust security community may be developed that will effectively and pragmatically evolve to better secure this nation’s critical aviation infrastructure and key aviation resources.

Considered in this context, then, the nation’s overall aviation security posture may be improved in a post-9/11 environment by incorporating a policing/security methodology within the domain that endorses the concepts of cooperation, community engagement, communication, and collaboration—in conjunction with intelligence-based threat assessment information as discussed in Chapters III and IV of this thesis. Accordingly, a contemporary policing strategy known as intelligence-led policing may provide the necessary organizational model to affect such as result.

The past 150 years of American policing has seen many eras, each of which has been characterized by the dominant policing strategy in place at the time. In fact, Kelling and Moore (1988) define three distinct periods of American policing, specifically: “the political, the reform and the community problem solving” eras (p. 2). Within the community era of policing defined by Kelling and Moore (1988), Ratcliffe (2008) identifies five distinct variations, or common models, of policing in the United States: 1) standard model of policing; 2) community policing; 3) problem-oriented policing; 4) Compstat; and 5) intelligence-led policing (p. 65).

The most current evolutional model of policing in the United States, intelligence-led policing, is based upon the strategic level and has linkages to all of the policing models cited hereinabove (Ratcliffe, 2008, p. 6). Moreover, Ratcliffe (2008) defines intelligence-led policing as a concept or “business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption, and prevention through both strategic management and effective strategies that target prolific and serious offenders" (p. 6). Consequently, as the theory of intelligence-led policing may relate to improving the U.S. aviation security enterprise, Ratcliffe (2008) postulates that the concept of intelligence-led policing "is theoretically possible . . . without involving the traditional public police force" and "is now being widely offered by institutions other than the state, including private companies and community volunteers" (p. 7).

Finally, in considering all of the data available and whether or not an adaptation of intelligence-led policing should be implemented throughout the NAD, Ratcliffe points to the following key elements that, if properly implemented and managed, further support utilization of the model (2008, pp. 235–6):

1. There is a supportive and informed command structure;
2. Intelligence-led policing is the heart of an organization-wide approach;
3. Crime and criminal analysis is integrated;
4. The focus is on prolific and serious offenders;
5. Analytical and executive training is available;
6. Both strategic and tactical tasking meetings take place;
7. Much routine investigation is screened out;
8. Data are sufficiently complete, reliable and available to support products that influence decision-making;
9. Management structures exist to action intelligence products; and,
10. There is appropriate use of prevention, disruption and enforcement.

Given the totality of the data presented herein, in conjunction with the identified needs to incorporate an intelligence- and risk-based security model within the NAD, the intelligence-led policing methodology deserves further discussion and consideration.

C. INTELLIGENCE-LED POLICING (ILP)

> At its core, ILP helps leaders make informed decisions to address agency priorities. These priorities can include issues such as crime prevention, crime reduction, case management, resource allocation, case clearance, anticipation of future threats, or crime problems. This process provides

> guidance and support to the agency leader, regardless of the type of priority established (U.S. Department of Justice, Bureau of Justice Statistics, 2009)

Aviation security and law enforcement are two distinctly different work groups that operate, for the most part, in historically different work environments; however, both groups are charged with the duty to detect, deter, deny, delay, and respond to adversaries' attempts to compromise the national air transportation network. Moreover, as established in Chapter V of this thesis, the acquisition and deployment of physical countermeasures remains the principal responsibility of aviation security groups, not law enforcement. As such, the need to integrate threat assessment information into operations is critical to both domains if decisions regarding protective measures are to be predicated upon more than mere intuition. The concept of intelligence-led policing (ILP) may provide a methodological framework from which the U.S. civil aviation domain may adapt an intelligence-led aviation security megacommunity. For example, Carter (2004) defines ILP as ". . . an underlying philosophy of how intelligence fits into the operations of a law enforcement operation. Rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the overall mission of the organization" (p. 41). Furthermore, in support of the aviation security megacommunity theme, Carter (2009) denotes that ". . . ILP must be created through an inclusive developmental process to ensure that it is integrated with an agency's goals and functions, its capabilities, and the characteristics of both the agency and the jurisdiction it serves" (p. 79). Given Carter's definition of ILP along with this thesis's pre-established nexus between the U.S. commercial aviation operator's principal legal and operational responsibilities to protect the NAD at the infrastructure level (the nation's Category X airport facilities), it appears that conceptually an adaptation of ILP within the NAD may serve to more efficiently and effectively deal with threats within the national aviation system—on both a local as well as a national level. How?

Since the task of protecting a large U.S. Category X aviation facility involves, or should involve, as this thesis argues, decision-making relative to the deployment of both human and physical countermeasures on a recurrent basis dependent upon threat streams in order to be most effective, those involved in apportioning scare security resources must adopt a common rationale, structure or security philosophy. Otherwise, a security management team's "best guess" will be the only guiding principle for the rationing of protective assets. As such, an aviation security group must organize and avail itself to an organizational structure that seeks and requires the use of threat assessment information in the development and deployment of its overall security strategy. Ratliffe (2008) corroborates this point by stating that ILP:

> . . . is a business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders" (p. 6).

Accordingly, as applied within the realm of aviation security, one could slightly modify Ratliff's definition to include intelligence-based information such as threat assessment data for a particular facility or region of the nation, and simply supplant the phrase "enforcement strategy" for "security strategy."

With regard to the implementation of ILP into an organization, Carter (2009) states that "out the outset, ILP should be viewed as a philosophy, not a process "(p. 86). Therefore, the integration of ILP into an organization is contingent upon: 1) an agency's ability to create a threat assessment information network both inside and outside of its organization;[65] and 2) creating an internal management structure that supports the ILP process (Carter, 2009, p. 86).[66] Consequently, in addition to seeking access to computer-based intelligence networks, such as the Homeland Secure Data Network and Secret Internet Protocol Router Network, an aviation security organization should endeavor to create relationships within the broader security megacommunity. This strategic community outreach should not only include aviation-centric security organizations, such

[65] This key element of Carter's ILP integration plan is directly related to the concept of an aviation security megacommunity heretofore discussed in this chapter.

[66] This element of Carter's ILP integration plan is directly related to this thesis's argument that aviation security groups should move beyond implementing just the standard TSA-mandated baseline security measures and endeavor to routinely utilize intelligence-based threat assessments to guide, adjust and supplement available protective resources for any given aviation facility.

as proprietary air carrier security groups and the Federal Air Marshal Service and TSA, but affiliations with the local police, FBI, ICE, and CBP elements that also operate within the region of the Category X airport to be protected. Furthermore, the aviation security megacommunity outreach, and network, should extend throughout the nation’s 27 TSA-designated airport security coordinators representing all Category X airports within the United States.

Moreover, with regard to implementation, there is not a specific model that all organizations should emulate in order to apply ILP within their agency. In fact, Carter (2009) notes:

> …there are tools that can be used to identify the intelligence needs of an agency and then craft the policies and processes to make ILP functional for each department . . . [because] essentially, intelligence is about managing information . . . that is needed to identify threats of concern to a community, and having sufficient information about the threat to develop operational responses to prevent or mitigate the threat” (p. 99).

Consequently, Carter (2009) is urging the creation of two principal elements within any ILP-driven agency: 1) an overall management framework that accepts, inculcates and ultimately determines what the ILP process should be for any given protective agency; and 2) the inclusion of a trained intelligence analyst to collect, distinguish and advise the agency’s command hierarchy of the specific threat streams within the jurisdiction’s environment, or area of responsibility, that need to be addressed.

Therefore, philosophically, an aviation security management group must first agree that intelligence-based information should form the foundation of their respective airport security plan beyond that which is required by TSA regulations. Thereafter, once both technical as well as human resources have been developed to routinely receive intelligence-based information, the operational application of this information should be introduced into the security group’s decision-making processes at all levels within the organization. For example, in normal circumstances this could occur on a weekly basis with the local security group meeting to discuss any intelligence-based information recently obtained and dependent upon the contingent risks identified by use of that information, security patrol beats to heighten visibility in certain areas could be adjusted, or engagement in other security practices that may tend to disrupt an adversary's planning cycle could be introduced into the environment to be protected.[67]

In the event of a rapidly evolving threat, however, there is certainly nothing that prevents impromptu meetings to discuss potential response options vis-à-vis available resources. Moreover, with the occurrence of an immediate, time-sensitive threat, on-duty supervisory staff must retain the authority to control protective service resources and respond with agility to fast moving threat streams. This may be aided by the use of pre-determined contingency plans for various events, but the central point here is that intelligence-based information should be available and utilized by all levels of membership within a protective services organization on a consistent, continuous basis. Finally, the chart below outlines the seven basic strategic priorities that security managers should consider when implementing a version of ILP into their organization.

Table 3. Seven Strategic Priorities that Should be Considered When Implementing ILP into an Organization (From Carter, 2009, p. 100)

The Concept...	Asks the question…	Responsibility…
Strategic Priority	What problems are important to me?	Executive
Intelligence Requirements	What additional information do I need to better understand each problem, its causes, and its effects?	Executive, Commander, and Analyst
Collection Plan	Where (sources) and how (methods) will I get the additional information that I need to better understand the problem?	Commander and Analyst
Analysis	Collectively, what does the new information mean and what new insights does it provide about the problem?	Analyst with review by Supervisor

[67] The number of security practices that may be adopted and altered on an ongoing basis is limited only by a security group's collective imagination and the need to balance security operations with the least amount of disruption to routine flight operations at a Category X airport. This routine planning by the security group also includes other measures that may include planning and budgeting for major capital infrastructure improvements relative to security, such as the addition of closed captioned television coverage, and thereafter, the addition of a specially trained staff to monitor the environs for pattern of life anomalies, and so on. Nothing herein is meant to suggest, however, that quickly evolving threats must be addressed through a slow, bureaucratic process. Indeed, quick, agile response(s) are typically necessary in fast-paced, high-threat environments—such as in commercial aviation environments. Accordingly, this notation is made simply to remind the reader that intelligence-based information should form the basis of operational decisions—at all levels and regarding all threat conditions - whenever such information is available.

The Concept...	Asks the question…	Responsibility…
Intelligence Products	What actionable information do I need to tell other people in order to prevent or control the problem?	Analyst with Commander's Advice
Operational Responses	What explicit operational activities may be implemented to prevent or mitigate the priority problems? What resources are needed?	Intelligence and Operations Commanders
Process Review	From this process: › • Was the information accurate and useful? › • Could the problem be altered as a result of the information? › • What will make the process better? Did the operational response generate more local intelligence which should now be evaluated in connection with the threat?[68]	Intelligence and Operations Commanders with Feedback to Executive

D. CONCLUSION

Effectively defending the United States from another attack within the National Aeronautical Domain will require a more participative, inclusive and collaborative effort from traditional security entities, the private sector and the citizenry who utilize commercial air transportation services. The routine and timely use of intelligence-based threat assessment information juxtaposed against a Category X aviation facility's known security strengths and weaknesses is equally important for security groups to adjust the security posture of a particular facility in real time. Consequently, the adaptation of ILP into the aviation security domain on a national basis will naturally facilitate the merger of both intelligence-based threat information as well as formalized risk-assessment processes. As such, incorporated by an underpinning that recognizes the networked

[68] This question was posed, and subsequently added to Table 3 after consultation with the thesis advisors reviewing this document. Thesis co-advisor Paul Smith suggests that "this is an example of the intelligence cycle in action," and consequently should always be asked during the Process Review stage (Smith, 2010).

strength of a cross-functional group, a security megacommunity may emerge that will ultimately produce a more resilient, more flexible and, ultimately, a more secure national air transportation network.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. POLICY OPTIONS AND EVALUATION

A. INTRODUCTION: RESTATEMENT OF PROBLEM

As a critical component of the national infrastructure, the collective and sustained efforts of all levels of government, coupled along with collaboration from the private sector as well, must continue to bear upon the deterrence, detection and denial of future adversaries to the NAD. This fact is particularly true today since the enemies who attacked America on 9/11 remain committed to replicate the same type of catastrophic damage, death and destruction that the world witnessed on 9/11.[69]

Indeed, despite the fact that advances in aviation security have been achieved since 9/11, such as the passage of the *2001 Aviation Transportation Security Act* which created the TSA with a mandate to focus solely on national transportation security issues, impediments to optimizing the national aviation security enterprise still exist. As such, the foregoing chapters have attempted to explore the various key aspects of an effective local aviation security program—those elements which, if either instituted and or improved upon, may enhance air domain security even more across the United States. In so doing, this thesis discussed, among other factors:

1. The routine utilization of threat assessment information for the local security manager in managing regional aviation security plans;
2. The incorporation of a risk-based assessment methodology as a critical element in developing and refining local aviation security plans; and finally,
3. The application of an adaptation of intelligence-led policing, an organizational management construct that incorporates or merges both threat assessment information along with a risk-based assessment methodology into a security enterprise's philosophical and operational plans.

[69] This supposition is further supported, for example, by: 1) Richard Reid's 12/22/2001 "shoe bomb" attempt to destroy American Airlines Flight 63; 2) the August 2006 plot of al Qaeda operatives to destroy several U.S.-bound aircraft from Europe (re: UK's Operation OVERT); and 3) The 12/25/09 plot by Umar Abdulmutallab to destroy Northwest Airlines Flight 253 by detonating explosives hidden in his undergarments.

B. EVALUATIVE CRITERIA AND POLICY ALTERNATIVES CONSIDERED

Within the context of cost, legality, political acceptability, level of effort, and effectiveness, the following policy alternatives identified in Chapter I will now again be considered. Before that examination is begun in detail, however, note the Policy Options Matrix below from Chapter I. Additionally, as a review of the definitions assigned to the evaluative criterion at the beginning of this thesis, each element noted on the top horizontal line of the matrix is assigned the following meaning:

- ***Cost*****—**Refers to the monetary expense associated with implementing recommended changes.
- ***Legality*****—**Refers to the legal permissibility of state and federal statutes with regard to instituting recommended changes.
- ***Political Acceptability*****—**Relates to the acceptability of any proposed changes by local, state and federal legislative and executive bodies; also to the American public as a whole.
- ***Level of Effort*****—**The total amount of energy or exertion required by the managing body to implement any recommended changes.
- ***Effectiveness*****—**The total projected benefit to be yielded upon implementation of any proposed changes.

Finally, the first vertical box on each line of the matrix denotes the expected result of each policy option considered. Consequently, after careful consideration of the research and anticipated results, the results yielded at the end of this research product reaffirm what was originally hypothesized in Chapter I.

Table 4. Policy Options Matrix

Policy	**Cost**	**Legality**	**Political Acceptability**	**Level of Effort**	**Effectiveness**
1	Low	Yes	Poor	Minimal	Minimal
2	Low to Med	Yes	Med	Med	Med
3	Med to High	Yes	High	Med to High	High

Immediately below are the original policy questions posed at the beginning of this thesis in Chapter I. These policy options are enumerated as 1, 2, and 3, and correspond to the evaluative criteria in the Policy Options Matrix (Table 4). A detailed analysis and explanation of each policy option is undertaken in Subsection C of this chapter. Finally, also in Subsection C of this chapter, is a detailed explanation of the results recorded herein, which then leads to the Conclusion Chapter and the final recommendations.

1. Improve the Dissemination Element of the Intelligence Cycle[70] within the NAD

Homeland security intelligence processes and dissemination procedures have improved since 9/11, but instituting federal policies and procedures to further refine the dissemination element of the intelligence cycle may help ensure a timelier, more regular, and detailed distribution of threat assessment information to aviation security operators. This option might include the selective sharing of classified details regarding emerging threats within the NAD, which may ultimately assist the local aviation security manager at Category X facilities in better understanding and responding to the overall threat picture within the aviation domain.

To be clear, this option refers to the DHS-TSA Office of Intelligence and Analysis generating intelligence products, principally intelligence-based threat assessment products, for local aviation security managers on a more timely and consistent basis, which is a fundamental necessity currently not being accomplished by DHS-TSA. This could be accomplished, however, by the use of technology, such as secure video teleconferencing with local security partners, or through the use of incumbent field intelligence analysts already detailed to many TSA field offices around the nation. It does not necessarily require additional TSA intelligence personnel, but rather a more efficient dissemination of threat assessment information by some means. Conversely, this option may require local security operations to recruit intelligence analysts to interact with the DHS-TSA Office of Intelligence and Analysis personnel to receive information and properly analyze its meaning in a local context.

[70] According to Johnson and Wirtz (2008), *Intelligence and National Security: The Secret World of Spies*, the U.S. intelligence cycle consists of five steps: planning and direction, collection, processing, analysis and production, and dissemination (p. 49).

2. Increase the Frequency of the TSA Threat Assessment Process

Some improvements to the U.S. civil aviation security infrastructure have been realized since 9/11. For example, federalization of the screening workforce, standardization of the passenger/baggage screening processes and implementation of a broad-based triennial threat assessment of Category X airport facilities by TSA have all been incorporated within the NAD. But since large commercial aviation facilities are typically under a perpetual state of construction, reconfiguration, and expansion, a slight modification and improvement to the national aviation security posture may be realized if the triennial threat assessment currently mandated for Category X airports were required on an annual basis.

For clarification, this option merely refers to TSA conducting the triennial threat assessment on an annual basis, which, as noted in this research project, is currently a one-week review. This option does not propose to incorporate a more comprehensive threat assessment process, simply a more frequent one to account for the rapid changes in environmental conditions experienced at most Category X airport facilities.

3. Institute an Intelligence-Driven, Risk-Based Security Doctrine

Introduce federal legislation and or national policies to mandate the improved sharing and utilization of threat assessment information, along with the incorporation of a standardized risk-based management methodology,[71] into all U.S. aviation security programs at Category X airports across the nation. This option would necessarily also include a mandate for each local aviation security operator to institute an appropriate organizational model to analyze and respond to threat assessment information against specific risk assessment and reduction criteria.

Finally, this policy option incorporates much more than the small, incremental changes that may benefit U.S. aviation security in options one and two, above. In this

[71] An appropriate risk assessment methodology (RAM) may include, but not be limited to: Sandia National Laboratories RAM for sector-specific plans: criticality, accessibility, recoverability, vulnerability, effect, and recognizability (CARVER) methodology; or mission, symbolism, history, accessibility, recognizability, population, and proximity (MSHARPP) methodology.

policy option, a suggestion is made to: 1) increase DHS-TSA's sharing of threat assessment information with local partners in a more timely and consistent manner; 2) have DHS-TSA designate one specific risk-assessment methodology for use across the NAD; and 3) incorporate an adaptation of intelligence-led policing into the local aviation security domain that meshes elements policy options one and two together and into a comprehensive aviation security doctrine, which currently does not exist. This policy option suggests, as noted repeatedly throughout this research project, that intelligence-based threat assessment information should lead, guide, and direct aviation security operations beyond the minimum baseline measures currently mandated by DHS-TSA. Finally, this policy option may require additional personnel at the local level as well as specific training in intelligence matters, which are details covered in the main text.

C. POLICY OPTIONS ANALYSIS

1. Improve the Dissemination Element of the Intelligence Cycle Within the NAD

a. Lawfulness

Writing on behalf of the President of the United States as well as the Director of National Intelligence, and citing Executive Orders 12333[72] and 13470[73] as the legal predicate for sharing threat assessment information at the state, local and tribal levels (SLT), Information Sharing Environment[74] (ISE) Program Manager Thomas E. McNamara noted in his *2009 ISE Plans and Progress Annual Report to Congress* that ". . . the essential role of SLT and private sector partners is fundamental to the ISE and is a

[72] Executive Order 12333 "prescribes a uniform system for classifying, safeguarding, and declassifying information, including information relating to defense against transnational terrorism (White House, 2009).

[73] Executive Order 13470 amends and clarifies the President's intent with regard to the United States' intelligence activities, which prescribes, among other issues, the dissemination of threat assessment information (White House, 2008).

[74] Pursuant to Section 1016 of the Intelligence Reform and Terrorism Act, in 2005 the President directed that an Information Sharing Program Manager be a part of the Office of the Director of National Intelligence to ensure terrorism information is shared across federal, state and local governments (White House, 2005).

critical driver of information sharing in the homeland security and law enforcement communities" (p. 11). Furthermore, again referencing amended Executive Order 12333, McNamara (2009) stated, "State, local and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United States and its interests," and that "our national intelligence efforts should take into account the responsibilities and requirements of State, local and tribal governments . . . when undertaking the collection and dissemination of information and intelligence to protect the United States" (p. 11). As such, both the legal as well as the traditional "need to know" standards of receiving open source, sensitive, and classified intelligence products from the federal government are firmly established. Furthermore, as discussed in Chapter I of this thesis, both the *Intelligence Reform and Terrorism Prevention Act of 2004*, as well as *National Security Presidential Directive—47/Homeland Security Presidential Directive 16's Air Domain Surveillance and Intelligence Integration Plan* establish the legal prerequisites necessary to share threat information with local aviation security managers. Accordingly, the legal threshold for sharing threat assessment information with local aviation security managers is not only permitted by the spirit and intent of current law and Presidential mandate, but is actually required.

b. Effectiveness

The potential effectiveness of sharing threat assessment information to better protect the NAD is good. Beyond providing the local aviation security operator with enhanced situational awareness, trend analysis, and risk appraisal capabilities, if threat assessment information were shared more openly and regularly by the federal government then pragmatic changes and supplements to any one particular airport security operator's existing plans could be adjusted accordingly. Additionally, the intelligence-driven actions proactively enacted by local aviation operators could be monitored by TSA-HQ and replicated as a smart practice when and where appropriate at other Category X aviation facilities across the United States.

Conversely, two problems may exist with this approach alone relative to effectiveness. First, this approach alone presupposes that local aviation security managers are properly trained to analyze and interrupt intelligence information correctly. And second, assuming that a local security official is competently trained as an intelligence analyst, without the aid of a comprehensive risk-based analysis of their Category X facility the effective application of countermeasures may be marginalized. Consequently, while the approach of more widely disseminating threat assessment information at the local level would be better than the current limited state of dissemination across the NAD, the overall efficacy of establishing this measure alone would most likely be limited in scope.

c. Political Acceptability

Given the long history and support for better dissemination of threat assessment information across the NAD, particularly to local aviation security operators who as discussed in Chapter I of this thesis are in large part legally responsible for the security of Category X aviation facilities nationwide, the political acceptability of this measure would most likely be high. For example, the report produced by the *1989 President's Commission on Aviation Security and Terrorism* recommended sharing threat assessment information more widely at the local level, and that report was subsequently buttressed by the 9/11 Commission's recommendation to do the same. Consequently, along with a plethora of federal legislation and Presidential executive orders mandating better intelligence sharing with state and local homeland security officials, the political acceptability and public support for such an act would probably be very significant. Indeed, it appears clear from this research project that the spirit and intent of both the executive and legislative branches of the United States government, and vicariously from the people of the United States, is that there is a high expectation that threat assessment information will be shared at all levels of government in order to better protect the country against future attacks.

d. Level of Effort

The level of effort required to better share threat assessment information across the NAD is estimated to require a medium level of exertion in its preliminary stages of implementation. Placed into proper context, one should remember that the number of Category X aviation facilities in the United States numbers at a total of 27. As such, properly training and equipping approximately 100[75] additional local intelligence analysts across the United States with the resources to properly and regularly interact with regional fusion centers, the TSA Office of Intelligence, the DHS Office of Intelligence, and the FBI would be minimal. This estimation of effort is also supported by the probability that technological resources such as secure telephones and secure internet connections to resources such as the FBI's e-Guardian system and the Homeland Secure Data Network would be fairly inconsequential to acquire. However, a great deal of effort would probably exist to finally inculcate a custom and tradition within the intelligence and law enforcement communities that recognizes a vital need to share information with local aviation security mangers, thus requiring additional effort to break down the traditional lines of cultural demarcation and exclusion. Finally, the initial intelligence training for the local intelligence analysts may require a medium level of effort because all should receive an orientation and training DHS-TSA's Office of Intelligence and Analysis to familiarize the new personnel with DHS-TSA's policies, customs, and traditions regarding the aviation intelligence processes.

e. Cost

The relative costs, associated with better threat assessment information dissemination across the AND, are estimated to be low to medium in overall capital outlay and expenditures for travel and training. For example, since most Category X aviation facilities manage maintenance and operations budgets that require annual expenditures of hundreds of millions of dollars, the appropriation of funding for additional equipment, training and office space could most likely be managed with a modest to moderate increase to a Category X facility's budget.

[75] While the 100 is indeed an estimate of the total number of local intelligence analysts that would need to be recruited, hired and trained by local aviation authorities, it is an informed approximation. For example, a common staffing multiplier of 3.4 is oftentimes used to ensure that one person is on-duty 16-hours per day, 365 days per year. As such, 3.4 x 27 = 91.8 individuals necessary for this task across the NAD's 27 Category X airport facilities. As a consequence, this author simply rounded the number up to 100.

2. Increase the Frequency of the TSA Risk Assessment Process

a. Lawfulness

The law with respect to conducting risk- and threat-based assessments at Category X aviation facilities in the United States is clearly mandated by current statute and executive decree. Specifically, this mandate is evidenced by a litany of federal directives aimed at this objective with, for example, *Presidential Decision Directive 29* (PDD-29). PDD-29 was signed by President Bill Clinton in 1994 and ordered various elements of the federal government to develop post-Cold War security policies and procedures relative to threat analysis and risk management in order to better protect the critical infrastructure of the United States. Likewise, in 2003 President George W. Bush enacted *Homeland Security Presidential Directive 7* (HSPD-7), which directed federal agencies to identify, prioritize, and develop risk-based protective plans for all critical infrastructure sectors within the United States. The *National Infrastructure Protection Plan* and the *Transportation Systems Critical Infrastructure and Key Resources Sector-Specific Plan for the Aviation Sector* sprung from HSPD-7 and required, among other initiatives, to improve the security and resiliency of the NAD through the use of risk-based threat assessments. As such, increasing the frequency of tri-annual TSA threat-based assessments is not prohibited by either statute or executive declaration.

b. Effectiveness

The potential effectiveness of increasing the frequency of TSA risk-based assessments is judged as low, which is due to several reasons. First, the scope of the current tri-annual assessment is severely limited as most evaluations are conducted within a one-week timeframe, which is hardly long enough to conduct a comprehensive assessment of a sprawling Category X aviation facility. Second, the current TSA assessment process fails to include either a comprehensive assessment of the current protective measures and procedures utilized at an assessed commercial aviation facility, or any type of comprehensive engineering study to determine the critical components associated with the facility (e.g., major electrical and water supply sources), or any type of engineering study to calculate the structural resiliency of critical buildings, aeronautical navigational aids, etc. from a potential bomb blast. Third, the current assessment process utilized by TSA fails to include the local operator's input in any meaningful way, save and except the typical in-brief and out-brief after the week's assessment has been completed. Fourth, since most Category X aviation facilities are in a constant state of construction and physical reconfiguration, increasing the assessment process to even an annual basis would be of little assistance because of the rapid growth and change that most facilities experience on a continuous basis. As such, the viability or relative usefulness of such a work product is marginal in the first place, and simply increasing the frequency of such an assessment process would most likely continue to yield a product of questionable utility.

c. Political Acceptability

The political acceptability of increasing the frequency of the current TSA risk assessment process is judged as poor. While initially the measure may garner some support with both the public and the elected representatives evaluating such a measure, if and when it was revealed that the current TSA assessment process lacked in both breadth and depth (that it still a non-comprehensive, high-level, one-week review of a very large critical infrastructure site), then both a public and political backlash could result. Furthermore, as noted above, the relative usefulness of simply replicating an already sub-standard assessment process more frequently would most likely be viewed as a waste of time and taxpayer monies, thus adding to the popular public outcry of "airport security theater."[76]

d. Level of Effort

The level of effort to achieve an increased TSA risk assessment frequency is judged to be minimal. Since TSA assessment teams are fairly small, requiring only three to four personnel in total, then deploying these teams on a more frequent basis to

[76] The phrase "airport security theater" is defined by CNN commentator Bruce Schneier as "measures that make people feel more secure without doing anything to actually improve their security" (Schneier, 2009).

the nation's 27 Category X aviation facilities represents a fairly inconsequential burden for the federal government. Furthermore, unless the risk assessment process was altered to become more substantive or comprehensive in nature, then the time expended at any given commercial aviation facility would not be altered beyond the current timeframe of one-week.

e. Cost

The cost for increasing the frequency of the current TSA risk assessment process is judged to be low to medium. The rationale for this estimation is predicated upon the fact that only personnel costs associated with salaries and travel expenses would be impacted by deploying TSA risk assessment teams around the nation on a more frequent basis. As such, dependent upon whether or not TSA chose to increase staffing numbers to facilitate a more frequent assessment schedule, only travel expenses for incumbent personnel would affect the current cost burden associated with this process.

3. Institute an Intelligence-Driven, Risk-Based Security Doctrine

a. Lawfulness

With respect to both intelligence dissemination/use and the implementation of a specific risk-based assessment methodology within the NAD at the local level, the legality of instituting an intelligence-driven, risk-based security doctrine within the U.S. aeronautical domain is a legally viable option. Incorporated by reference herein, the rationale heretofore cited in sections 1(a) and 2 (a) of this chapter are also included herein as the legal foundation for which such measures may be instituted. Additionally, however, in order to ensure consistency and uniformity throughout the NAD in effectuating an intelligence-driven, risk-based aviation security doctrine, the legal authority to even mandate such measures are also found in Title 49 CFR § 1502.1.[77]

[77] Title 49 CFR § 1502.1 defines the responsibilities and authority delegated to the administrator of TSA by the U.S. Congress and the President of the United States. This statute lists, among other responsibilities, the designated administrator's duty to plan, direct and control the TSA as well as ensure security in all modes of transportation.

Accordingly, there are no legal barriers for the TSA to: 1) begin to share threat assessment information more regularly with local security partners within the NAD; or 2) designate a specific risk-based assessment model for use in the aviation domain.

b. Effectiveness

The projected benefits from instituting an intelligence-led, risk-based security model within the aviation domain are judged to be high. The basis for this conclusion is predicated upon the notion that if threat assessment information were shared more consistently with local security operators then pragmatic changes and supplements to any one particular airport's security plan may be augmented based upon that facility's risk-based assessment of strengths and contingent weaknesses. Once identified, vulnerabilities could then be addressed with a tailored approach at each of the nation's airports dependent upon the unique physical, environmental, financial, and human resources available to each facility. The inevitable differences in the type, amount and frequency of the countermeasures deployed at each airport would then result in a more random and unpredictable threat mitigation strategy, thus forcing adversaries to either abandon a particular plan or otherwise expend appreciably more time and resources conducting preoperational surveillance.[78] Finally, the effectiveness of this particular approach would be realized by moving beyond the standard baseline, or minimum, measures typically required by TSA-HQ, and would also facilitate creativity and collaboration at both the local and federal levels of government.

4. Political Acceptability

The political acceptability for adopting an intelligence-led, risk-based security strategy across the NAD is judged to be high. The foundation for this judgment is supported by the statutory requirements related to intelligence sharing and risk-based

[78] The effective utilization of available resources to thwart potential attacks is related to, and consistent with, the stated security philosophy of detecting, deterring, delaying, and denying adversaries to the NAD.

threat and vulnerability assessments already discussed in this chapter and incorporated herein by reference. Additionally, however, this concept is also supported by the recommendations of the 9/11 Commission.

For example, Chapter 12.4 of the *9/11 Commission Report* recommends that federal, state and local governments develop “a layered security system” across the U.S. aviation infrastructure “that [is] redundant and coordinated” (pp. 391–392). Moreover, the protective layers instituted must be deployed based upon a *plan* to identify and “improve weak individual layers and the effectiveness of the layered systems” deployed (*9/11 Commission Report*, 2004, p. 392). Likewise, the *9/11 Commission Report* in Chapter 13.3 details the fact that federal, state and local entities should organize themselves in order to achieve “unity of effort” in information sharing, recognizing that the Cold War standard of sharing intelligence based upon a “need to know” standard should evolve into a culture of “need to share” (p. 417).

a. Level of Effort

The level of effort required to institute a two-pronged approach of intelligence-led, risk-based aviation security is judged to be medium to high. This is assessment is based upon principal two factors: 1) the TSA will have to identify and mandate the use of one particular risk-based assessment model to be utilized within the aviation domain, a decision-making process that will inevitably provoke much discussion and debate between the aviation industry and federal government; and 2) while providing the appropriate technologies and developing adequate procedures for changing culture with respect to intelligence sharing may be moderate, the larger challenge will be changing the culture within the intelligence community to recognize their responsibility to share information more readily. However, the level of effort necessary to effect these changes may be mitigated somewhat by again recognizing the relatively small population of 27 Category X airport security managers across the nation that would have to folded into this proposed change.

b. Cost

The cost to incorporate an intelligence-led, risk based security model into the NAD at all Category X airport facilities is estimated to be medium to high. This estimate takes into account the funding necessary to purchase a comprehensive, technology-driven, risk-based assessment program for all Category X airport facilities in the United States, as well as associated technologies for secure communications equipment, security clearances and appropriate training for local security personnel. Additionally, as discussed in Policy Option 1, approximately 100 local intelligence analysts would have to recruited, hired, and trained for this model (see Policy Option 1 for details relative to staffing and training). Considered it its totality, however, the relative cost borne from instituting an intelligence-led, risk-based security model, and actually creating a defined aviation security doctrine into the NAD, may be insignificant if compared to the potential of the U.S. sustaining another preventable attack within the air domain—preventable, perhaps, by the institution of this policy option.

D. CONCLUSION

> If you know the enemy and know yourself you need not fear the results of
> a hundred battles. (Sun Tzu, c. 6th century B.C.)

Centuries ago, the ancient Chinese General Sun Tzu wisely cautioned those engaged in conflict to know themselves as well as their adversaries in order to ensure long-term success. While those involved in today’s struggle to defend the National Aeronautical System against terrorism are certainly not operating on an active battlefield in a traditional sense, the sage advice imparted long ago remains relevant for modern day security managers nonetheless. Specifically, public safety officials must know and understand what needs to be protected—as well as its relative strengths and weaknesses—and at the same time also know and understand the likely tactics, techniques and procedures that adversaries may use to again attack the United States by exploiting the weaknesses within the national air transportation system.

To this end, this chapter examined three alternatives that may provide an enhanced level of protection for commercial use aviation facilities across the United States under a methodology utilizing key elements of public policy decision-making. As such, only Option 3, *Instituting an Intelligence-driven*, *Risk-based Security Doctrine*, accomplishes a more practicable, holistic approach of improving both aspects of a viable aviation security program through: 1) the acquisition and proactive deployment of resources against pre-identified contingent risks/weaknesses as suggested by a comprehensive risk assessment methodology; and 2) the effective and efficient utilization of those protective resources as suggested by threat assessment information. Accordingly, a comprehensive risk appraisal program used in conjunction with threat assessment information will best serve to bolster the overall aviation security posture of the NAD, above and beyond improving either the risk appraisal or threat assessment elements alone.

THIS PAGE INTENTIONALLY LEFT BLANK

VIII. LIMITATIONS, RECOMMENDATIONS, AND CONCLUSION

> Men never do evil so completely and cheerfully as when they do it from religious conviction. Blaise Pascal (1623–1662)

A. INTRODUCTION

Blaise Pascal's historic quotation is as true today as it was over 300 years ago: religion may sometimes be used as a pretextual justification for brutal and violent behavior. Indeed, in today's society, the threats against the United States are, to a very large and very real extent, deeply associated with religious extremism. Evidence of this fact was horribly manifested on September 11, 2001, when 2,974 (Alfano, 2006) innocent people were murdered on our nation's east coast in the name of religion. On that dreadful day, 19 hijackers[79] from a radical Islamic organization known as al-Qaeda[80] exploited the free and open principles that form the foundation of this country's existence and converted commercial airliners into weapons of mass destruction. This attack sparked the nation's Global War on Terror (GWOT) and subsequently resulted in the deployment of U.S. military and law enforcement resources around the globe—to distant places like Afghanistan, Iraq, and Pakistan. But, despite all that has been done to better secure the United States since 9/11, the threat to the U.S. homeland and commercial aviation continues to this day and may endure as such for three to four more generations. Consequently, ensuring the adequate defense of the National Aeronautical Domain is vital to the physical, psychological, and economic security interests of the United States.

With the unrelenting problem of aviation-based terrorism acutely recognized throughout this thesis, and while this research project offers many pragmatic solutions to the U.S. aviation security quandary, it does not, in any way, purport to address all of the problems and remedies necessary to render the United States completely safe within the

[79] All 19 hijackers were Islamic extremists. In fact, the hijackers involved were chosen because they were "young mujahideen" (9/11 Commission, 2004, p. 234).

[80] The al-Qaeda terrorist group is the widely acknowledged and self-proclaimed organization responsible for the September 11, 2001 hijackings of commercial aircraft and murder of 2,974 individuals.

national air transportation network. To be certain, this research is necessarily limited in scope in order to focus on three key issues within the National Aeronautical Domain, namely: 1) intelligence sharing; 2) risk management and associated methodologies; and 3) the interrelated concept of intelligence-led policing in order to fuse the key issues of one and two together in some structured and consistent manner, at all levels of government, across the United States.

B. LIMITATIONS OF RESEARCH

While this thesis attempts to identify the most critical elements of a more effective aviation security program to better protect this nation and its people, it admittedly does not delve into the complicated and admittedly difficult tasks of actually designing and implementing the intelligence-led, risk-based methodology that is ultimately recommended herein. To be sure, the subject of implementation in simply beyond the scope of this research product. In fact, in the end, this thesis prompts more questions than it answers with respect to both policy implication and field implementation. For example, the following questions arise with regard to actually instituting an intelligence-led, risk-based aviation security doctrine, to wit:

- How does one induce DHS to research and adopt a specific risk assessment methodology for all Category X airport facilities in the United States?
- How does one persuade the U.S. intelligence community to begin sharing more intelligence-based threat assessment information across the intelligence enterprise?
- How does one persuade DHS to begin sharing more intelligence-based threat assessment information with local aviation security managers nationwide?
- How should an adaptation of the intelligence-led policing methodology actually be introduced into the air domain?
- How may individual airport authorities across the NAD contribute to the collection efforts of the USIC?
- Will DHS-TSA sponsor the security clearances of all 27 Category X airport security operators in the United States in order to enhance situational awareness of threats within the domain?

- Beyond Category X aviation facilities, at what point should the recommendations contained in this thesis be implemented throughout the entire U.S. aviation infrastructure, particularly at Category I facilities in the United States?
- What technology is necessary to facilitate an intelligence-led, risk based process across the nation?
- Which types of training would be necessary for local aviation security operators to effectively implement an intelligence-led, risk-based methodology?
- How and to what extent may the international security perspectives documented in this thesis be incorporated into the intelligence-led, risk-based methodology referenced herein?
- How and to what extent does the flying public need to be brought into the homeland security megacommunity that is referenced herein?
- Should either DHS security funding or federal legislation be tied to the mandatory implementation of an intelligence-led, risk-based methodology for all U.S. Category X airports in order to ensure uniformity of process, or application of doctrine?
- Akin to the U.S. Navy's *Naval Doctrine Publication 2*: *Naval Intelligence*, should DHS develop a similar doctrine for U.S. aviation intelligence activities in order to articulate civil aviation intelligence doctrine and provide the foundation for the development of tactics, techniques and procedures within the National Aeronautical Domain?

C. DISCUSSION

The fact that the civil air domain is a critical component of the U.S. and international aviation infrastructure is a truth well known to our nation's adversaries. In fact, worldwide this reality is demonstrated in the following chronology of attacks/attempted attacks on international commercial aviation assets since 2001:

- September 11, 2001 attacks, United States
- Russian aircraft attacks, Russia
- Al-Qaeda aviation plot on London's Canary Wharf District, United Kingdom
- Richard Reid attack (shoe bomber), United Kingdom
- Los Angeles airport plot, United States
- Liquid explosives plot (Operation OVERT), United Kingdom

- JFK airport plot, United States
- Glasgow airport attack, Scotland
- December 25, 2009 aircraft attack, United States
- October 29, 2010 cargo aircraft plot, Yemen/Dubai/United Kingdom

Indeed, it is the recurring persistence of aviation-related terrorist attacks that, in large part, precipitated the U.S. Congress' hearings into these matters in September 2010.

In his written testimony presented to the Full Committee of the U.S. House of Representative's Homeland Security Committee on September 15, 2010, in a hearing entitled *The Evolving Nature of Terrorism: Nine Years after the 9/11 Attacks*, Mr. Peter Bergen, Co-Director of the New America Foundation's Counterterrorism Strategy Initiative, posits: "What kinds of future targets or tactics might jihadist groups attack or use?" Without much surprise, Bergen's number one response to Congress was: "Attacking commercial aviation—***the central nervous system of the global economy*** [emphasis added]—continues to preoccupy al-Qaeda" (Bergen, 2010). Similarly, also providing written testimony before the same Congressional committee, Dr. Bruce Hoffman, Director of the Security Studies Program and a tenured professor at Georgetown University, commented, "Today, America faces a dynamic threat that has diversified to a broad array of attacks, from shootings to car bombs to simultaneous suicide attacks ***to attempted in-flight bombings of passenger aircraft*** [emphasis added]" (Hoffman, 2010). And so, according to these two leading experts in international terrorism, the future challenges facing the national security of the United States generally, and the security of the commercial aviation industry specifically, remain significant. Sadly, however, as pointed out in both Bergman's and Hoffman's testimony, this fact is true even nine years after the 9/11 attacks—a tragedy of the magnitude that proved to be one of those milepost events in the history of the world.

It is against this backdrop of calamity that the inherent and persistent issues relative to the security of the National Aeronautical Domain were identified and examined in this thesis with the intent to somehow stimulate thought and offer real-world possibilities with respect to potential improvements that both the federal and local elements of governments engaged in protecting America's air transportation network could implement. This has been accomplished in this research by revealing that an effective partnership, or true collaboration, between our federal and local governments, in conjunction with the flying public, is actually necessary in order to better protect commercial aviation operations in the United States. Once a real partnership is established—one that is predicated upon real trust and partnership—then both the local and federal governments may work together to address the specific areas related to aviation security that need to be improved. In fact, borrowing from the "security megacommunity" theme already discussed in Chapter VI of this thesis, the pragmatic, real-world improvements noted hereinabove will not possess a viable opportunity for implementation unless collaboration, communication, and cooperation is first established between the federal and local entities responsible for execution of policy in the field. This statement should not be extrapolated to infer that such relationships do not already exist in certain instances; but to be certain, they must exist at all U.S. aviation facilities if the full benefit of these recommendations are to be realized across the entire U.S. aviation network.

D. RECOMMENDATIONS

With respect to the substantive issues relative to security improvements within the U.S. aviation community, this thesis argues, for example, that:

- The federal government must do more to ensure, once and for all, that intelligence-based threat assessment information is shared with local aviation security counterparts on a more regular and comprehensive basis. This simply is not occurring with any consistency at the time of this writing (November 2010). This recommendation is drawn from the cumulative analysis conducted in Chapter VII of this thesis, particularly with regard to the evaluative criteria identified in the Policy Options Matrix data developed vis-à-vis Policy Option 1, to wit: "Improve the Dissemination Element of the Intelligence Cycle within the NAD."[81]
- The federal government must identify and mandate a specific risk-based assessment methodology for local Category X airport operators in the United States. Ironically, although risk assessments are mandated in number of federal guidance documents cited throughout this thesis, risk

[81] See, for example, Chapters I, II and III of this thesis for a detailed discussion regarding this recommendation.

assessment methodologies are neither consistent, nor timely, nor typically comprehensive (if completed at all on the local level) throughout the aviation industry. This recommendation is predicated upon the cumulative analysis of this thesis project as demonstrated in Chapter VII, particularly with regard to the evaluative criteria established in the Policy Options Matrix's overall data developed vis-à-vis Policy Option 2, to wit: "Increase the Frequency of the TSA Threat Assessment Process." In this particular segment of the thesis, the original hypothesis of merely increasing the frequency of the current TSA process was not only discerned to be both superficial and too infrequent, it was also determined that no specific, comprehensive risk-based methodology is currently being utilized that could be replicated by both the TSA as well as airport operators across the United States.[82]

- Local governments that own and operate commercial airport facilities must shed the mindset that the mere enactment of TSA-mandated baseline measures alone are adequate in the overall defense of the national air transportation network. Local units of government must endeavor to do more to enhance aviation security throughout the U.S. aviation network, in conjunction with the federal government, to be certain, but at times must be prepared to lead the way in a reasonable, prudent and responsible manner. This is particularly true with respect to conducting *comprehensive* risk assessments at the nation's commercial aviation facilities. This recommendation emanates from Chapter VII's Policy Options Matrix and the Policy Option 2 hypothesis, which is noted immediately above at recommendation two. Additionally, however, as noted in Chapter II of this research product, federally-regulated Category X airport facility operators possess a legal responsibility to ensure the security of their respective facilities. As such, if the current actions of the federal government are deemed insufficient—and this research respectfully draws that conclusion—then local authorities alone should better ensure public safety by addressing this important issue.[83]

- An active and ongoing partnership between all levels of government and the flying public must be achieved in order to substantively improve the security posture of the National Air Domain. Presently there are no meaningful programs known to this thesis' author/aviation security practitioner that really endeavor to coalesce representatives of government, private business, and the citizenry together in pursuit of heightened aviation security objectives—beyond the "if you see something say something" slogan. This recommendation is drawn from the

[82] See, for example, Chapters I and IV of this thesis for a detailed discussion regarding this recommendation.

[83] See, for example, Chapters I, II, and IV of this thesis for a detailed discussion regarding this recommendation.

discussion in Chapter VI of this thesis wherein the absolute need for collaboration and true partnership within all levels of government, the private sector, and citizens is undertaken in the concept of developing an aviation security megacommunity. This recommendation is also the result of the evaluative criteria established in the Policy Options Matrix data developed vis-à-vis Policy Option 3, to wit: "Institute an Intelligence-driven, Risk-based Security Doctrine." [84]

- In order to achieve these goals, an adaptation of an intelligence-led policing model must be incorporated within the aviation sector's Category X airport security organizations, a policing/ homeland security concept that the federal government should endorse—and somehow induce—across the entire security enterprise of the U.S. aviation domain. The foundation of this recommendation is centered upon the cumulative analysis conducted in Chapter VII of this thesis, particularly with regard to the evaluative criteria established in the Policy Options Matrix data assimilated for Policy Option 3, to wit: "Institute an Intelligence-driven, Risk-based Security Doctrine." As reflected in the aforementioned data and rationale, this particular element of the various recommendations cited herein is absolutely critical because it meshes together the intelligence process, the risk assessment/management process, as well as the organizational culture within which to create a successful aviation security environment. [85]And finally,
- The foreign aviation security services of Israel, Australia, and the United Kingdom should be extensively reviewed because, as evidenced in Chapter V of this thesis, it appears that many of the problems relative to intelligence sharing, risk assessment/mitigation, and interagency security service collaboration within the aviation domain have already been successfully addressed and resolved. This recommendation is predicated upon the comprehensive discussion undertaken in Chapter V of this research product wherein the referenced nations have already addressed the issues regarding U.S. aviation security brought to light herein. Additionally, however, this recommendation is based upon the cumulative analysis of the evaluative criteria established for all three policy options heretofore identified.[86]

[84] See, for example, Chapters V, VI, and VII of this thesis for a detailed discussion regarding this recommendation.

[85] See, for example, Chapters VI and VII of this thesis for a detailed discussion regarding this recommendation.

[86] See, for example, Chapters V and VII of this thesis for a detailed discussion regarding this recommendation.

E. ESTIMATING THE OUTCOMES

This section will consider the estimated outcomes of instituting an intelligence-led policing strategy within the National Aeronautical Domain to: 1) utilize intelligence-based threat assessment information to, 2) merge intelligence information with the threat assessment process to develop a more accurate overall threat picture to then, 3) drive the development of policies and the deployment of physical resources to better protect any given Category X aviation facility. Included in this section as well is the projected benefit of creating a networked aviation security megacommunity (composed of non-traditional security members such as ticket/gate/ramp agents, citizens, etc.) to aid and support the aviation security enterprise.

In *Blue Ocean Strategy*, Kim and Mauborgne (2005) discuss using a strategy canvass as "both a diagnostic and an action framework for building a compelling" plan to address a problem, such as to understand market variables of a particular industry, or to implement a program where many factors must be considered (p. 25). In assessing the recommendations made in this thesis, those interested in improving the U.S. aviation security enterprise possess a responsibility to understand the various elements extant within the environment as they currently exist, as well as understand the likely outcome of those same elements once they have been addressed by the policy options proposed herein. The strategy canvass developed to evaluate this research product is described herein below.

Represented graphically, the following *Eliminate-Reduce-Raise-Create Grid* (E-R2-C Grid) (Figure 6) depicts the essential elements necessary in creating an aviation security megacommunity by use of an intelligence-led policing model. This grid was developed by asking by asking four essential questions necessary to effect change, such as:

- What needs to be eliminated?
- What needs to be raised?
- What needs to be reduced?
- What needs to be created?

With this information answered, a strategy canvas was then created to convey the current state of the U.S. aviation security program, as well as the subsequent intent and expectation, or effect, that the policy options, identified in Chapter VII of this thesis, are expected to yield. In the example shown below, the horizontal axis lists nine elements deemed essential for implementing an improved national aviation security program. Those elements are:

- **TSA Regulatory Compliance** = comportment to federal baseline, or minimum, security mandates.
- **Standard Response Protocols** = common industry practices regarding reactive issues such as responses to access control breaches, etc.
- **Communications** = within and across all of the agencies comprising the local security enterprise.
- **Community Outreach** = the level to which the security enterprise interacts and solicits input from both non-traditional members as well as traditional members within the aviation community.
- **Dynamic Budgeting** = the relative flexibility regarding financial matters that both the federal and local governments possess in responding to unexpected security appropriations within a budget cycle.
- **Security Awareness** = the relative level of consciousness and responsiveness that individuals within the aviation community as a whole possess toward aviation security.
- **Risk-based Assessments** = the degree to which, if any, comprehensive risk-based security assessments are conducted at U.S. Category X aviation facilities.
- **Intelligence Sharing** = the degree to which, if any, that intelligence-based threat assessment information is shared with local security counterparts to influence security policy and field operations.
- **Security Community** = the level to which a sense of responsibility and accountability exists within the aviation environment to ensure or improve security standards.

The vertical axis of the strategy canvass depicts the relative degree to which—from high to low—each listed essential element supports the critical components listed above. The process for rating and plotting each essential element was predicated upon intuition as developed by this research, empirical evidence, and other professional law enforcement experience.

In the strategy canvass (Figure 6) listing the relevant elements of an effective aviation security program, this author estimates the current state of U.S. aviation security in red boxes. On the same high to low scale, this author utilizes blue triangles to estimate the expected state of overall improvement if an intelligent-led policing model is implemented within the air domain security enterprise. Of particular importance, the value proposition elements identify the general areas of aviation security that must be focused upon, and the three value innovation elements identified are those principal factors examined and deemed most important in this thesis. A score of high indicates the estimated efficacy of each critical element listed.

While all of the factors cited for improving the U.S. aviation security environment are estimated to be positively influenced by the recommendations made herein, particular attention should be given to risk-based assessments, intelligence sharing and the creation of a security community, all of which are judged to be significantly improved by the incorporation of the recommendations made herein. In fact, in reviewing this strategy canvass in detail, note that the most critical elements listed under the Value Proposition section are not rated as indicated by the red boxes. This is because these elements do not currently exist in any real, organized, and discernable degree within the NAD at this time.

David S. Williams CHDS 0903
June 16, 2010

ER^{2}C Grid: Improving US Aviation Security by Building a Security Community

Eliminate	**Raise**
Minimalist Security Culture Traditional Service Model	Institutional Security Awareness Public Awareness Political Awareness Customer Service Overall Security Posture
Reduce	**Create**
Contingent Risk	Flexible Countermeasures Institutional Forecasting Security Partnerships

Notes:

Red Ocean Strategy = Traditional Aviation Security Delivery Model
Blue Ocean Strategy = Flexible, responsive aviation security delivery model beyond that which is mandated by TSA

Application of Blue Ocean Strategy Principals:

1. Reconstruct Market Boundaries - Community Outreach
2. Focus on the Big Picture - Reduce Contingent Risks
3. Reach Beyond Existing Demand - Flexible Budgeting
4. Get Strategic Sequence Right - Collaborative Planning and Response
5. Overcome Organizational Hurdles - Cultural Awareness
6. Build Execution Into Strategy - Institutionalization of Security Strategy

Strategy Canvas: Improving US Aviation Security by Building a Security Community

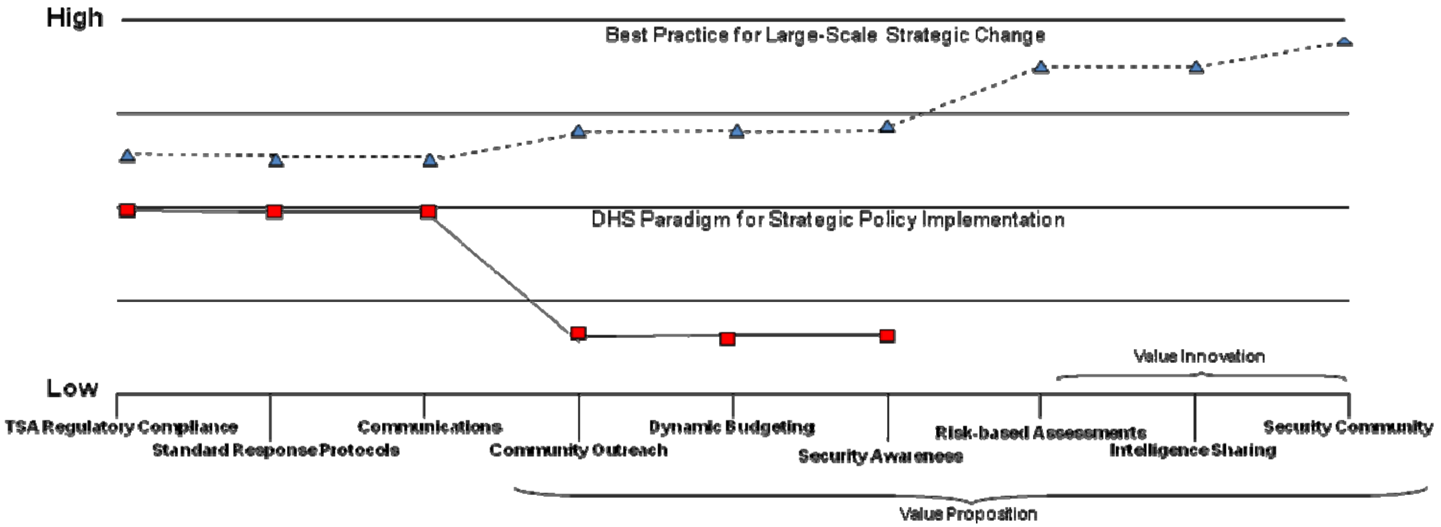

Figure 6. A Strategy Canvass for Improving U.S. Aviation Security

F. CONCLUSION AND PROPOSAL

In conclusion, since the scope of this research is admittedly limited with respect to implementation, the creation of a multi-agency aviation security working group is proposed. This group should be formed by DHS to further evaluate the viability of the recommendations made herein and report the findings to the:

- Secretary of Homeland Security
- Administrator of the Transportation Security Administration
- Attorney General
- Director of the FBI
- National Security Advisor
- Chairman, U.S. House of Representatives Committee on Homeland Security

The composition of this working group should include representatives from the following federal and local agencies, as well as the private sector, and should be co-chaired by representatives from both the federal and local levels of government. Since the utility of the security cooperation model outlined in this thesis may also benefit other entities within the U.S.—mass transit, maritime, and freight transportation industries—consideration should also be given to include members from of those critical infrastructure sectors as well.

The composition of this working group should include, at a minimum, security representatives from the following organizations:

- DHS Office of Intelligence and Analysis
- DHS Office of National Protection and Programs Directorate
- DHS-TSA Office of Intelligence
- DHS-TSA Office of Transportation Threat Assessment and Credentialing
- DHS-TSA Office of Security Operations
- The Federal Bureau of Investigation
- The National Counterterrorism Center
- Airports Council International—North America

- American Association of Airport Executives
- Airport Law Enforcement Agencies Network
- The Airport Security Coordinator from a U.S. Category X Airport
- The International Air Transport Association

In addition to the questions posed in subsection B of this chapter, the following three overarching subject areas, which collectively form the foundation of this entire research product, should be addressed initially by the interagency working group proposed herein:

1. Intelligence Collection and Sharing

- Specifically which type(s) of intelligence products should be shared with local aviation security practitioners?
- How often should intelligence products be shared with local counterparts?
- Who will disseminate intelligence-based threat assessment products to whom?
- What information exists that is not currently being collected by local airport authorities that should be forwarded to the USIC?
- What level of federal security clearance, if any, will be necessary for local aviation security practitioners in order to implement this process?
- What type of information not currently provided by airport authorities could be produced and passed forward to the USIC?
- What type of training will be necessary for both local as well as federal aviation security counterparts across the nation involved in the intelligence collection and dissemination processes?
- What is the relative cost of such an initiative in terms of training and infrastructure development?
- Who will bear the costs for implementing and sustaining this aspect of the program?

2. Risk Assessment Methodology

- Specifically which risk assessment methodology should be selected for the National Aeronautical Domain?
- Once selected, who will conduct comprehensive risk assessments at each of the nation’s Category X airport facilities?

- What type of training will be necessary to ensure that a minimum level of competency and consistency will be achieved once a specific risk assessment methodology is chosen?
- How often should a comprehensive risk assessment be updated at the nation’s Category X airport facilities?
- What are the relative costs for conducting comprehensive risk assessment at the nation’s Category X airport facilities?
- Who will bear the cost for implementing and sustaining this aspect of the program?

3. Introduction of an Intelligence-Led Policing Construct Throughout the NAD to Conjoin the Intelligence and Risk Assessment/Management Processes

- What is the definition of intelligence-led policing as it applies to the National Aeronautical Domain?
- Should the idea of intelligence-led policing with the civil aviation environment be re-named “intelligence-led aviation security”?
- Will the newly defined adaptation of intelligence-led policing be considered the risk management methodology that must be used consistently throughout the National Aeronautical Domain in order merge the subject areas of intelligence and risk assessment together?
- What type of training will be necessary for both local as well as federal partners who are engaged in the process of instituting intelligence-led policing throughout the National Aeronautical Domain?
- What are the relative costs associated with inculcating and sustaining an intelligence-led policing process throughout the National Aviation Domain?
- What are the cultural barriers that will have to be overcome to effectively institute intelligence-led policing throughout the National Aeronautical Domain?
- Should the federal government mandate the implementation of a form of intelligence-led policing to ensure the relative efficacy of security countermeasures deployed across the National Aeronautical Domain?
- In order to create a security megacommunity as discussed in this thesis, how may passengers and other citizens involved in the aviation industry participate and otherwise add value to the process of aviation-specific intelligence-led policing?
- Should one or two of the nation’s Category X airport facilities be chosen to field test the concept of merging intelligence-based threat assessment

> information with a specific comprehensive risk assessment methodology—through and by use of an intelligence-led policing organizational structure?

In summary, as the conclusion to this thesis is being written, the inveterate threats posed to the United States through the vulnerabilities of the National Aeronautical Domain remain starkly obvious as once again evidenced by the October 29, 2010 aviation-borne parcel bomb plot sponsored by al-Qaeda in the Arabian Peninsula. This somber reminder that a creative and committed enemy is seeking to attack the civilian population of this country by the exploitation of civil aviation assets should encourage the leaders of the United States government to immediately consider, and act upon, the common sense policy recommendations contained in this thesis. This call-to-action is particularly relevant now since history reminds us that post-incident counterterrorism policy is oftentimes made in haste—is fraught with the collective emotions of a grieving nation—and as a consequence oftentimes yield poor results. Acting upon the policy recommendations in this thesis now with calm certitude, however, will allow us to better protect ourselves as a people and as a nation, and, most importantly, as a society that recognizes and values the supremacy of the rule of law as dictated by that most sacred document we know as the Constitution of the United States of America.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

9/11 Commission. (2004). *The 9/11 Commission report*: *Final report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton and Company.

About.com. (2010). *Management: Pareto's Principle: The 80–20 rule*. Retrieved November 18, 2010, from http://management.about.com/cs/generalmanagement/a/Pareto081202.htm

Alfano, S. (2006). *War casualties pass 9/11 death toll*. Retrieved November 20, 2010, from http://www.cbsnews.com/stories/2006/09/22/terror/main2035427.shtml

Airports Council International. (2010). *Israel Airports Authority*. Retrieved April 24, 2010, from http://www.airports.org/cda/aci_common/display/main/aci_content07_banners.jsp?zn=aci&cp=1^9812_725_2

Alea Holdings, L.L.C. (2010, August*). INTELOS Airport-Assessment Solutions*. Retrieved November 20, 2010, from http://www.aleaholdings.com/products-airport.html

Answers.com. (2010). *Sir Robert Peel*. Retrieved October 10, 2010, from http://www.answers.com/topic/sir-robert-peel

Australian Civil Aviation Security Authority. (2010). *Designated International Airports in Australia*. Retrieved November 19, 2010, from http://www.infrastructure.gov.au/aviation/international/icao/desig_airports.aspx

Australian Department of Infrastructure, Transport, Regional Development and Regional Government. (2010). *Aviation International airline activity 2009*. Retrieved November 19, 2010, from http://www.bitre.gov.au/publications/04/Files/CY09.pdf

Baker, G. H. (2005). *A vulnerability assessment methodology for critical infrastructure sites.* Retrieved August 18, 2010, from http://works.bepress.com/cgi/viewcontent.cgi?article=1001&context=george_h_baker

Bardach, E. *Part III smart practices research.* Retrieved February 9, 2010, from http://archive.epinet.org/real_media/010111/materials/Bardach.pdf

Bergen, P. (2010). *The evolving nature of terrorism: Nine years after the 9/11 attacks.* Retrieved October 10, 2010, from http://homeland.house.gov/Hearings/index.asp?ID=268

Brafman, O. and Beckstrom, R.A. (2006). *The starfish and the spider: the unstoppable power of leaderless organizations*. New York: Penguin Group.

British Airports Authority (BAA). (2010). *Where We Operate*. Retrieved November 19, 2010, from http://www.baa.com/portal/page/BAA+Airports%5EAbout+BAA%5EWho+we+are%5EWhere+we+operate/794aa2c71124f110VgnVCM10000036821c0a____/448c6a4c7f1b0010VgnVCM200000357e120a___

British Civil Aviation Authority (CAA). (2010). *Main Outputs of Reporting Airports 1981-2009*. Retrieved November 19, 2010, from http://www.caa.co.uk/docs/80/airport_data/2009Annual/Table_02_1_Main_Outputs_Of_UK_Airports_2009.pdf

Carter, D. L. (2004) *Law enforcement intelligence: A guide for state, local, and tribal agencies*. Retrieved October 18, 2009, from http://www.iacti.org/publications/Carter_Intelligence_Guide.pdf

Carter, D. L. (2009). *Law enforcement intelligence: A guide for state, local, and tribal agencies*. Washington, DC: Office of Community Oriented Policing Services, U.S. Department of Justice.

Chertoff, M. (August 13, 2010). *DHS Adjusts Threat Level from Red to Orange For In-Bound Flights from the UK.* Retrieved November 18, 2010, from http://www.dhs.gov/xnews/releases/pr_1156517870332.shtm

Chertoff, M. (November 28, 2006). *Keynote address to the 2006 Grants and Technology Conference*. Washington, DC: Department of Homeland Security. Retrieved August 20, 2010, from http://www.dhs.gov/xnews/speeches/sp_1164738645429.shtm

Clausewitz, K. (1832). *On war: The COMPLETE translation by Colonel J.J. Graham1873*. Retrieved October 18, 2009, from http://www.clausewitz.com/readings/OnWar1873/TOC.htm

Covey, S. M.R. (2006). *The Speed of Trust: The one thing that changes everything*. New York: Free Press.

Debrett's. (2010). *The Right Honorable Sir John Wheeler, JP, DL*. Retrieved October 7, 2010, from http://www.debretts.com/people/biographies/browse/w/4412/John+Daniel.aspx

Federal Bureau of Investigation. (2010). *The Intelligence Cycle*. Retrieved November 18, 2010, from http://www.fbi.gov/about-us/intelligence/intelligence-cycle

Free Dictionary. (2010). *Tripwire*. Retrieved July 25, 2010, from http://www.thefreedictionary.com/tripwire

Government Accounting Office. (1998). *Aviation security: FAA's deployments of equipment to detect traces of explosives* (GAO Report B-281440). Retrieved November 18, 2010, from http://archive.gao.gov/paprpdf2/161456.pdf

Government Accounting Office. (2001). *Homeland security: Key elements of a risk management approach* (GAO -02-150T). Retrieved October 17, 2009, from http://www.gao.gov/new.items/d02150t.pdf

Government Accounting Office. (2001). *Key elements of a risk management approach* (GAO Report 02-150T. Retrieved August 22, 2010, from http://www.gao.gov/new.items/d02150t.pdf

Government Accounting Office. (2004a). *Aviation security: Further steps needed to strengthen the security of commercial airport perimeters and access controls* (GAO Report 04-728). Washington, DC: US General Accounting Office.

Government Accounting Office. (2004b). *Information technology: Major federal networks that support homeland security functions* (GAO Report GAO-04-375). Washington, DC: US Government Printing Office. Retrieved online November 18, 2010 from http://www.gao.gov/new.items/d04375.pdf

Government Accounting Office. (2007). *Applying risk management principles to guide federal investments* (GAO Report 07-386T. Retrieved online August 22, 2010, from http://www.gao.gov/new.items/d07386t.pdf

Government Accounting Office. (2007). *Aviation security: TSA's staffing allocation model is useful for allocating staff among airports, but its assumptions should be systematically reassessed.* (GAO-07-299). Retrieved November 17, 2010, from http://www.gao.gov/new.items/d07299.pdf

Gerencser, M., Lee, R. V., Napolitano, F., and Kelly, C. (2008). *Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together.* New York: Palgrave MacMillan.

Haimes**,** Y. (2002). *Roadmap for Modeling Risks of Terrorism to the Homeland*. Retrieved August 21, 2010, from http://www.healthsystem.virginia.edu/internet/ciag/conference/articles/s2006/haimes_roadmap_for_modeling_risks_of_terrorism.pdf

High Beam Research. (2010, October). *Political Subdivisions*. Retrieved October 7, 2010, from http://www.highbeam.com/doc/1G2-3401803314.html

Hoffman, B. (2010). *The evolving nature of terrorism: Nine years after the 9/11 attacks, hearings before the full House Committee on Homeland Security*. Retrieved October 10, 2010, from http://homeland.house.gov/Hearings/index.asp?ID=268

Houston Airport System. (2010). *History of HAS*. Retrieved online November 18, 2010, from http://www.fly2houston.com/aboutHistory

Israel Airports Authority. (2010). *Facts and Figures*. Retrieved April 24, 2010, from http://www.iaa.gov.il/Rashat/en-US/Airports/BenGurion/AbouttheAirport/Statistics/

Israel Security Agency. (2010a). *Frequently Asked Questions*. Retrieved November 19, 2010, from http://www.shabak.gov.il/English/about/FAQ/faq2/Pages/default.aspx

Israel Security Agency. (2010b). *Information Systems and Technology*. Retrieved November 19, 2010, from http://www.shabak.gov.il/english/information%20systems%20and%20technology/technology/pages/default.aspx

Jenkins, B. D. (1998*). Security risk analysis and management—Risk analysis helps establish a good security posture; Risk management keeps it that way*.” Retrieved August 21, 2010, from http://www.nr.no/~abie/RA_by_Jenkins.pdf

Joint Security Commission. (2004) *Redefining security*. Retrieved October 17, 2009, from http://www.fas.org/sgp/library/jsc/index.html

Jones, P. and Edmunds, Y.(2008). *Risk-based strategies for allocating resources in a constrained environment*. Retrieved August 22, 2010, from http://www.homelandsecurity.org/journal/Default.aspx?oid=171&ocat=1

Kelling, G. L. & Moore, M. H. (1988). *The evolving strategy of policing*. Retrieved October 10, 2010, from http://www.ncjrs.gov/pdffiles1/nij/114213.pdf

Kim, W. C. & Mauborgne, R. (2005). *Blue ocean strategy: How to create uncontested market space and make the competition irrelevant*. Boston, MA: Harvard Business School Press.

Lewis, T. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. Hoboken, NJ: John Wiley & Sons, Inc.

Looney, R. L. (2002). *Economic costs to the United States stemming from the 9/11 attacks*. Retrieved January 26, 2010, from http://www.hsdl.org/homesec/docs/dod/economiccosts.pdf&code=802b3b9a6d0f1db1048ac8c87bfbd466

McNamara, T. (2009). *Information sharing environment plans and progress: Annual report to Congress*. Retrieved September 11, 2010, from http://www.fas.org/irp/agency/ise/2009report.pdf

Mineta, N. (2003). *9/11 Commission testimony of Secretary of Transportation Norman Y. Mineta on May 23, 2003*. Retrieved on April 10, 2010, from http://www.9-11commission.gov/archive/hearing2/9-11Commission_Hearing_2003-05-23.htm

NI2 Center for Infrastructure Expertise. (2009). *CARVER2®*. Retrieved October 18, 2009, from http://www.ni2cie.org/CARVER2.asp

Operations Research: The Science of Better®. (2010). *The Edelman Award*. Retrieved August 21, 2010, from http://www.scienceofbetter.org/Edelman/about.htm

Peed, C. R. (2008). *The community policing umbrella*. Retrieved October 10, 2010, from http://findarticles.com/p/articles/mi_m2194/is_11_77/ai_n31058455/

Raffel, R. R. (2007). *Intelligence in homeland security*. Retrieved November 18, 2010, from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol50no3/airport_security_5.htm

Ratcliffe, J. H. (2008). *Intelligence-led policing*. Retrieved October 19, 2009, from http://www.amazon.com/Intelligence-Led-Policing-Jerry-H-Ratcliffe/dp/1843923394#reader_1843923394

Reid, J. (2006). *Airline terror plot foiled in UK soon before planned bombings*. Retrieved April 10, 2010, from http://www.pbs.org/newshour/bb/terrorism/july-dec06/itn_08-10.html

Ron, R. (2002). *Congressional Testimony of February 27, 2002*. Retrieved October 7, 2010, from https://www.hsdl.org/?view&doc=7663&coll=limited

Sandia National Laboratories. (2009). *Security risk management methodologies.* Retrieved October 17, 2009, from http://www.sandia.gov/mission/homeland/solutions/critical/risk.html

Schneier, B. (2009). *Airport security: Is aviation security mostly for show?* Retrieved September 11, 2010, from http://articles.cnn.com/2009-12-29/opinion/schneier.air.travel.security.theater_1_terrorists-aviation-security-airport-security?_s=PM:OPINION

Sun Tzu. (n.d.). *The art of war*. Retrieved September. 14, 2010, from http://www.brainyquote.com/quotes/authors/s/sun_tzu.html

Tucker, J.B. (2003). *Strategies for countering terrorism: Lessons from the Israeli experience*. Retrieved May 31, 2010, from: https://www.hsdl.org/?view&doc=19996&coll=documents

U. K. Office of the Home Secretary. (2010). *The United Kingdom's strategy for countering international terrorism*. Retrieved October 7, 2010, from http://www.official-documents.gov.uk/document/cm78/7833/7833.pdf

U.K. Parliamentary Office of Science and Technology. (2002). *Postnote: CCTV*. Retrieved November 19, 2010, from http://www.parliament.uk/documents/post/pn175.pdf

U.S. Congress. (2002) *Homeland Security Act of 2002*. Retrieved November 20, 2010, from http://www.dhs.gov/xlibrary/assets/hr_5005_enr.pdf

U.S. Congress. (2004). *Intelligence Reform and Terrorism Prevention Act of 2004*. Retrieved July 18, 2009, from http://www.nctc.gov/docs/pl108_458.pdf

U.S. Department of Defense. (2006). *The national strategy for the physical protection of critical infrastructure and key assets*. Retrieved August 18, 2010, from http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf

U.S. Department of Homeland Security. (2007a). *Air domain surveillance and intelligence integration plan.* Retrieved October 19, 2010, from http://www.DHS.gov/xlibrary/assets/hspd16_domsurvintelplan.pdf

U.S. Department of Homeland Security. (2007b*). National strategy for aviation security*. Retrieved October 17, 2009, from http://www.DHS.gov/xlibrary/assets/laws_hspd_aviation_security.pdf

U.S. Department of Homeland Security. (2007c). *Transportation systems critical infrastructure and key resources sector-specific plan.* Retrieved October 18, 2009, from http://www.TSA.gov/assets/pdf/transportation_base_plan_appendixes.pdf

U.S. Department of Homeland Security. (2009). *National infrastructure protection plan*. Retrieved on October 17, 2009, from http://www.DHS.gov/files/programs/editorial_0827.shtm

U.S. Department of Homeland Security. (2010). *Homeland security advisory system.* Retrieved November 18, 2010, from http://www.dhs.gov/files/programs/Copy_of_press_release_0046.shtm

U.S. Department of Justice. (2009). *Community policing defined*. Retrieved January 24, 2010, from http://www.cops.usdoj.gov/files/RIC/Publications/e030917193-CP-Defined.pdf

U.S. Department of Justice. (2009). *Navigating your agency's path to intelligence-led policing*. Retrieved November 19, 2009, from http://www.rodgersgroupllc.com/Navigating_Your_Agencys_Path.pdf

U.S. Office of the Director of National Intelligence. (2008). *Information sharing strategy*. Retrieved November 18, 2010, from http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf

U.S. Navy. (n.d.). *Naval doctrine publication 2*: *Naval intelligence.* Retrieved October 17, 2010, from http://www.dtic.mil/doctrine/jel/service_pubs/ndp2.pdf

U.S. Sandia National Laboratory. (2010). *Sandia National Labs' security risk assessment methodologies*. Retrieved August 20, 2010, from http://www.sandia.gov/ram/RAM%20Overview%20%20Presentation%20Aug%2006.pdf

U.S. Department of Transportation (DOT) - Bureau of Transportation Statistics. (2009). *Air Traffic Hubs 2009.* Retrieved November 17, 2010, from http://www.bts.gov/programs/geographic_information_services/maps/hub_maps/2009/html/map.html

U.S. Department of Transportation & Bureau of Transportation Statistics. (2010). *Passengers: All Carriers, All Airports.* Retrieved April 5, 2010, from http://www.transtats.bts.gov/Data_Elements.aspx?Data=1

Wells, A. T. (2000). *Airport planning and management* (4th ed.). New York: McGraw-Hill Companies.

Wells, A. T. and Young, S. B. (2004). *Airport planning and management* (5th ed.). New York: McGraw-Hill Companies.

Wheeler, J. (2005). *An Independent Review of Airport Security and Policing for the Government of Australia*. Retrieved October 7, 2010, from http://www.customs.gov.au/webdata/resources/files/SecurityPolicingReview.pdf

White House. (1990). *Findings and recommendations of the 1989 commission on aviation security and terrorism*. Retrieved November 19, 2010, from http://www.globalsecurity.org/security/library/congress/1990_cr/s900511-terror.htm

White House. (1994). *Presidential decision directive 29: Security policy coordination.* Retrieved October 17, 2009, from http://www.fas.org/sgp/spb/jscrept.html

White House. (1997). *1996 White House Commission on aviation safety and security: Final report to President Clinton*. Retrieved November 21, 2010, from http://www.fas.org/irp/threat/212fin~1.html

White House. (1998). *Presidential Decision Directive/NSC-63: Critical infrastructure protection.* Retrieved August 21, 2010, from http://www.fas.org/irp/offdocs/pdd/pdd-63.htm

White House. (2003a). *Homeland security presidential directive 7: Directive on critical infrastructure identification, prioritization and protection.* Retrieved October 18, 2009, from http://www.DHS.gov/xabout/laws/gc_1214597989952.shtm

White House. (2003b). *Homeland security presidential directive 8: National preparedness.* Retrieved October 18, 2009, from http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm#1

White House. (2005). *Guidelines and requirements in support of the Information Sharing Environment*. Retrieved September 11, 2010, from http://www.fas.org/sgp/news/2005/12/wh121605-memo.html

White House. (2006). *National security presidential directive 47/homeland security presidential directive 16: Aviation security policy.* Retrieved October 18, 2009, from http://www.DHS.gov/files/laws/gc_1173113497603.shtm

White House. (2008). *Further amendments to executive order 12333, United States Intelligence Activities*. Retrieved September 11, 2010, from http://www.fas.org/irp/offdocs/eo/eo-13470.htm

White House. (2009). *Executive order: Classified national security information*. Retrieved September 11, 2010, from http://www.whitehouse.gov/the-press-office/executive-order-classified-national-security-information

White House. (2010). *White House review summary regarding 12/25/2009 Attempted terrorist attack*. Retrieved November 19, 2010, from http://www.whitehouse.gov/the-press-office/white-house-review-summary-regarding-12252009-attempted-terrorist-attack

Word IQ. (2010, August).*Wicked problems*. Retrieved online August 22, 2010 from http://www.wordiq.com/definition/Wicked_problems

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California