



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**INCREASING EFFECTIVENESS AND EFFICIENCY
THROUGH RISK-BASED DEPLOYMENTS**

by

Thomas Randolph Cotten IV

December 2015

Thesis Co-Advisors:

Kathleen Kiernan
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			<i>Form Approved OMB No. 0704-0188</i>	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington, DC 20503.				
1. AGENCY USE ONLY <i>(Leave blank)</i>		2. REPORT DATE December 2015	3. REPORT TYPE AND DATES COVERED Master's thesis	
4. TITLE AND SUBTITLE INCREASING EFFECTIVENESS AND EFFICIENCY THROUGH RISK-BASED DEPLOYMENTS			5. FUNDING NUMBERS	
6. AUTHOR(S) Thomas Randolph Cotten IV				
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 (maximum 200 words) Over the past several years, the Transportation Security Administration (TSA) has begun shifting away from a "one-size-fits-all" approach to security and toward one predicated upon risk-based security principles. The TSA has also been called upon by the Government Accountability Office and U.S. Department of Homeland Security Office of Inspector General to make risk-based decisions regarding the allocation and deployment of its resources. This thesis established an initial strategic framework with which to evaluate possible options and applied this framework to explore three possible paths forward. The first path was maintaining the current approach to resource deployments. The second path was the collection and analysis of various data points in order to understand the risk environment. The third path was the use of Bayesian game-theory to model adversarial actions. With the framework applied, the use of Bayesian game-theory was identified as the most beneficial to TSA in comparison to the other two assessed options. Strategic recommendations are also provided based upon research into the experiences of other entities with risk-based deployment methodologies.				
14. SUBJECT TERMS aviation security, Transportation Security Administration, risk-based security, resource deployment, game theory, big data			15. NUMBER OF PAGES 77	
			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

Approved for public release; distribution is unlimited

**INCREASING EFFECTIVENESS AND EFFICIENCY THROUGH RISK-BASED
DEPLOYMENTS**

Thomas Randolph Cotten IV
Supervisory Program Analyst, Transportation Security Administration, Arlington, VA
B.S., North Carolina State University, 2006
B.A., North Carolina State University 2007

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 2015**

Approved by: Kathleen Kiernan
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Erik Dahl
Associate Chair of Instruction
Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Over the past several years, the Transportation Security Administration (TSA) has begun shifting away from a “one-size-fits-all” approach to security and toward one predicated upon risk-based security principles. The TSA has also been called upon by the Government Accountability Office and U.S. Department of Homeland Security Office of Inspector General to make risk-based decisions regarding the allocation and deployment of its resources.

This thesis established an initial strategic framework with which to evaluate possible options and applied this framework to explore three possible paths forward. The first path was maintaining the current approach to resource deployments. The second path was the collection and analysis of various data points in order to understand the risk environment. The third path was the use of Bayesian game-theory to model adversarial actions.

With the framework applied, the use of Bayesian game-theory was identified as the most beneficial to TSA in comparison to the other two assessed options. Strategic recommendations are also provided based upon research into the experiences of other entities with risk-based deployment methodologies.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	BACKGROUND	1
B.	PROBLEM STATEMENT	2
C.	RESEARCH QUESTIONS	3
1.	Primary Research Question	3
2.	Secondary Research Questions	3
D.	ARGUMENT	3
E.	SIGNIFICANCE OF RESEARCH	4
F.	POLICY OPTIONS ANALYSIS	5
G.	EVALUATIVE CRITERIA	6
1.	Security Effectiveness	6
2.	System Efficiency	6
3.	Risk Mitigation.....	7
a.	<i>Constitutional Considerations</i>	7
b.	<i>Social Acceptance</i>	8
4.	Political Feasibility.....	8
II.	HISTORY AND BACKGROUND	9
A.	RISK-BASED DEPLOYMENT METHODOLOGIES IN TSA.....	9
B.	RISK-BASED DEPLOYMENT METHODOLOGIES IN BUSINESS	12
C.	RISK-BASED DEPLOYMENT METHODOLOGIES IN LAW ENFORCEMENT AND SECURITY	13
III.	RISK-BASED DEPLOYMENT MODELS CURRENTLY IN-USE IN SECURITY SETTINGS.....	15
A.	CURRENT DATA-DRIVEN RISK-BASED DEPLOYMENT MODELS	15
1.	DDACTS	15
2.	RTM	17
3.	PredPol.....	19
B.	CURRENT BAYESIAN GAME THEORY RISK-BASED DEPLOYMENT MODELS.....	21
1.	Bayesian Game Theory.....	21
2.	Applications of Bayesian Game Theory in Homeland Security	23
C.	INHERENT CHALLENGES	25
1.	Defining Risk	25
2.	Establishing Inputs	25

3.	Useful Products	26
4.	Measuring Effectiveness	27
5.	Protecting Civil Rights and Liberties.....	27
IV.	POLICY EVALUATION	29
A.	OPTION A—MAINTAIN CURRENT RESOURCE DEPLOYMENT STRATEGY	29
1.	Security Effectiveness	30
2.	System Efficiency	31
3.	Constitutional Considerations	32
4.	Social Considerations.....	32
5.	Political Feasibility	34
B.	OPTION B—ADAPT AN EXISTING DATA-DRIVEN RISK- BASED DEPLOYMENT METHODOLOGY	34
1.	Security Effectiveness	35
2.	System Efficiency	37
3.	Constitutional Considerations	37
4.	Social Considerations.....	39
5.	Political Feasibility	40
C.	OPTION C—INVEST IN THE DEVELOPMENT OF A BAYESIAN GAME THEORY RISK-BASED DEPLOYMENT METHODOLOGY	41
1.	Security Effectiveness	41
2.	System Efficiency	43
3.	Constitutional Considerations	44
4.	Social Considerations.....	44
5.	Political Feasibility	44
V.	FINDINGS, RECOMMENDATIONS, AND CONCLUSION	45
A.	FINDINGS	45
B.	RECOMMENDATIONS.....	45
1.	Work with Stakeholders (Particularly the General Public)	46
2.	Mitigate Personnel Concerns and Prevent Overreliance	46
3.	Maintain Unpredictable Security	47
4.	Focus on Effectiveness, Then Efficiency	48
C.	CONCLUSION	48
	LIST OF REFERENCES	49
	INITIAL DISTRIBUTION LIST	57

LIST OF FIGURES

Figure 1.	Sample Risk Terrain Model Map.....	18
Figure 2.	Sample PredPol Map.....	20

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1.	Known Prohibited Item Encounter Rate.....	31
Table 2.	Passengers and Baggage Screened per FTE	31
Table 3.	Public Opinion of TSA PreCheck Vetting Measures	33
Table 4.	Policy Option Analysis Findings	45

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

AIT	advanced imaging technology
BDO	behavior detection officer
CATA	civil aviation threat assessment
CHDS	Center for Homeland Defense and Security
COTS	commercially available off-the-shelf
CREATE	Center for Risk and Economic Analysis of Terrorism Events
DDACTS	data-driven approaches to crime and traffic safety
DHS	Department of Homeland Security
DUI	driving under the influence
FAMS	Federal Air Marshal Service
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FTE	full-time equivalent
FYXX	fiscal year XXXX
GAO	Government Accountability Office
GIS	geographic information systems
GUARDS	game-theoretic unpredictable and randomly deployed security
IRIS	intelligent randomization in scheduling
IRTPA	Intelligence Reform and Terrorism Prevention Act
OIG	Office of Inspector General
PII	personally identifiable information
PROTECT	Port Resilience Operational/Tactical Enforcement to Combat Terrorism
PSC	passenger screening canine
RTM	risk terrain modeling
SPOT	screening of passengers by observation techniques
TSA	Transportation Security Administration
TSO	transportation security officer
UCLA	University of California Los Angeles
UCR	uniform crime reporting
USCG	United States Coast Guard
VIPR	visible intermodal prevention and response

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

Over the past several years, the U.S. Transportation Security Administration (TSA) has begun shifting away from a “one-size-fit-all” approach to security and towards risk-based security principles “based on the understanding that the vast majority of people traveling pose little to no threat to aviation.”¹

The TSA has the opportunity to continue this evolution, and address calls from the Government Accountability Office (GAO) and the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) to make risk-based decisions regarding the allocation and deployment of its resources, by investing in the development and refinement of a more tactical-level risk-based deployment methodology. Such a methodology can be thought of as an attempt to ensure that *the right resources are at the right location at the right time to buy-down the greatest amount of risk.*

This thesis first proposes a framework for evaluating the use of various risk-based methodologies in the aviation security domain. The primary criteria of this framework are overall impacts to security effectiveness and system efficiency, as a successful risk-based deployment methodology should lead to an increase in both. The secondary criteria of this framework are compliance with the U.S. Constitution, likelihood of societal acceptance, and general political feasibility.

With a framework established, three possible paths forward were proposed and assessed to determine which would yield the greatest likelihood of a positive outcome. The first path is maintaining the current approach towards resource deployment. At present, TSA as an enterprise lacks a standardized tactical-level risk-based deployment methodology for its assets and tends to instead rely upon a combination of individual subject matter expertise and the occasional program-specific approach. The second path is the adoption of a data-driven approach, similar to the use of existing tools, such as

¹ “Risk-based Security: What This Means for You.” August 7, 2014, <http://www.tsa.gov/pressroom-channel/risk-based-security-what-means-you>.

PredPol and risk terrain modeling by law enforcement agencies. The third path is the adoption of a methodology based in Bayesian game theory.

Using the framework, the use of Bayesian game theory was identified as the most advantageous to TSA in comparison to the other two assessed options. Among the benefits of this approach is that it is one with which the agency already possesses some knowledge of through its development of two such models, intelligent randomization in scheduling (IRIS) and game-theoretic unpredictable and randomly deployed security (GUARDS). This thesis also offers several strategic recommendations based upon research into the experiences of other entities with risk-based deployment methodologies.

ACKNOWLEDGMENTS

This thesis is dedicated to my best friend, and now wonderful wife, Betsy. Her encouragement and understanding throughout my participation in the program has made a world of difference, and for that I am grateful.

I am also grateful for the love and support of my family and friends throughout this journey. Your understanding when I had to slip away over holidays or bow out of invitations was much appreciated.

I would like to thank the Transportation Security Administration for affording me the opportunity to participate in this program. A special thanks to Melanie Harvey, Sarah Tauber, Mike Silata, and the “nerd herd” for your support while I traveled for school and for your constant inspiration.

To my classmates, it is difficult to put into words the impact that each of you has had on me over the past year and a half. Whether it was a healthy debate in class, reading your posts online, or a late-night discussion in the lobby of the hotel, I always walked away from our interactions having learned something new and greatly appreciate having had the opportunity to get to know you.

To my advisors, Kathleen Kiernan and John Rollins, thank you for coaching me throughout this process. Your feedback and insight have been invaluable and have helped make me a better writer and researcher.

Lastly, I would like to thank the faculty and staff of the Center for Homeland Defense and Security at the Naval Postgraduate School. The experience has been life-changing and it is an honor to have been part of such a great tradition.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The Transportation Security Administration (TSA) is charged with “protect[ing] the Nation’s transportation systems to ensure freedom of movement for people and commerce.”¹ In the realm of aviation security, which will serve as the primary focus of this thesis, “Transportation Security Officers [TSOs] screened approximately 650 million passengers and more than two billion carry-on and checked bags, preventing approximately 105,000 dangerous prohibited items, including 2,300 firearms, from being carried onto planes” in Fiscal Year 2014 (FY14) alone.²

A. BACKGROUND

To execute its mission, TSA employs nearly 50,000 TSOs, 700 aviation transportation security inspectors, 800 canine teams, 700 advanced imaging technology (AIT) machines, and many other resources to include a classified number of Federal Air Marshals (FAMS).³ By simply examining the number of passengers that each canine team would need to screen each year for 100% coverage, for example, the complexity of executing TSA’s expansive mission with its relatively limited resources quickly becomes apparent.

It is important to note that the challenge of optimizing resource deployment is certainly not unique to TSA, as agencies in both the public and private sectors commonly struggle with similar circumstances. However, many of these same entities have successfully developed and implemented frameworks and methodologies designed to help support important decisions, such as where to deploy resources to realize the greatest returns.

¹ “Mission,” July 23, 2014, <http://www.tsa.gov/about-tsa/mission>.

² U.S. Transportation Security Administration, *Transportation Security: Are Our Airports Safe?* (Washington, DC: U.S. Transportation Security Administration, 2015), http://www.tsa.gov/sites/default/files/assets/pdf/tsa_testimony5-13-15.pdf.

³ U.S. Transportation Security Administration, *TSA by the Numbers* (Washington, DC: U.S. Transportation Security Administration, 2015), http://www.tsa.gov/sites/default/files/publications/pdf/tsabythenumbers_final.pdf.

B. PROBLEM STATEMENT

Over the past several years, TSA has been shifting away from a “one-size-fits-all” approach to security and towards risk-based security principles “based on the understanding that the vast majority of people traveling pose little to no threat to aviation.”⁴ While this approach has certainly had an impact on the interactions between the traveling public and the agency, it has also spurred changes within the agency itself including continued refinements in the strategic risk-based allocation of its resources at the operational (i.e., national) level.

TSA has the opportunity to continue this evolution, and address calls from the Government Accountability Office (GAO) and the U.S. Department of Homeland Security (DHS) Office of Inspector General (OIG) to make risk-based decisions regarding the allocation and deployment of its resources, by investing in the development and refinement of a more tactical-level risk-based deployment methodology. Such a methodology can be thought of as an attempt to ensure that *the right resources are at the right location at the right time to buy-down the greatest amount of risk.*

Through the following research, the author hopes to begin to identify and address some of the questions that TSA would need to consider should the determination be made to pursue such a methodology actively. How is “risk” defined? How will “effectiveness” and “efficiency” be measured? Have other organizations undertaken similar projects, and if so, what was the outcome? Are there legal concerns? Are there public policy concerns? How will the methodology accommodate new information?

Lastly, the author presents three possible paths forward with the goal of demonstrating the viability, or lack thereof, of a tactical-level risk-based deployment methodology.

⁴ “Risk-Based Security: What This Means for You,” August 7, 2014, <http://www.tsa.gov/pressroom-channel/risk-based-security-what-means-you>.

C. RESEARCH QUESTIONS

This thesis attempts to answer the following research questions.

1. Primary Research Question

How can TSA use a risk-based deployment methodology to deploy its resources in an effort to increase security effectiveness and system efficiency?

2. Secondary Research Questions

- How could risk be defined and how could it be measured?
- How could security effectiveness be defined and how could it be measured?
- How could system efficiency be defined and how could it be measured?
- Do any risk-based deployment models currently exist that could be studied?
- What legal, social, and political concerns might inhibit the adoption of a different model for resource deployment in the aviation security domain?

D. ARGUMENT

The primary argument for adopting a tactical-level risk-based deployment methodology is quite simple, why would an entity not use readily available information, or that could be easily collected to optimize the deployment of its limited resources?

When exploring companies in the private sector, for example, those that are successful understand the importance of being at the right place at the right time, which is why retailers work hard to be located near and available for their target demographic. While unique challenges certainly arise that come along with operating in the public sector versus private industry, they can be (and oftentimes are) overcome. A prime example is the ability for a private company to hire, transfer, and occasionally, lay off, individuals at-will in response to the ebbs and flows of the business world. TSA has a similar ability to shift resources through programs, such as the National Deployment

Force, which is designed in part to surge “personnel in support of screening requirements that exceed airport staffing levels.”⁵

The second argument for adopting an enterprise approach towards tactical-level risk-based deployment methodology is that the information that serves as the underpinning can be shared with others, both within and outside of TSA, to enhance everyone’s understanding of the risk environment. As a recent study on the sharing of spatial information (e.g., home addresses) amongst sub-national government entities noted, the data that emergency responders need to make informed decisions rarely exists in a single place.⁶ While certainly considered to be problematic, it is also an issue that can be overcome through something as simple as a data-sharing initiative. That said, it is important for willing entities to recognize and overcome the “organisational/institutional issues, technical and technological issues, economic factors, legal considerations and political issues” that oftentimes complicate the sharing of information.⁷

E. SIGNIFICANCE OF RESEARCH

TSA will likely continue to face a paradoxical scrutiny of its operations, to include the allocation of personnel and equipment, in the absence of a significant incident that simultaneously validates the need for security the agency provides while calling into question the effectiveness of its current approach. In other words, a possibility exists that the agency will face budget cuts moving into the future until such a time that the cuts directly jeopardize its ability to execute its mission successfully. With this understanding, and the shift towards risk-based security already underway, TSA can benefit from the adoption a methodology that will facilitate the effective and efficient deployment of its increasingly limited resources.

⁵ U.S. Department of Homeland Security Office of Inspector General, *TSA’s National Deployment Force–FY 2012 Follow-Up* (Washington, DC: U.S. Department of Homeland Security Office of Inspector General, 2012), 201, https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-14_Dec12.pdf.

⁶ Kevin McDougall, “A Local-State Government Spatial Data Sharing Partnership Model to Facilitate SDI Development” (Ph.D. diss., The University of Melbourne, 2006), http://www.csdila.unimelb.edu.au/publication/theses/Kevin_Mcdougall_PhD_Thesis.pdf.

⁷ *Ibid.*

At present, research exists regarding the use of risk-based deployment methodologies in fields ranging from private sector retail outlet site selection to law enforcement activities in major cities. However, little research exists regarding their application in the aviation security domain and this thesis seeks to begin the process of filling this gap and initiate further academic discussion on the topic.

Lastly, effectiveness and efficiency are oft-cited nebulous terms whose meaning is generally implicitly understood while simultaneously difficult to define in absolute terms. For example, during the 113th Congress, the U.S. Senate Committee on Homeland Security and Governmental Affairs previously established the Subcommittee on the Efficiency and Effectiveness of Federal Programs and the Federal Workforce. This subcommittee was charged with “oversee[ing] the management, efficiency, effectiveness, and economy of all agencies and departments in the federal government” without ever truly defining how these principles could be applied across a diverse landscape like the entirety of the federal bureaucracy.⁸

Understanding that effectiveness and efficiency are two very important principles, particularly within the federal government, this thesis seeks to establish a working framework that will allow readers to understand their meaning with regards to the deployment of aviation security assets and make informed decisions.

F. POLICY OPTIONS ANALYSIS

Like most entities, both public and private, TSA faces the challenge of determining how to best invest constrained resources to accomplish its overarching mission, which in the case of TSA, is “protect[ing] the Nation’s transportation systems to ensure freedom of movement for people and commerce.”⁹ While this mission, not unlike those of most organizations, is fairly straightforward, the complexity quickly comes into focus when the size of this nation’s transportation systems relative to number of assets available to help protect it is considered.

⁸ “About Efficiency and Effectiveness of Federal Programs and the Federal Workforce,” accessed July 29, 2015, <http://www.hsgac.senate.gov/subcommittees/fp/w/about>.

⁹ “Mission.”

In such an environment, any opportunity to increase the effectiveness and efficiency of deployed resources sounds ideal; however, careful deliberation must be given to the facts and circumstances surrounding each of the options presented to help ensure a positive outcome. Given that little scientific research exists on the use of risk-based deployment methodologies in the aviation security domain relative to other domains, such as law enforcement, a policy options analysis allows for the exploration and assessment of opportunities in this emerging field.

G. EVALUATIVE CRITERIA

To assess each of the policy options equally, the following criteria have been established as a baseline for comparison.

1. Security Effectiveness

As a measureable increase in security effectiveness is the first output of the primary research question, a working definition must be established. For the purposes of this research, this definition draws upon the mission of TSA and is understood as *the likelihood of a provided policy to holistically protect a provided transportation system*.

While this definition could certainly be considered overly broad, it is also scalable and makes it possible to explore a transportation system at a relatively micro-level (e.g., airports) or macro-level (e.g., aviation systems). Additionally, this definition allows for the entirety of a given ecosystem, such as the public and sterile (to include aircraft) areas of an airport, to be considered. This concept is particularly important, as it is highly unlikely that any given system will always have sufficient resources to carry out its mission. As such, the deployment of resources to one particular area will likely deprive another of their protective capabilities, if not at least temporarily.

2. System Efficiency

Increased system efficiency is the second expected output of a successful risk-based deployment methodology. For the purposes of this research, system efficiency will be understood as “maintaining federal government services or outcomes using fewer

resources (such as time and money) or improving or increasing the quality or quantity of services or outcomes while maintaining (or reducing) resources.”¹⁰

This definition is borrowed from a 2011 GAO report titled *Streamlining Government—Key Practices from Select Efficiency Initiatives Should Be Shared Governmentwide*. The benefit of using this definition is that it has been previously cited by the U.S. government’s primary audit agency in its own independent study on the topic, thereby lending credibility in the event of scrutiny.

3. Risk Mitigation

While increasing security effectiveness and system efficiency should be the primary objectives of a risk-based deployment methodology, their execution must be carefully balanced with many other factors. Among these considerations are compliance with the U.S. Constitution, likelihood of social acceptance, and general political feasibility.

a. Constitutional Considerations

The U.S. Constitution is the primary cornerstone for laws the United States and compliance with the principles it establishes is non-negotiable. While all laws are based, in some form or fashion, in the U.S. Constitution, the Fourth and Fifth Amendments are of particular importance with regards to a risk-based deployment methodology. As such, the following questions are considered for the purposes of this research:

- Does the proposed option violate “the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” as established in the Fourth Amendment of the U.S. Constitution?¹¹

¹⁰ U.S. Government Accountability Office, *Streamlining Government—Key Practices from Select Efficiency Initiatives Should Be Shared Governmentwide* (GAO-11-908) (Washington, DC: Government Accountability Office, 2011), <http://www.gao.gov/assets/590/585552.pdf>.

¹¹ “The Constitution of the United States, Amendment IV,” accessed June 6, 2015, http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

- Does the proposed option deprive individuals of “life, liberty, or property, without due process of law,” as established in the Fifth Amendment of the U.S. Constitution?¹²

b. Social Acceptance

With nearly two million encounters with the traveling public each and every day in the aviation domain alone, it is vitally important TSA adopt a strategy that considers the opinions of those it serves and protects.¹³ It is particularly important when stopping to consider recent polling that indicates nearly half (46%) of respondents felt TSA was doing an “only fair” or “poor” job compared to a rating of “pretty good” or “excellent.”¹⁴

- What is the anticipated impact to travel time? Will the option reduce overall travel time or increase it?
- What is the anticipated impact to individual screening scrutiny? Will the option reduce screening scrutiny or increase it?
- If information regarding individual travel will be used, how will it be used and how will it be protected?

4. Political Feasibility

Like many federal agencies, TSA relies heavily upon funding allocated by the U.S. Congress and approved by the President. As such, it is important to consider the likely questions from these important stakeholders.

- Is the option in-line with the established mission of the agency?
- What is the anticipated impact to allocated resources? Can the current resources allocated be reduced or will additional resources be required?

¹² “The Constitution of the United States, Amendment V,” accessed June 6, 2015, http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.

¹³ “TSA by the Numbers.”

¹⁴ Larry Shannon-Missal, “Harris Interactive: Harris Polls > U.S. Mint & FAA Receive Highest Ratings of 17 Government Agencies; FBI, CDC, NIH, CIA and Office of the Surgeon General Also Well Regarded,” *The Harris Poll*, February 26, 2015, <http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/1557/Default.aspx>.

II. HISTORY AND BACKGROUND

It is important to note that the underlying concept of using information to ensure that an organization has the right people at the right place at the right time, or for the purposes of thesis called a resource deployment methodology, is certainly not novel. The necessity of information has long been recognized as a key ingredient to strategic decision making, particularly in the field of security. As the fabled Chinese military strategist Sun Tzu noted in his 6th century BC work, *The Art of War*, “if you know your enemies and know yourself, you will not be imperiled in a hundred battles.”¹⁵

This section provides a brief overview of risk-based methodologies within TSA, business, and law enforcement.

A. RISK-BASED DEPLOYMENT METHODOLOGIES IN TSA

Historically, TSA has been a “risk-based” organization since its inception in many ways, although not always in a traditional “adversarial” sense of the word. For example, when it was first established, one of the primary “risks” that it needed to address was not having enough staffing to execute its mission in the first place. In an effort to mitigate this risk, TSA hired and deployed more than 55,000 individuals in its first year of existence.¹⁶

In the years that followed, TSA began to recognize certain locations were overstaffed while others were understaffed and initiated a study to mitigate this risk and right-size its workforce in September 2003.¹⁷ This study continued into 2004, at which point, TSA was formally called upon by the Intelligence Reform and Terrorism

¹⁵ Samuel B. Griffith, *The Art of War* (London: Oxford University Press, 1971).

¹⁶ U.S. Government Accountability Office, *Testimony, Before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate, Aviation Security—Improvement Still Needed in Federal Aviation Security Efforts* (GAO-04-592T) (Washington, DC: Government Accountability Office, 2004), <http://www.gao.gov/new.items/d04592t.pdf>.

¹⁷ U.S. Government Accountability Office, *Report to the Ranking Democratic Member, Committee on Transportation and Infrastructure, House of Representatives More Clarity on the Authority of Federal Security Directors Is Needed* (GAO-05-935) (Washington, DC: Government Accountability Office, 2005), <http://www.gao.gov/assets/250/247917.pdf>.

Prevention Act (IRPTA) of 2004 to develop a set of staffing allocation standards that would provide “the necessary levels of aviation security” while minimizing the “average aviation security related delay experienced by passengers.”¹⁸

In 2005, TSA presented a more standardized staffing allocation model to the U.S. Congress in accordance with the IRTPA and received generally positive feedback in a subsequent GAO audit.¹⁹ While the GAO did note that TSA’s use of the model had “helped guide its allocation of resources,” it also found that its use still resulted in some airports having too many screeners while others were left having too few and recommended periodic reevaluations of the model’s underlying assumptions and factors.²⁰

In the years that have followed, TSA has continued to hone its approach with a notable shift being its adoption of the screening procedures now commonly thought of when the term “risk-based security” is used. This passenger screening approach, covered more extensively by Kenneth Fletcher, Center for Homeland Defense and Security (CHDS) MASTER’S PROGRAM alum, in his thesis is designed to “calibrate security measures to groups of individuals based on risk.”²¹

The GAO and the DHS OIG have also pressed for TSA to continue to evolve over the past several years, with both releasing reports noting the need for TSA to develop risk-based deployment methodologies for several of its deployable assets.

- Behavior Detection Officers (BDOs)—A recent GAO report noted the need to “conduct a comprehensive risk assessment to include threat, vulnerability, and consequence of airports nationwide to determine the effective deployment of [Screening of Passengers by Observation

¹⁸ U.S. Government Accountability Office, *Report to Congressional Committees, Aviation Security: TSA’s Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed* (GAO-07-299) (Washington, DC: Government Accountability Office, 2007), <http://www.gao.gov/assets/260/257256.pdf>.

¹⁹ Ibid.

²⁰ Ibid.

²¹ Kenneth C. Fletcher, “Aviation Security: A Case for Risk-Based Passenger Screening” (master’s thesis, Naval Postgraduate School, 2011), <https://calhoun.nps.edu/bitstream/handle/10945/10601/11Dec%255FFletcher.pdf?sequence=3&isAllowed=y>.

Techniques] (SPOT) if TSA’s ongoing Aviation Modal Risk Assessment lacks this information.”²²

- Passenger Screening Canines (PSCs)—A recent GAO report noted “that PSC teams have not been deployed to the highest-risk airport terminals and concourses based on TSA’s high-risk list.”²³
- Visible Intermodal Prevention and Response (VIPR) Teams—A recent DHS-OIG report noted the need to “provide enhanced guidance regarding risk-based planning and increase access to risk assessment information that VIPR teams can use to prioritize deployments with partners and stakeholders”²⁴

It is important to note that TSA has already begun to address many of these recommendations. For example, BDOs were historically allocated based solely upon information from the civil aviation threat assessment (CATA) at the time the GAO report was released.²⁵ Today, the annual allocation of all threat assessment division assets, including PSCs and BDOs, across the United States is now conducted through risk-based allocation models that utilize a variety of data points to identify which locations should receive these specialized assets and how many they should receive.²⁶

²² U.S. Government Accountability Office, *Report to the Ranking Member, Committee on Transportation and Infrastructure, House of Representatives, Aviation Security, Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges* (GAO-10-763) (Washington, DC: U.S. Government Accountability Office, 2010).

²³ U.S. Government Accountability Office, *Report to Congressional Requesters, TSA Explosives Detection Canine Program—Actions Needed to Analyze Data and Ensure Canine Teams are Effectively Utilized* (GAO-13-239) (Washington, DC: U.S. Government Accountability Office, 2013).

²⁴ U.S. Department of Homeland Security, *Office of Inspector General, Efficiency and Effectiveness of TSA’s Visible Intermodal Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)* (OIG-12-103) (Washington, DC: U.S. Department of Homeland Security, 2012).

²⁵ U.S. Government Accountability Office, *Report to the Ranking Member, Committee on Transportation and Infrastructure, House of Representatives, Aviation Security, Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges*.

²⁶ *Utilizing Canine Teams to Detect Explosives and Mitigate Threats: Hearing Before the Committee on Homeland Security, Subcommittee on Transportation Security, United States House of Representatives, 113th Cong.* (2014) (statement of Melanie Harvey, Division Director, TSA TAD); *TSA’s SPOT Program and Initial Lessons From the LAX Shooting: Hearing Before the Committee on Homeland Security, Subcommittee on Transportation Security, United States House of Representatives, 113th Cong.* (2014) (statement of John Pistole, Administrator, TSA).

B. RISK-BASED DEPLOYMENT METHODOLOGIES IN BUSINESS

For a broad application of the concept of using models to inform “risk-based” decisions about where to place resources, in many towns across the United States, look not much further than down the street and find the nearest Starbucks. Since 1971, Starbucks has grown from a single retail outlet in Seattle, Washington, into the largest coffeehouse company in the world with over 20,000 stores in 64 countries.²⁷ The company has also been tremendously profitable and the price of Starbucks stock has risen from \$0.76/share to over \$77/share since it was first offered in 1992.²⁸ Despite this success, the company has certainly faced its share of challenges along the way.

In 2008, the former chief executive officer of Starbucks, Harry Schultz, came out of retirement to close hundreds of locations, many of which had only recently opened, following a period of rapid growth and declining sales. During a biennial investors’ conference in December 2012, Schultz noted, “In 2007 and 2008, the growth of Starbucks was undisciplined, and growth was more of a strategy as opposed to an outcome.”²⁹ In an effort to instill discipline and better inform decisions regarding where to open new locations, Starbucks turned to geographic information systems (GIS) technology.³⁰

By working with Esri, a GIS provider with access to thousands of data points ranging from consumer voting preferences to the amount of money spent on recreation, Starbucks was able to identify prime locations with the greatest amount of market potential.³¹ During the same 2012 conference, Schultz went on to announce plans to open “at least 1,500 new stores over the next five years in the United States alone” and boasted that “as a result of the demography, the data, the science and the experience we have, that

²⁷ Starbucks Corporation, “Q2–FY14 Earnings Release,” April 24, 2014, pp. 1–6.

²⁸ “SBUX Historical Prices,” accessed August 7, 2015, <http://finance.yahoo.com/q/hp?s=SBUX>.

²⁹ Malcom Wheatley, “Data-Driven Location Choices Drive Latest Starbucks Surge,” January 10, 2013, DataInformed, <http://data-informed.com/data-driven-location-choices-drive-latest-starbucks-surge/>.

³⁰ *Ibid.*

³¹ Taryn Luna, “Retailers Tap Software to Pick Best Locations for New Stores,” *Boston Globe*, August 29, 2013, <http://www.bostonglobe.com/business/2013/08/28/retailers-tap-software-programs-select-ideal-locations-for-new-stores/f6hsWesAX2NwrPXRPeUu4O/story.html>.

these locations in the returns will mirror what we've been able to accomplish in 2011 and 2012" which was a period of particularly high growth.³² This forecasted growth has thus far proven accurate with Starbucks revenue increasing nearly 45% from \$13.3 billion 2012 to \$19.2 billion 2015.³³

C. RISK-BASED DEPLOYMENT METHODOLOGIES IN LAW ENFORCEMENT AND SECURITY

The use of information and a structured methodology within law enforcement to understand crime and determine where to deploy resources can serve as a strong model for understanding potential applications at TSA given the similar, and oftentimes, overlapping, missions of law enforcement and homeland security.

The first known application of using data to understand criminal activity occurred in 1829 when André-Michel Guerry and Adriano Balbi published a series of maps that identified where crimes occurred relative to school instruction.³⁴ Guerry, along with fellow researcher Adolphe Quetelet, later went on to include other factors ranging from the prevalence of alcoholism to population diversity in an effort to understand better the role that sociological conditions play in criminal activity.³⁵ This concept continued to evolve and soon made its way to the United States in the 1920s when Clifford Shaw and Henry McKay, both University of Chicago professors, began using maps to understand juvenile delinquency better in Chicago, IL.³⁶

In the 1960s, the availability of computers led to several advances not only in the field of crime mapping but also resource allocation. For example, by using programs, such as SYMAP, designed by Harvard University, the St. Louis Police Department was

³² Wheatley, "Data-Driven Location Choices Drive Latest Starbucks Surge."

³³ "SBUX Income Statement."

³⁴ Michael Friendly and Nicolas de Sainte Agathe, "André-Michel Guerry's Ordonnateur Statistique: The First Statistical Calculator?," *The American Statistician* 66, no. 3 (August 1, 2012): 195–200, doi:10.1080/00031305.2012.714716.

³⁵ Luc Anselin et al., "Spatial Analyses of Crime," *Criminal Justice 2000* 4 (2000), http://www.ncjrs.org/criminal_justice2000/vol_4/04e.pdf.

³⁶ Keith Harries, *Mapping Crime: Principle and Practice* (Washington, DC: National Institute of Justice, 1999), <https://www.ncjrs.gov/html/nij/mapping/front.html>.

able to establish the Resource Allocation Research Unit with the goal of using “this new technical capability in the area of resource allocation.”³⁷ This trend continued into the 1980s and 1990s as computers became increasingly more commonplace.³⁸ Today, police departments in several major cities including Los Angeles, Atlanta, Seattle, and New York City use crime-mapping and other techniques to determine where to deploy their officers.³⁹

³⁷ Glenn A. Pauly, J. Thomas McEwen, and Stephen J. Finch, *Computer Mapping—A New Technique in Crime Analysis* (Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration, 1967), <https://www.ncjrs.gov/pdffiles1/Digitization/199NCJRS.pdf>.

³⁸ Harries, *Mapping Crime: Principle and Practice*.

³⁹ Nate Berg, “Predicting Crime, LAPD-Style,” *The Guardian*, June 25, 2014, <http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report>.

III. RISK-BASED DEPLOYMENT MODELS CURRENTLY IN-USE IN SECURITY SETTINGS

A number of different resource deployment approaches are in use throughout the world of law enforcement, ranging from the unstructured (e.g., pure gut-instinct) to the highly structured (e.g., SYMAP). A selection of some of the more structured approaches that have demonstrated positive results and could serve as models going forward is provided in the following sections.

A. CURRENT DATA-DRIVEN RISK-BASED DEPLOYMENT MODELS

For the purposes of this research, data-driven approaches to crime and traffic safety (DDACTS), risk terrain modeling (RTM), and PredPol are explored as they are designed to provide information at a tactical-level.

1. DDACTS

DDACTS is a joint initiative between the National Highway Traffic Safety Administration, the Bureau of Justice Assistance, and the National Institute of Justice designed to “reduce the incidence of crime, crashes, and traffic violations across the country.”⁴⁰ As summarized in an article appearing in the *CALEA Update*, “the basic premise of DDACTS is that the use of highly visible traffic enforcement in areas that have been shown to experience high levels of both crime and traffic problems is an efficient and effective way to improve the safety of the public.”⁴¹

While the nexus between DDACTS and data-driven risk-based deployment models may at first glance appear non-existent, it is DDACTS “strategic and tactical focus on places” that makes it an interesting model for comparison.⁴² DDACTS is based

⁴⁰ “Data-Driven Approaches to Crime and Traffic Safety,” accessed July 22, 2015, <http://www.nhtsa.gov/ddacts>.

⁴¹ Howard B. Hall, “Data-Driven Approaches to Crime and Traffic Safety—Its Application to Public Safety and Accreditation,” *CALEA Update*, no. 103, 2010, <http://www.calea.org/calea-update-magazine/issue-103/data-driven-approaches-crime-and-traffic-safety-its-application-publ>.

⁴² Alexander Weiss, *Data-Driven Approaches to Crime and Traffic Safety (DDACTS)—An Historical Overview* (Washington, DC: U.S. Department of Transportation, National Highway Safety Administration, 2013), <http://www.nhtsa.gov/staticfiles/nti/pdf/809689.pdf>.

upon the assumptions that “it is more efficient to focus on places than to focus on individuals” and “tools like computer mapping have made it easier to adopt place-based strategies.”⁴³ Furthermore, this approach has thus far proven successful in the field. For example, an evaluation of crime rates before and after DDACTS was implemented in Baltimore County, MD, found “robberies had decreased by 33.5 percent, burglaries by 16.6 percent, and auto thefts by 40.9 percent.”⁴⁴

The Nashville Police Department also experienced success through the use of DDACTS after it was deployed in January 2004 following a spike in drunk driving accidents.⁴⁵ Between 2003 and 2009, the department saw the number of fatal vehicle accidents decrease 15.6 percent, accidents resulting in injuries decrease 30.8 percent, and arrests for driving under the influence (DUI) increase 72.3 percent.⁴⁶ Additionally, an “analysis of the [Federal Bureau of Investigation] FBI [Uniform Crime Reporting] UCR data for the Nashville metropolitan area also revealed that the rate of Part 1 crimes committed between 2003 and 2008 decreased by 13.9 percent,” which demonstrates the potential of power of data-driven deployment decisions.⁴⁷

DDACTS is currently deployed in several municipalities throughout the United States, including Baltimore County, Maryland Police Department; Lafourche Parish, Louisiana Sheriff’s Office; Nashville, Tennessee Police Department; Oakland, California Police Department; Rochester, New York Police Department; St Albans Police Department and Vermont State Police; and Washoe County, Nevada Police Department.⁴⁸

⁴³ Weiss, *Data-Driven Approaches to Crime and Traffic Safety (DDACTS)—An Historical Overview*.

⁴⁴ Walter L. Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations* (Santa Monica, CA: RAND Corporation, 2013), http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf.

⁴⁵ Ibid.

⁴⁶ Ibid.

⁴⁷ Ibid.

⁴⁸ “Data-Driven Approaches to Crime and Traffic Safety.”

2. RTM

Similar to DDACTS, RTM is a data-driven risk-based deployment methodology that can be explored to gain a better understanding of the viability of concept. RTM is a conceptual methodology developed by Rutgers University professors Dr. Leslie Kennedy and Dr. Joel Caplan. The framework centers on the understanding that “risk is a continuous dynamic value that increases or decreases intensity and clusters or dissipates in different areas over time.”⁴⁹ Dr. Kennedy and Dr. Caplan have also noted that “risk is determined by a nexus of certain factors and it changes only as the characteristics and interactions of those factors vary.”⁵⁰ This working definition and understanding of risk is particularly relevant to a tactical-level risk-based deployment methodology, which seeks to place resources in the most optimal locations at the most optimal times relative to assessed risk.

With this understanding of risk, RTM uses GIS and applies layers of information to maps to identify potential risk hotspots and subsequently inform where police or other assets should be deployed.⁵¹ See Figure 1. This information can include historical criminal activity, demographic factors (e.g., where parolees live), environmental factors (e.g., vacant buildings), or any other factor that the users deem relevant to their analysis.⁵²

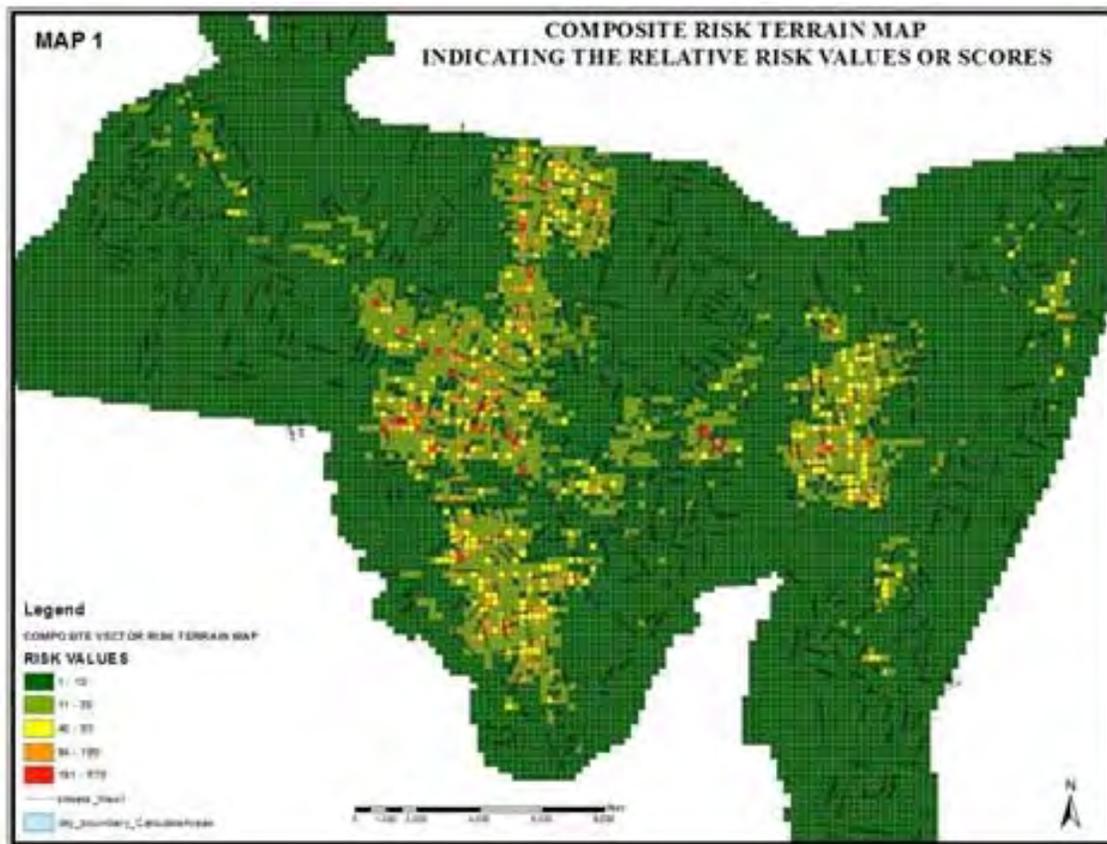
⁴⁹ Joel Caplan and Leslie Kennedy, *Introduction to Risk Terrain Modeling (RTM) for Strategic Decision-Making and Tactical Action* (Newark, NJ: Rutgers Center on Public Security, October 8, 2009), http://www.rutgerscps.org/docs/IntroToRTM_Brief.pdf.

⁵⁰ Ibid.

⁵¹ Joel Caplan and Leslie Kennedy, *Risk Terrain Modeling Compendium* (Newark, NJ: Rutgers Center on Public Security, 2011), http://www.rutgerscps.org/rtm/RiskTerrainModelingCompendium_CaplanKennedy2011.pdf.

⁵² Ibid.

Figure 1. Sample Risk Terrain Model Map



Source: Charles Anyinam, “Using Risk Terrain Modeling Technique to Identify Places with the Greatest Risk for Violent Crime in New Haven,” *Crime Mapping & Analysis News*, Spring 2015, <http://crimemapping.info/article/using-risk-terrain-modeling-technique-identify-places-greatest-risk-violent-crimes-new-haven/>.

A major benefit of this approach is that police departments are able not only to identify risk hotspots by location but also identify the risk presented by these locations.⁵³ For example, RTM may indicate that a particular neighborhood in a city is not only a hotspot for criminal activity but that the commerce and usage of illegal narcotics poses the greatest challenge.⁵⁴ This information allows police departments to deploy their

⁵³ Jonas H. Baughman and Joel Caplan, “Applying Risk Terrain Modeling to a Violent Crimes Initiative in Kansas City, Missouri,” *RTM Insights*, September 2010, http://rutgerscps.weebly.com/uploads/2/7/3/7/27370595/kcpd_rtminaction_brief.pdf.

⁵⁴ *Ibid.*

limited resources strategically, in this case, narcotics officers to mitigate the greatest amount of risk.⁵⁵

Several police departments are currently utilizing RTM with demonstrated success. In 2010, the Kansas City, Missouri Police Department conducted an annual exercise called the Violent Crimes Initiative and noted their “activities were most effective at suppressing crime and preventing the emergence of new crimes when they simultaneously targeted crime (density) hotspots and the highest-risk places identified by the RTM.”⁵⁶

3. PredPol

PredPol is another commercially available tool designed by a team of Ph.D. mathematicians and social scientists at the University of California Los Angeles (UCLA) and Santa Clara University in close collaboration with crime analysts and line level officers at both the Los Angeles and Santa Cruz Police departments.⁵⁷ Similar to RTM, PredPol uses data regarding historical criminal activity to forecast future criminal activity but it does not include information regarding specific individuals or groups.⁵⁸ This information is also graphically displayed using a GIS to help determine when and where to deploy police and other assets, shown is Figure 2.

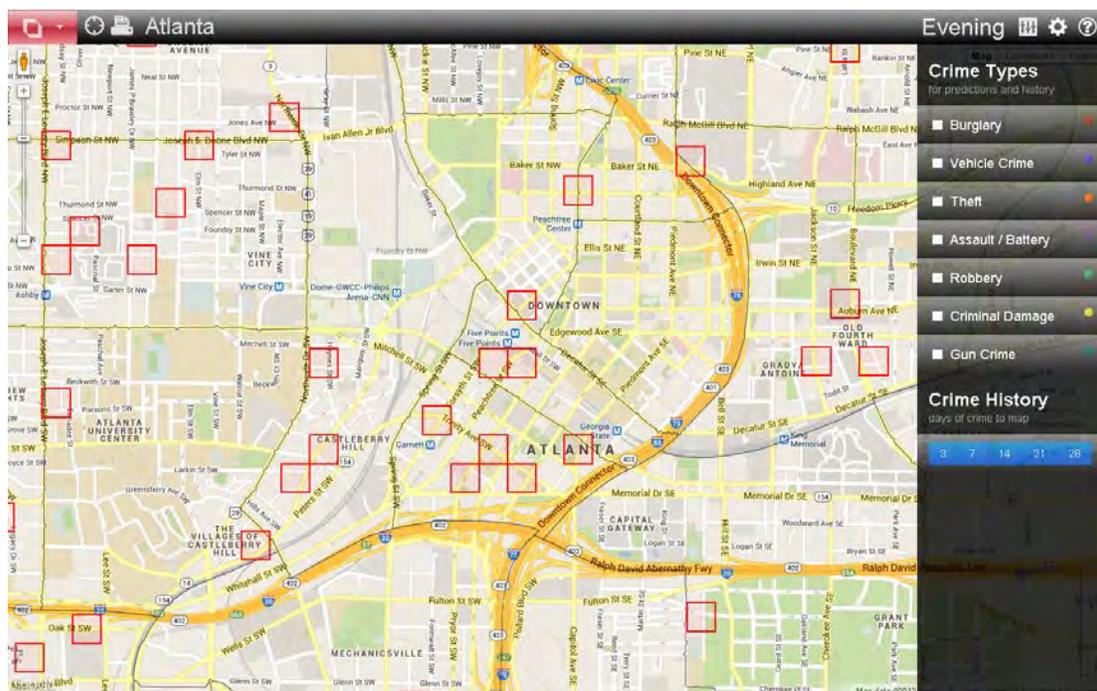
⁵⁵ Ibid.

⁵⁶ Baughman and Caplan, “Applying Risk Terrain Modeling to a Violent Crimes Initiative in Kansas City, Missouri.”

⁵⁷ “About Us,” 2015, <http://www.predpol.com/about/>.

⁵⁸ Ibid.

Figure 2. Sample PredPol Map



Source: Michell Eloy, “APD Rolls Out Crime Predicting Program,” 90.1FM WABE—Atlanta’s NPR Station, September 30, 2013, <http://news.wabe.org/post/apd-rolls-out-crime-predicting-program>.

Several police departments in the United States and abroad have begun using PredPol in recent years with positive results. In Los Angeles, CA, one of the first major U.S. police departments to adopt the system, the use of PredPol led to a 12% reduction in property crimes during a six-month period when compared to the previous year.⁵⁹ Similar results were seen in neighboring Santa Cruz, CA, with a 19% reduction in burglaries in a six-month period with PredPol while other variables (e.g., shift length) were held constant.⁶⁰

Internationally, Kent Police began their journey into the world of risk-based deployment methodologies after officers first asked how their peers in the United States

⁵⁹ “Don’t Even Think about It,” July 20, 2013, <http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it>.

⁶⁰ Zach Friend, “Predictive Policing: Using Technology to Reduce Crime,” *FBI*, April 9, 2013, <https://leb.fbi.gov/2013/april/predictive-policing-using-technology-to-reduce-crime>.

were using technology for predictive policing efforts in 2012.⁶¹ Soon after, the department began working with PredPol and developed a plan to bring this approach to Kent that culminated with the launch of several pilots nearly one year later.⁶²

The initial findings of these pilots were positive, with one trial finding that street crime occurred in PredPol defined locations 8.5% of the time compared to the Kent Police Analysis department's score of 5%.⁶³ By the conclusion of the pilot, this number had increased to an average of 11% with a singular high reported at 19%, while a 4% overall reduction in crime was seen.⁶⁴

B. CURRENT BAYESIAN GAME THEORY RISK-BASED DEPLOYMENT MODELS

Before transitioning into a discussion on intelligent randomization in scheduling (IRIS) and game-theoretic unpredictable and randomly deployed security (GUARDS), two models that show promise for helping TSA increase its security effectiveness and system efficiency, it is important to understand the basic premises of Bayesian game theory and its utility in risk-based resource deployment.

1. Bayesian Game Theory

Bayesian game theory is based upon Bayes' rule, which essentially holds "by updating our initial belief about something with objective new information, we get a new and improved belief."⁶⁵ For example, if individuals went hiking in the woods with a belief that they had a 50% of encountering a bear, only to learn from a park ranger that a bear had not been spotted in the forest in which they were hiking in the past 100 years,

⁶¹ Ćemal Dolićanin et al., *Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services* (Hershey, PA: IGI Global, 2014).

⁶² Kent Police, Corporate Services, Analysis Department, *PredPol Operational Review—Initial Findings* (Kent, UK: Kent Police, 2013), <http://www.statewatch.org/docbin/uk-2013-11-kent-police-pp-report.pdf>.

⁶³ "Don't Even Think about It."

⁶⁴ Kent Police, Corporate Services, Analysis Department, *PredPol Operational Review* (Kent, UK: Kent Police, 2014), <http://www.statewatch.org/docbin/uk-2014-kent-police-predpol-op-review.pdf>.

⁶⁵ Sharon Bertsch McGrayne, *The Theory That Would Not Die: How Bayes' Rule Cracked the Enigma Code, Hunted Down Russian Submarines, & Emerged Triumphant from Two Centuries of Controversy* (New Haven, CT: Yale University Press, 2011).

they would likely downgrade their initial belief to something much closer to 0%.⁶⁶ Now, if the park ranger yelled to the hikers as they parted ways “Yeah, no bears have been ‘spotted’ because no one is silly enough to hike in that bear-infested forest!” then the hikers would likely reconsider and increase their belief that they may encounter a bear.

When Bayes’ rule is applied to a risk-based resource deployment model, it allows the methodology to account for changes in the risk environment with an understanding that risk is not a static value. Furthermore, Bayes’ rule is an important concept to combine with game theory, which seeks to analyze the interaction between agents in a situation in which a set of possible moves exists and each move has a set of possible outcomes.⁶⁷

For example, consider a simple scenario with the aforementioned hikers continuing their journey into the woods and entering a long, narrow cave in which they discover a bear attempting to exit. Keeping things relatively simple, both the hikers and bear each have three options: stand their ground, turn around and move away in the opposite direction, or continue moving forward. Each permutation of these options has a possible outcome, such as a violent interaction if both the hikers and bear decide to move forward, and game theory holds that both actors will weigh these outcomes based on their own objectives.

If it is learned that the both the bear and the hikers decide to move forward in the narrow cave, a likelihood of the hikers surviving the ensuing encounter can be assigned based on the knowledge of previous bear and human interactions. However, if the hikers move forward only to discover that the bear is actually a newborn cub, Bayes’ rule makes it possible to change people’s understanding of the danger the situation presents yet again.

The relevance of Bayesian game theory in aviation security, or any security domain, cannot be understated, as defenders (e.g., TSA) seldom possess all possible

⁶⁶ B. John Garrick et al., “Confronting the Risks of Terrorism: Making the Right Decisions,” *Reliability Engineering & System Safety* 86, no. 2 (November 2004): 129–76.

⁶⁷ Shaun Hargreaves-Heap and Yanis Varoufakis, *Game Theory: A Critical Introduction* (London: Routledge, 2004).

information regarding the current risk environment with which to make resource deployment decisions. Despite this “fog of war,” both the defender and adversary tend to possess at least some cursory knowledge upon which their beliefs are predicated and upon which a Bayesian game theory model can be applied.

2. Applications of Bayesian Game Theory in Homeland Security

With an understanding of Bayesian game theory established, two existing models can be leveraged by TSA. The first, IRIS, was initially developed by the University of Southern California’s Center for Risk and Economic Analysis of Terrorism Events (CREATE) for use by the FAMS in deploying officers aboard U.S. commercial flights shows and has demonstrated positive results in several evaluations.⁶⁸

In one such evaluation, regional deployment schedules were generated using three different approaches. The first approach incorporated a uniform random policy in which FAMS could be deployed to any flight irrespective to its assessed risk, while the second used a naïve weighting policy in which the likelihood of deployment was proportionate to assessed risk.⁶⁹ When the results were compared to the schedules generated by IRIS, IRIS was shown to be “superior to the other two strategies in every region tested.”⁷⁰

Shortly after IRIS was introduced, GUARDS was developed by CREATE to aid with the deployment of TSA resources throughout airports across the nation.⁷¹ One unique aspect of GUARDS, as the name suggests, is that it was based upon an understanding that TSA does not have enough resources to provide 100% security and subsequently works to maximize the effectiveness of unpredictable scheduling in an

⁶⁸ Jason Tsai et al., *IRIS—A Tool for Strategic Security Allocation in Transportation Networks* (Los Angeles: USC Vitberbi, Teamcore Research Group, University of Southern California, 2009), <http://teamcore.usc.edu/papers/2009/aamas-09-industry.pdf>.

⁶⁹ Tsai et al., *IRIS—A Tool for Strategic Security Allocation in Transportation Networks*.

⁷⁰ Ibid.

⁷¹ James Pita et al., *GUARDS—Innovative Application of Game Theory for National Airport Security* (Los Angeles: USC Vitberbi, Teamcore Research Group, University of Southern California, 2011), http://teamcore.usc.edu/papers/2011/GUARDS_Ind2.pdf.

effort to mitigate assessed risk.⁷² Much like IRIS, GUARDS has demonstrated positive results with regards to its impact on security effectiveness in trial evaluations.

In one such evaluation, the impact of GUARDS deployments was compared against those of two other deployment strategies to determine which would provide the greatest mitigation against a notional adversarial attack. The first deployment strategy could be characterized as uniform, as all areas received equal treatment.⁷³ The second deployment strategy deployed resources using the underlying GUARDS methodology; however, the adversary was not allowed to plan around security countermeasures (a point of distinction in Bayesian game theory).⁷⁴ The results of these trials were then compared against those using GUARDS with the adversarial security circumvention constraint removed, with both GUARDS results outperforming the uniform approach.⁷⁵ Furthermore, the results were far superior when the adversary was allowed to plan around existing security countermeasures, which is a more likely representation of the real world.⁷⁶

The U.S. Coast Guard's (USCG) Port Resilience Operational/Tactical Enforcement to Combat Terrorism (PROTECT) is another example of a Bayesian game theory deployment initiative.⁷⁷ One of the more unique aspects of the PROTECT initiative is that it has undergone a real-world evaluation using adversary perspective teams, comprised of trained security professionals equipped with the understanding of "the adversary's known intent, capabilities, skills, commitment, resources, and cultural influences," in an effort to gain relevant feedback in lieu of interaction with an actual

⁷² Ibid.

⁷³ Ibid.

⁷⁴ Ibid.

⁷⁵ Ibid.

⁷⁶ Ibid.

⁷⁷ Eric Shieh et al., "PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States," in *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems—Volume 1*, AAMAS '12 (Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2012), 13–20, <http://teamcore.usc.edu/people/eshieh/AAMAS2012-protect.pdf>.

adversary.⁷⁸ The results of these evaluations demonstrated “a positive trend where the effectiveness of deterrence increased from the pre- to post- PROTECT observations.”⁷⁹

C. INHERENT CHALLENGES

Several challenges are associated with risk-based deployment methodologies that must be at a minimum understood, and ideally overcome, by any organization that seeks their use.

1. Defining Risk

The first challenge is simply defining risk. As Chris Reifel, a CHDS master’s program alum, noted in his thesis, “[e]xisting approaches to risk management hinge upon the how risk is defined.”⁸⁰ While Reifel’s thesis goes on to explore the etymology of the term and provides numerous competing definitions and understandings, the U.S. DHS Risk Steering Committee has established a definition for its purposes that can subsequently be leveraged by TSA. As defined by the U.S. DHS Risk Steering Committee, risk is the “potential for an adverse outcome assessed as a function of threats, vulnerabilities, and consequences associated with an incident, event, or occurrence.”⁸¹

2. Establishing Inputs

With a working definition of risk established, several additional challenges begin to emerge. The first is identifying the inputs for threat, vulnerability, and consequence. Holistically, the RAND Corporation touches upon this in its report titled *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, where it was noted that “relying on poor-quality data” is a pitfall when pursuing predictive policing.⁸² According to the RAND Corporation, there are “three typical deficiencies that can affect

⁷⁸ Ibid.

⁷⁹ Ibid.

⁸⁰ Christopher S. Reifel, “Quantitative Risk Analysis for Homeland Security Resource Allocation” (master’s thesis, Naval Postgraduate School, 2006), <https://www.hSDL.org/?view&did=469650>.

⁸¹ U.S. Department of Homeland Security, Risk Steering Committee, *DHS Risk Lexicon* (Washington, DC: U.S. Department of Homeland Security, 2010), <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.

⁸² Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

data quality: data censoring, systematic bias, and relevance.”⁸³ This pitfall is probably best summarized by the adage garbage-in, garbage-out, and can be overcome by either ensuring that quality data is utilized or understanding the limitations of the data provided, and subsequent limitations of the outputs. In an article appearing in the journal *Risk Analysis*, authors Dillon, Liebe, and Bestafka further expand upon this challenge by noting while “most researchers agree that the risk of terrorism is some function of threat, vulnerability, and consequences, many competing theories exist on how to consider these components.”⁸⁴

3. Useful Products

Once the aforementioned challenges are overcome, or at a minimum understood, the focus shifts towards turning the output of a risk-based deployment methodology into something of value to tactical-level operators. The RAND Corporation touches upon this concept when it discusses the pitfall of “focusing on prediction accuracy instead of tactical utility.”⁸⁵ Erik Dahl in his book, *Intelligence and Surprise Attack*, further corroborates the importance of this concept. As Dahl notes, “precise, tactical-level intelligence warning together with policymakers who are receptive to that warning” is the difference between intelligence successes and intelligence failures.⁸⁶ The sheer spontaneity that is the human experience will likely keep 100% accuracy an idealized target and, as RAND notes, “we must accept some limits on ‘accuracy.’”⁸⁷ However, it is likely much easier said than done. As Henry H. Willis notes in the journal, *Risk Analysis*, “Establishing tolerable levels of risk is one of the most contentious and important risk management decisions.”⁸⁸

⁸³ Ibid.

⁸⁴ Robin L. Dillon, Robert M. Liebe, and Thomas Bestafka, “Risk-Based Decision Making for Terrorism Applications,” *Risk Analysis* 29, no. 3 (March 2009), <http://onlinelibrary.wiley.com.lib.proxy.nps.edu/doi/10.1111/j.1539-6924.2008.01196.x/pdf>.

⁸⁵ Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

⁸⁶ Erik J. Dahl, *Intelligence and Surprise Attack—Failure and Success from Pearl Harbor to 9/11 and Beyond* (Washington, DC: Georgetown University Press, 2013).

⁸⁷ Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

⁸⁸ Henry H. Willis, “Guiding Resource Allocations Based on Terrorism Risk,” *Risk Analysis* 27, no. 3 (June 2007): 597–606.

4. Measuring Effectiveness

Another challenge is how to measure the amount of risk that was mitigated through the deployment of resources. The RAND Corporation outlines “underemphasizing assessment and evaluation” as a pitfall to avoid and points out that “very few [practitioners] said that they had evaluated the effectiveness of the predictions they produced or the interventions developed in response to their predictions.”⁸⁹ In all likelihood, it is due to the reality that measuring risk mitigation is very difficult. Although speaking about challenges with homeland security grant funding, Willis’s assessment that “currently, neither the methods nor the data are available to answer questions about the effectiveness of available risk reduction alternatives” is applicable to the field at large.⁹⁰ The researchers who developed risk terrain modeling, however, suggest that results can be achieved “by regularly re-assessing risk, and then measuring changes in risk values among different risk terrain maps at micro or macro levels using basic inferential statistics.”⁹¹

5. Protecting Civil Rights and Liberties

It is also important to note that a risk-based deployment methodology will, by definition, drive resources to areas deemed to present greater risk. As the RAND Corporation notes, “the very act of labeling areas and people as worthy of further law enforcement attention inherently raises concerns about civil liberties and privacy rights,”⁹² and “overlooking civil and privacy rights” is a pitfall that must be avoided. While the overwhelming majority of TSA employees are not law enforcement officers, this concern is no less valid and is in fact of particular importance to the TSA, which interacts with approximately two million aviation passengers every day.⁹³ Furthermore,

⁸⁹ Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

⁹⁰ Willis, “Guiding Resource Allocations Based on Terrorism Risk.”

⁹¹ Joel Caplan, Leslie W. Kennedy, and Joel Miller, “Risk Terrain Modeling: Brokering Criminological Theory and GIS Methods for Crime Forecasting,” *Justice Quarterly* 28, no. 2 (2011), <http://search.proquest.com/docview/863479648?accountid=12702>.

⁹² Perry et al., *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*.

⁹³ U.S. Transportation Security Administration, *TSA at a Glance* (Washington, DC: U.S. Department of Homeland Security, n.d.), https://www.tsa.gov/sites/default/files/assets/pdf/tsaatglance_final.pdf.

TSA does have much in common with law enforcement when considering its responsibility to screen both individuals and items along with its ability to prevent the introduction of either into the transportation system when they present a security threat.

As a risk-based deployment methodology becomes more granular, the importance of protecting individual civil rights and liberties becomes increasingly more significant. According to the U.S. Supreme Court, the standards for what “constitutes reasonable suspicion are relaxed” in areas deemed high-crime, or “hot-spots,” which affords some leeway for operators.⁹⁴ However, in a 2012 presentation to the *Law Enforcement Information Management Conference*, researchers noted that this “issue [is] minor in comparison to civil and privacy rights issues raised by identifying “hot people.”⁹⁵

⁹⁴ Illinois v. Wardlow (U.S. 119 2000).

⁹⁵ John S. Hollywood et al., “Predictive Policing: What It Is, What It Isn’t, and Where It Can Be Useful.” 2012 Law Enforcement Information Management Conference, Indianapolis, IN, May 22, 2012, <http://www.theiacp.org/portals/0/pdfs/leim/2012presentations/ops-predictivepolicing.pdf>.

IV. POLICY EVALUATION

With an understanding of several potential ways to address the challenge of optimizing resource deployment and a cursory framework upon which to form an objective recommendation, three options are presented and assessed.

A rating of 1 reflects a positive correlation while a rating of 3 reflects a negative correlation for a given criterion. Using this scale facilitates a simple initial postulation while avoiding the challenges that a more granular scale introduces (e.g., is it a 4 or a 5?)

A. **OPTION A—MAINTAIN CURRENT RESOURCE DEPLOYMENT STRATEGY**

If it ain't broke, don't fix it.

~ Bert Lance

In a scientific experiment, Option A would be considered the control group, as it makes it possible to measure the effects of a given treatment against an established baseline. In the absence of an experiment, analyzing Option A allows the current approach to be assessed.

At present, TSA as an enterprise lacks a standardized tactical-level risk-based deployment methodology for its assets and tends to instead rely upon a combination of individual subject matter expertise and the occasional program-specific approach. For example, a 2014 DHS OIG report found, “TSA created documents and schedules with short term goals based on institutional knowledge to deploy AIT” and “did not have a policy or process requiring program offices to document strategic deployment plans for new technology that align with the goals of the Passenger Screening Program.”⁹⁶

In its response, TSA noted that it has “launched the effort to develop and approve updated deployment strategies that address short- and long-term goals,” however, it

⁹⁶ Office of Inspector General, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology* (OIG-13-120 (Revised)) (Washington, DC: U.S. Department of Homeland Security, 2014), https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-120_Mar14.pdf.

appears as though these are still in development and this research provides TSA an opportunity to further its endeavor.⁹⁷

1. Security Effectiveness

Determining the precise level of security effectiveness of TSA's current resource deployment strategy would require considerable resources to include active participation by the agency and is not necessary for the objectives of this evaluation. However, it would be reasonable to assume that an opportunity may exist to improve after a recent classified DHS OIG report released in May 2015 showed how often "red team" security auditors were able to circumvent security screening.⁹⁸ While unendorsed results are available in the public domain, the official results remain classified and are not included in this research. That said, Secretary Johnson has noted, "The numbers in these reports never look good out of context" before laying out a six-point improvement plan that lends itself to some semblance of poor performance.⁹⁹

Despite these challenges, the fact remains that TSA has prevented hundreds of thousands of prohibited items, including firearms and explosives, from being carried onto planes over the past several years, as demonstrated in Table 1. While it is impossible to calculate an exact rate of detection using these numbers alone, as the precise number of items that were introduced and could have been potentially detected by officers must be known, the interdiction of these items does point to a level of efficacy.¹⁰⁰

⁹⁷ Office of Inspector General, *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology*.

⁹⁸ Jeh C. Johnson, "Statement By Secretary Jeh C. Johnson On Inspector General Findings On TSA Security Screening," U.S. Department of Homeland Security, June 1, 2015, <http://www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-tsa-security-screening>.

⁹⁹ Ibid.

¹⁰⁰ Ibid.

Table 1. Known Prohibited Item Encounter Rate

	FY12¹⁰¹	FY13¹⁰²	FY14¹⁰³
# of Items Screened	2,425,000,000	2,425,000,000	2,040,000,000
# of Prohibited Items Discovered	117,000	111,000	111,000
Known Encounter Rate (%)	0.0048%	0.0046%	0.0054%

As such, a rating of 2 is given for this particular criterion.

2. System Efficiency

With regard to current system efficiency, a combination of TSA’s staffing numbers and publicly available screening results can be used to develop a cursory understanding of how the system is operating, as shown in Table 2.

Table 2. Passengers and Baggage Screened per FTE

	FY12¹⁰⁴	FY13¹⁰⁵	FY14¹⁰⁶
# of Employees	51,767	51,378	49,427
# of Passengers Screened	640,000,000	640,000,000	660,000,000
# of Items Screened	2,425,000,000	2,425,000,000	2,040,000,000
Average Passengers per FTE	12,363	12,457	13,353
Average Bags per FTE	46,845	47,199	41,273

For example, TSA received 49,427 full-time equivalent (FTE) in FY14 for aviation security purposes while screening approximately 660 million passengers during the same timeframe.¹⁰⁷ At that rate, each FTE screened an average of approximately

¹⁰¹ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2014* (Washington, DC: U.S. Department of Homeland Security, 2013), <http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf>.

¹⁰² U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2015* (Washington, DC: U.S. Department of Homeland Security, 2014), <http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf>.

¹⁰³ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2016* (Washington, DC: U.S. Department of Homeland Security, 2015), http://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf.

¹⁰⁴ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2014*.

¹⁰⁵ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2015*.

¹⁰⁶ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2016*.

¹⁰⁷ Ibid.

13,353 passengers and 41,237 bags for the year, or nearly 257 passengers and 792 bags each week.

While these figures might seem rather low, it is important to note that outliers also certainly exist in a network as large as the approximately 440 federalized airports that TSA operates at across the nation, such as Hartsfield–Jackson Atlanta International with nearly 47 million enplanements in 2014 versus approximately 5,700 at Cheyenne Regional/Jerry Olson Field.¹⁰⁸

As such, a rating of 2 is given for this particular criterion.

3. Constitutional Considerations

From a purely functional perspective, TSA’s current resource deployment strategy does not violate citizen’s rights under the Fourth or Fifth Amendments of the U.S. Constitution. However, all resources require proper jurisdiction to operate in a given location once they have been deployed and their activities are certainly subject to legal scrutiny. The scope and nature of these activities is not relevant for the purposes of this research in that they have no bearing on the actual deployment of resources and a rating of 1 is given for this particular criterion.

4. Social Considerations

When considering some of the social issues surrounding TSA’s current deployment approach, understanding the role and impact of its flagship program, TSA PreCheck, is helpful. Passengers enrolled in TSA PreCheck undergo additional preflight screening, to include a background check, and are subsequently, deemed “low-risk” and eligible to use dedicated lines and receive expedited screening at select airports throughout the United States.¹⁰⁹ In return, TSA is better able to focus its resources on individuals deemed high-risk (e.g., selectees) or who present an unknown risk.

¹⁰⁸ “Commercial Service Airports Based on Preliminary CY 2014 Enplanements,” June 29, 2015, http://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/media/cy14-commercial-service-enplanements.pdf.

¹⁰⁹ Risk-Based Security: What This Means for You.”

By maintaining this strategy, it can be presumed that TSA will continue to decrease overall travel time as more individuals are enrolled into the TSA PreCheck program and become eligible for expedited screening. While TSA PreCheck enrollments reached 1 million passengers in its first 15 months of operation, which lends itself towards some level of sustainability, it is also important to note that the success of this strategy is dependent on both passenger participation in the program and TSA’s ability to provide dedicated resources to serve this growing population.¹¹⁰

Despite the “strong majority” of individuals in a recent poll (79%) reporting that they believe separating pre-screened passengers into a different line will speed up the screening process, the method of doing so is divisive with nearly one-third (29%) felt that the requirements for TSA PreCheck violated applicants’ privacy.¹¹¹ When those polled were asked to specify the level of scrutiny they felt would be appropriate for inclusion into the program, the results varied considerably, as demonstrated in Table 3.

Table 3. Public Opinion of TSA PreCheck Vetting Measures

	Percent Agreeing¹¹²
Passing a criminal background check	76%
Submitting to a fingerprint scan	73%
Holding U.S. citizenship	70%
An analysis of past travel habits	56%
Passing a drug test	37%
A check of family and social connections	35%
Other	9%
None	8%

Perhaps most interestingly, over half (56%) felt that treating passengers differently in the first place was unfair.¹¹³

¹¹⁰ “TSA Pre✓® Reaches Milestone with More than 1 Million Travelers Enrolled,” March 24, 2015, <https://www.tsa.gov/press/releases/2015/03/24/tsa-precheckR-reaches-milestone-more-1-million-travelers-enrolled>.

¹¹¹ Larry Shannon-Missal, “Who Screens the Screeners? American Opinions on the TSA,” The Harris Poll, April 24, 2014, <http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/1419/Default.aspx>.

¹¹² Ibid.

¹¹³ Ibid.

As such, a rating of 2 is given for this particular criterion.

5. Political Feasibility

Lastly, when considering political feasibility of TSA's current deployment approach, it is certainly focused on its established mission of protecting the nation's transportation systems, which includes pivoting to meet emerging challenges, as evidenced by its focus on mitigating the insider threat following a high-profile incident in December 2014.¹¹⁴ In the aftermath of this particular incident, in which aviation employees allegedly leveraged their privileged access to smuggle firearms onto aircraft, TSA responded to by redeploying many of its officers to conduct unpredictable employee screenings.¹¹⁵

TSA also continues to realize savings as a result of its risk-based security posture, with the agency requesting \$119 million less in FY16 when compared to its previous year's request, citing several "risk-based security efficiencies."¹¹⁶ These reductions included a 1,666 FTE reduction in the screening workforce, with TSA noting "RBS methods have proven more efficient in moving people through the checkpoint than regular screening lanes and require fewer resources."¹¹⁷

As such, a rating of 1 is given for this particular criterion.

B. OPTION B—ADAPT AN EXISTING DATA-DRIVEN RISK-BASED DEPLOYMENT METHODOLOGY

If I have seen further, it is by standing on the shoulders of giants.

~ Sir Isaac Newton

In the world of the Federal Acquisition Regulation (FAR), this approach might be characterized as leveraging commercially available off-the-shelf (COTS) solutions to

¹¹⁴ Peter Neffenger, "Aviation Security Challenges: Is TSA Ready for the Threats of Today?" Transportation Security Administration, July 29, 2015, <https://www.tsa.gov/news/testimony/2015/07/29/testimony-tsa-aviation-security-challenges>.

¹¹⁵ Ibid.

¹¹⁶ U.S. Department of Homeland Security, *Budget-in-Brief Fiscal Year 2016*.

¹¹⁷ Ibid.

tackle the identified problem of increasing the efficient and effective deployment of resources.¹¹⁸ Several products already exist and are currently used in the law enforcement domain including DDACTS, RTM, and PredPol.

Option B entails exploring the use of these, or similar, products in the aviation security domain. While this solution ideally decreases the adoption curve, as it builds upon existing methodologies that have demonstrated success, it also exposes risks including the potential for gaps between the needs of the agency and the capabilities of the solution, as they were not expressly created for TSA's use.

1. Security Effectiveness

To hypothesize the potential impact properly that adapting an existing risk-based deployment methodology will have on TSA's security effectiveness, attention must be given to the past performance of such solutions by other entities.

As demonstrated and discussed in Chapter III, the performance of DDACTS, RTM, and PredPol has been measuredly positive with methodology-driven officer deployments with significant decreases in the illicit activity they seek to reduce. The importance of these decreases is particularly relevant in departments that, much like TSA at present, relied heavily upon human judgment and analysis to deploy officers tactically prior to the use of a data-driven methodology.

For example, consider the case of the Kent Police Department in which the accuracy of its crime forecasting more than doubled from 5% to 11% through the use of PredPol.¹¹⁹ While it is true that it is a far cry from 100% accuracy, it is nonetheless a step in the right direction and validates the ability for such methodologies to overcome countless years of relying upon a mix of intuition and manual analysis. Similarly, the use of such methodologies is a relatively new phenomenon and it is likely that improvements will be seen in accuracy, as departments continue to adopt them, as it will provide both the funding and tangible feedback critical for ongoing research and development.

¹¹⁸ 12.1 Acquisition of Commercial Items General, FAR 2005-83 (2005), <https://www.acquisition.gov/?q=browse/far/12/1>.

¹¹⁹ Kent Police, Corporate Services, Analysis Department, *PredPol Operational Review*.

Despite the generally positive results, it is important to note that none of the existing methodologies found in the literature, including the three methodologies discussed in detail (DDACTS, RTM, and PredPol), were specifically designed with the deployment of aviation security assets in mind. As such, a risk of decreased security effectiveness is possible should they be deployed, and more importantly, fully relied upon while they undergo any needed recalibration for this unique environment.

That said, it is also certainly within the realm of possibility to repurpose these methodologies and tools, as evidenced by several studies undertaken by the creators of RTM. One such example is a 2010 study conducted by researchers Dr. William Moreto and Dr. Joel Caplan to determine whether risk terrain modeling could be adapted to forecast maritime piracy throughout the world.¹²⁰ The research team began this study by identifying a number of different data points ranging from the number of maritime chokepoints to country assessments from the failed states index.¹²¹ Once all the data points had been identified, corresponding data from 2008 was loaded into the model and the results were compared against known incidents from 2009, with RTM successfully identifying the location of pirate attacks more than 60% of the time.¹²²

While the study was hypothetical in the sense that an actual deployment of countermeasures to mitigate the assessed risk never occurred, the study successfully demonstrated that RTM can be used to produce tactical-level information for non-traditional purposes.

While a more thorough discussion exists in Chapter III, it would be fair to characterize the results as generally positive. As such, a rating of 1 is given for this particular criterion.

¹²⁰ William D. Moreto and Joel Caplan, *Forecasting Global Maritime Piracy Utilizing the Risk Terrain Modeling (RTM) Approach* (Newark, NJ: Rutgers Center on Public Security, 2010), http://www.rutgerscps.org/publications/MaritimePiracy_Brief.pdf.

¹²¹ Leslie W. Kennedy and Edmund F. McGarrell, ed., *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice* (New York: Routledge, 2011).

¹²² Moreto and Caplan, *Forecasting Global Maritime Piracy Utilizing the Risk Terrain Modeling (RTM) Approach*.

2. System Efficiency

When considering system efficiency, an article appearing in the journal *Risk Analysis* by Henry H. Willis surmises “ultimately, efficient allocation of homeland security resources would distribute resources where they can most reduce risks, not where risks are the greatest.”¹²³ In this area, data-driven tools and methodologies can lead to increased performance, such as Kansas City’s use of RTM to guide the deployment of narcotics officers successfully in Chapter III.

Furthermore, many of these systems have demonstrated an ability to outperform the work of existing criminal analysts using other methods to optimize officer deployments.¹²⁴ As such, further efficiencies can be gained by redeploying these criminal analysts to other tasks and allowing deployments to be driven by tools like DDACTS, RTM, and PredPol and a rating of 1 is given for this particular criterion.

3. Constitutional Considerations

From a legal perspective, two primary questions appear to surround the use of a data-driven risk-based deployment methodology. The first question is what, if any, impact that such a methodology has on established thresholds for law enforcement engagement, and more specifically, search and seizure. The second question is what data elements can, and cannot, be used to formulate an understanding of the risk environment.

In the United States, the government must first establish a reasonable suspicion of criminal activity to search a citizen and probable cause to detain them.¹²⁵ The use of a risk-based deployment methodology raises several important questions regarding these precedents and its ability to play into the calculus of whether the thresholds have been met. Most notably, does an individual’s mere presence in a specific area that has been deemed high-risk by a given methodology in and of itself constitute reasonable suspicion, or even become a factor that effectively lowers the established threshold?

¹²³ Willis, “Guiding Resource Allocations Based on Terrorism Risk.”

¹²⁴ Kent Police, Corporate Services, Analysis Department, *PredPol Operational Review*.

¹²⁵ David A. Harris, “Particularized Suspicion, Categorical Judgments: Supreme Court Rhetoric Versus Lower Court Reality Under *Terry v. Ohio*,” *St. John’s Law Review* 72, no. 3 (March 2012), <http://scholarship.law.stjohns.edu/lawreview/vol72/iss3/11>.

For example, two women in Santa Cruz, CA were confronted, and subsequently, arrested (on unrelated charges) after they were found peering into car windows in an area identified by a predictive model as at-risk for car thefts.¹²⁶ As the author of a more comprehensive discussion on the topic noted, “it is arguable that peering into windows in a parking garage is sufficient reason to be stopped and detained by police.”¹²⁷ However, when this behavior was coupled with the results of predictive modeling, the Santa Cruz Police Department decided to move in.

A second point that must be established is the right for entities in the United State to collect the data that drives risk-based deployment methodologies. The United States operates under the framework of the U.S. Constitution and interpretations by the U.S. Supreme Court, which has held that certain limitations are placed on the government’s ability to infringe upon the privacy of citizens despite the word “privacy” never actually appearing in the U.S. Constitution.¹²⁸ When it comes to data privacy, what those limitations are has yet to be clearly defined through litigation, which has left some calling for the passage of a national statute or constitutional amendment to address the issue.¹²⁹ Several states have also begun adopting their own legislation regarding the right to data privacy in the absence of a more broad decree.¹³⁰

Despite this ongoing debate, it would appear as though the concerns raised can be abated through the use of rather broad, publicly available data, such as criminal activity in specific areas, as PredPol has done. Conversely, care must be taken when more sensitive data like personally identifiable information (PII) is used to identify risk hot-

¹²⁶ Erica Goode, “Data-Crunching Program Guides Santa Cruz Police before a Crime,” *The New York Times*, August 15, 2011, <http://www.nytimes.com/2011/08/16/us/16police.html>.

¹²⁷ Andrew G. Ferguson, “Predictive Policing and Reasonable Suspicion,” *Emory Law Journal* 62, no. 2 (2012), <http://law.emory.edu/elj/content/volume-62/issue-2/articles/predicting-policing-and-reasonable-suspicion.html>.

¹²⁸ William M. Beaney, “The Constitutional Right to Privacy in the Supreme Court,” *The Supreme Court Review* 1962, no. 1 (1962): 212–51.

¹²⁹ Marsha Cope Huie, Stephen F. Larabee, and Stephen D. Hogan, “The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues,” *Tulsa Journal of Comparative and International Law* 9, no. 2 (2002), <http://digitalcommons.law.utulsa.edu/tjcil/vol9/iss2/2/>.

¹³⁰ Pam Greenberg, “Privacy Protections in State Constitutions,” National Conference of State Legislatures, 2015, <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>.

spots. It is important that TSA work with experts not only well versed in data privacy laws, but also in its own unique operations (e.g., aviation security) to ensure that the use of given data elements usage will withstand legal scrutiny should it decide to pursue a data driven risk-based deployment methodology.

In light of these concerns, a rating of 2 is given for this particular criterion.

4. Social Considerations

Considering the amount of data that individuals willingly provide to private companies each and every day, and working off the understanding that the majority of individuals present little or no risk to aviation security, the holistic notion of using of data to decrease travel time and screening scrutiny would seemingly be a good thing. However, a great deal of public concurrence hinges on the actual data used seeing as how nearly one-third (29%) of respondents to a 2014 survey on TSA's practices felt that the current data requirements (e.g., criminal history) for TSA PreCheck violated applicants' privacy.¹³¹

Similar concerns have been raised regarding the use of big data methodologies by law enforcement agencies. For example, Kent Police Department's launch of PredPol quickly drew comparisons to the science fiction film *Minority Report* from British media, just as it had in previous U.S. deployments.¹³² In the film, set in the 2050s, a specialized PreCrime department is responsible for arresting murderers before they are able to actually carry out their attacks by using a combination of psychic ability and technology. While a common thread certainly exists in that police are attempting to be proactive rather than reactive in both cases, the notion that a methodology like PredPol could lead to a preventive arrest and/or conviction seems farfetched but certainly highlights both the fascination and fear that citizens have of living in such a world.

¹³¹ Shannon-Missal, "Who Screens the Screeners? American Opinions on the TSA."

¹³² Paul Peachey, "The Real Minority Report? Kent Constabulary Tests Computer Program to Predict Crime," *The Independent*, August 4, 2013, <http://www.independent.co.uk/news/uk/crime/the-real-minority-report-kent-constabulary-tests-computer-program-to-predict-crime-8744940.html>.

More pronounced concerns are seen when elements of PII are incorporated into the big data analyzed by law enforcement agencies. In a 2014 pilot study launched by the London Metropolitan Police to “identify groups of gang members that were at the highest risk of reoffending” using big data, a prominent privacy group was quick to caution police “to be very careful about how they use this kind of technology.”¹³³ The Chicago Police Department has faced similar criticism of its proactive outreach program that uses computer algorithms to identify specific individuals at risk of becoming victims of violent crime by combining criminal activity data with social network theory.¹³⁴

In light of these concerns, a rating of 2 is given for this particular criterion.

5. Political Feasibility

When exploring the political feasibility of adapting an existing risk-based deployment methodology to execute its mission, maintaining or increasing effective and efficient operations is critical. It includes creating a compelling need for decision makers to determine that the investment in data driven risk-based deployment methodologies is a sound one. The cost of the software alone is oftentimes hundreds of thousands of dollars. For example, the annual cost of the PredPol software used by the Kent Police was £130,000, or nearly \$200,000.¹³⁵

This price tag only increases when the cost of the hardware to run the software, specialized training, and similar costs are included. In an austere budget environment, such costs would most certainly be questioned. However, as a police analyst and part-time blogger noted in a discussion on the topic, “it’s cheaper to prevent a crime than to solve a crime, and that’s where I think the promise lies.”

¹³³ Leo Kelion, “London Police Trial Gang Violence ‘Predicting’ Software,” *BBC News*, October 29, 2014, <http://www.bbc.com/news/technology-29824854>.

¹³⁴ Matt Stroud, “The Minority Report: Chicago’s New Police Computer Predicts Crimes, but Is It Racist?,” *The Verge*, February 19, 2014, <http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist>.

¹³⁵ Peachey, “The Real Minority Report?”

Seeing as how a data-driven risk-based deployment methodology has the potential to help TSA execute its mission and increase efficiency, a rating of 1 is given for this criterion.

C. OPTION C—INVEST IN THE DEVELOPMENT OF A BAYESIAN GAME THEORY RISK-BASED DEPLOYMENT METHODOLOGY

When my information changes, I alter my conclusions. What do you do, sir?

~ John Maynard Keynes

Through careful planning, Option C can best be characterized as a calculated investment in the emerging field of predictive analysis. At present, only a handful of tactical-level risk-based deployment methodologies exist within TSA. While each of these methodologies strives to meet the unique needs of the individual stakeholders and agency program offices that sponsored their development, they lack congruence, and subsequently, deprive leaders at the strategic level of the organization potentially valuable information regarding risk across the environment while simultaneously depriving individuals at all levels of valuable time due to their oft-duplicative nature.

One of the benefits of Option C is that it would be a truly customized solution, which means that TSA could capitalize upon existing capital knowledge acquired as individual program offices developed their own tools and solutions by ensuring their participation in the early design stages. This participation will also help ensure that any solution meets the needs of these stakeholders in addition to those of the agency at-large.

As previously noted, several existing platforms are available; however, those based in Bayesian game theory, such as IRIS and GUARDS, hold a great deal of promise due to their inherent ability to (1) account for the actions of a defender, and (2) forecast the adversarial reaction.

1. Security Effectiveness

Similar to Option B, an assessment of the past performance of existing Bayesian game theory risk-based deployment methodologies must be conducted to hypothesize

properly the impact on TSA's security effectiveness. That said, an additional level of fidelity relative to the assessment of Option B exists in that the two primary examples, IRIS and GUARDS, were designed with aviation security in mind and evaluated accordingly. Furthermore, as demonstrated in Chapter III, both the quantitative and anecdotal results of several evaluations of these approaches have been largely positive.

However, game theory is certainly not without its critics, many of whom argue that its major flaw is its reliance on a rational actor with a given set of preferences to model possible outcomes.¹³⁶ Commonly cited examples of irrational acts that defy game theory include altruistic deeds, in which individual actors sacrifice more than they receive in return, and individuals who refuse to follow social norms of behavior that allow for rational modeling. While a great deal of debate is occurring within academia on whether game theory can explain such seemingly "irrational" behavior, the likelihood of encountering a truly irrational actor in the first place must also be considered, and weigh that against the utility of modeling against a rational one.

In returning to the private industry, it is unlikely that a successful company like Starbucks would open a retail outlet in the middle of a cornfield vice opening an outlet on Main Street of a nearby town unless it is highly probable that it would generate a greater return on investment. Yes, the possibility always exists that some individuals may seek out a Starbucks in the middle of a cornfield; however, the company's stockholders (i.e., U.S. taxpayers) are unlikely to see the merit of such a seemingly irrational move. Similarly, it is certainly possible to encounter an actor that cannot be modeled and is subsequently able to overcome the security of an entity that leverages a resource deployment system based in game theory, but a far more likely outcome is encountering and disrupting a rational actor.

It is also important to note that researchers have successfully demonstrated the ability for game theory models to overcome aspects of this rational actor limitation. In one such experiment, researchers with the USCG's PROTECT initiative were able to

¹³⁶ Gale Lucas, Matthew D. McCubbins, and Mark Turner, "Against Game Theory," in *Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource*, ed. Robert A. Scott and Stephen M. Kosslyn (Hoboken, NJ: John Wiley & Sons, Inc., 2015).

develop a “quantal response” model that mimics irrationality by “presume[ing] that humans will choose better actions at a higher frequency, but with noise added to the decision-making process.”¹³⁷ The results were positive, with the researchers finding that this new model “more robustly handles real-world uncertainties than a perfect rationality model.”¹³⁸ Furthermore, simply maintaining some aspect of randomness in an otherwise optimized resource deployment strategy can help mitigate this risk.

As such, a rating of 1 is given for this particular criterion.

2. System Efficiency

While Option C affords TSA an opportunity to tailor an approach to meet its unique needs, it also lacks the convenience of simply maintaining the status quo or pursuing a more readily available data-driven solution. In turn, it results in the government potentially expending additional resources when compared to Option A and Option B. However, the existence of two models that could be leveraged does have a mitigating effect. Furthermore, it could also be considered an investment likely to yield a positive return in the long-term as resource deployment would be further optimized to TSA’s needs.

When examining the USCG’s experience with PROTECT, it was noted by industry port partners that “the Coast Guard seems to be everywhere, all the time,” while the number of documented reports of illicit activity increased when compared to prior operations.¹³⁹ The relevance of these increases is that “no actual increase in the number of resources applied, and therefore no increase in capital or operating costs,” occurred, which lends credibility that such an approach can increase efficiency from an adversarial perspective.¹⁴⁰

As a result, a rating of 1 is given for the efficiency criterion.

¹³⁷ Shieh et al., “PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States.”

¹³⁸ Ibid.

¹³⁹ Ibid.

¹⁴⁰ Ibid.

3. Constitutional Considerations

When considering the legal issues surrounding this option, the Fourth and Fifth Amendments are unwavering, while the path that TSA determines to travel when designing a risk-based resource deployment strategy is far more flexible. Much like Option A, and to a lesser extent Option B, the impact of these protections is more likely to come into play as a deployment methodology is operationalized, which can be addressed through proper training and oversight.

As a result, a rating of 1 is given for this criterion.

4. Social Considerations

Similarly, TSA has the ability to take public interests into account when crafting a risk-based resource deployment methodology and address potential areas of concern proactively. It includes determining whether to utilize passenger information and to what extent should the decision be made to do so.

When this flexibility is coupled with the potential that the average low-risk passengers, which is understood to be a majority of the traveling public, could more easily traverse the transportation system as security resources will be more focused on high-risk areas and passengers, a rating of 1 is given for this criterion.

5. Political Feasibility

Lastly, when considering the political feasibility of this option, a customized solution to increase the effective and efficient deployment of its resources can certainly be considered in-line with the mission of TSA. It can also be presumed that an optimized solution will ultimately result in fewer resources being needed to execute TSAs mission, which should aid in its political salience.

As such, a rating of 1 is given to this criterion.

V. FINDINGS, RECOMMENDATIONS, AND CONCLUSION

The following sections provide an overview of the findings of the policy options analysis, and several recommendations to consider for implementation.

A. FINDINGS

The challenge of optimizing decisions, such as the deployment of limited resources in the case of TSA, is something that humans have long struggled with and the gravity of TSA’s counterterrorism mission only magnifies the difficulties that lie therein.

While certainly not an exhaustive collection of possible solutions to this challenge, three distinct options were presented and analyzed using a policy options analysis framework in an effort to begin answering the question:

- How can the Transportation Security Administration (TSA) use a risk-based deployment methodology to deploy its resources in an effort to increase security effectiveness and system efficiency?

The results of this analysis are presented in Table 4.

Table 4. Policy Option Analysis Findings

	Security Effectiveness	System Efficiency	Constitutional Considerations	Social Considerations	Political Feasibility	Total
Option A	2	2	1	2	1	8
Option B	1	1	2	2	1	7
Option C	1	1	1	1	1	5

It is important to note that Option C is certainly not a panacea to the challenge; however, it is a viable risk-based solution with an ancillary benefit of being one that TSA has already begun exploring.

B. RECOMMENDATIONS

Several strategic recommendations were identified while researching the use of risk-based deployment methodologies by other entities, and are shared with the hopes of promoting a positive outcome.

1. Work with Stakeholders (Particularly the General Public)

As previously noted, the use of risk-based resource deployment methodologies within the security domain tends immediately to conjure comparisons to fictional works, such as George Orwell's novel *1984* and the 2002 film amongst the general public.

While these comparisons represent, in part, a legitimate fear of tyrannical government and loss of due process, they also represent an opportunity for police departments and other users to engage with the public and dispel such exaggerated portrayals. The first step is simply making the use of such tools as transparent as possible, much like the Kent Police did through an aggressive media campaign and willingness to share information about their own experiences. Such transparency affords a tangential benefit in that messaging can help manage expectations within both the agency and community, as many of the fictional works individuals are familiar with portray tremendous accuracy, whereas the results of current tools are less profound.

2. Mitigate Personnel Concerns and Prevent Overreliance

Similarly, departments must work with their employees to help alleviate concerns that risk-based deployment methodologies are simply a replacement for their own expertise and experience. In a recent interview, a captain with the Los Angeles Police Department compared their own use of PredPol to using a fish finder.¹⁴¹ Just as an experienced fisherman would know where to drop their line, the captain noted, "a really good officer would be able to go out and find these boxes. This kind of makes the average guys' ability to find the crime a little bit better."¹⁴²

The beauty of this analogy is that not only can many relate to it or that it strokes the ego of the "fisher," but that it subtly reinforces the reality that someone with good judgment will always be needed to hold the reel. This approach also highlights the importance of critical thinking, imagination, and judgment. These are key factors to

¹⁴¹ Berg, "Predicting Crime, LAPD-Style."

¹⁴² Ibid.

successful decision making, which is critical given the inability for current technology to generate forecasts with 100% accuracy.

The researchers and developers of such models themselves have also noted the importance of the relationship between computer models and their operators. In one such study regarding mixed-initiative approaches, “in which human users and software assistants (agents) collaborate to make security decisions,” several individuals associated with the development of GUARDS and IRIS postulated that overall performance can be increased through such interactions.¹⁴³

3. Maintain Unpredictable Security

Any formula-driven methodology in which a defined set of variables are measured and analyzed is susceptible to reverse engineering and TSA must continue to promote unpredictable security programs as a mitigation strategy against this vulnerability.

Furthermore, as noted in the discussion of Bayesian game theory in Chapter III, it is improbable that TSA will ever have the benefit of knowing all possible attack scenarios against which it must defend. As noted in the work *Fooled by Randomness*, “Probability is not a mere computation of odds on the dice or more complicated variants; it is the acceptance of the lack of certainty in our knowledge and the development of methods for dealing with our ignorance.”¹⁴⁴ While minimizing the consequence of a successful attack (provided it cannot be stopped in the first place) is an ideal risk mitigation strategy in light of this uncertainty, maintaining some semblance of what is understood as unpredictability is another.

A primary example of such a program is Playbook, which is currently “part of the various security layers operating at our Nation’s airports, serv[ing] to mitigate both

¹⁴³ Bo An et al., “Mixed-Initiative Optimization in Security Games: A Preliminary Report,” in *AAAI Spring Symposium: Help Me Help You: Bridging the Gaps in Human-Agent Collaboration*, 2011, https://course.agent.csie.ntu.edu.tw/pluginfile.php/5503/mod_resource/content/0/reading/sss11-human-agent/SS11-05-004.pdf.

¹⁴⁴ Nassim Nicholas Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets* (New York: Random House, 2005).

passenger and insider threats using a range of proven tactics, techniques and procedures [by adding] unpredictability and flexibility to security initiatives.”¹⁴⁵ A particular benefit of this program is that it provides TSA with an existing mitigation strategy that requires no change to current operations.

4. Focus on Effectiveness, Then Efficiency

Throughout this paper, effectiveness has been noted before efficiency with the intention of ensuring that the focus remains on the successful execution of TSA’s mission of protecting the nation’s transportation systems. Only once a suitable level of effectiveness has been established, with an understanding that some level of risk is likely assumed in a risk-based model, should TSA shift its focus towards identifying how to optimize the process.

C. CONCLUSION

Essentially, all models are wrong, but some are useful.

~ George E. P. Box

While Bayesian game theory risk-based deployment methodologies like IRIS and GUARDS show promise, they are far from the tools used in science-fiction works like *Minority Report*. It is important for everyone from the department that decides to pursue this capability to the community at-large to understand the potential benefits, and limitations, of the systems currently available and the challenges they present. It is also important to keep the oft-cited fears from works of science-fiction like *Minority Report* part of the conversation as a cautionary tale of what can go wrong (or right) in a world without due process.

¹⁴⁵ *Statement of John S. Pistole, Administrator, Transportation Security Administration, U.S. Department of Homeland Security, Before the United States House of Representatives, Committee on Appropriations, Subcommittee on Homeland Security, 113th Cong. (2014) (statement of John Pistole, Administrator, TSA).*

LIST OF REFERENCES

- An, Bo, Manish Jain, Milind Tambe, and Christopher Kiekintveld. "Mixed-Initiative Optimization in Security Games: A Preliminary Report." In *AAAI Spring Symposium: Help Me Help You: Bridging the Gaps in Human-Agent Collaboration*, 2011. https://course.agent.csie.ntu.edu.tw/pluginfile.php/5503/mod_resource/content/0/reading/sss11-human-agent/SS11-05-004.pdf.
- Anselin, Luc, Jacqueline Cohen, David Cook, Wilpen Gorr, and George Tita. "Spatial Analyses of Crime." *Criminal Justice* 2000 4 (2000). http://www.ncjrs.org/criminal_justice2000/vol_4/04e.pdf.
- Anyinam, Charles. "Using Risk Terrain Modeling Technique to Identify Places with the Greatest Risk for Violent Crime in New Haven." *Crime Mapping & Analysis News*, Spring 2015. <http://crimemapping.info/article/using-risk-terrain-modeling-technique-identify-places-greatest-risk-violent-crimes-new-haven/>.
- Baughman, Jonas H., and Joel Caplan. "Applying Risk Terrain Modeling to a Violent Crimes Initiative in Kansas City, Missouri." *RTM Insights*, September 2010. http://rutgerscps.weebly.com/uploads/2/7/3/7/27370595/kcpd_rtminaction_brief.pdf.
- Beane, William M. "The Constitutional Right to Privacy in the Supreme Court." *The Supreme Court Review* 1962, no. 1 (1962): 212–51.
- Berg, Nate. "Predicting Crime, LAPD-Style." *The Guardian*, June 25, 2014. <http://www.theguardian.com/cities/2014/jun/25/predicting-crime-lapd-los-angeles-police-data-analysis-algorithm-minority-report>.
- Caplan, Joel, and Leslie Kennedy. *Introduction to Risk Terrain Modeling (RTM) for Strategic Decision-Making and Tactical Action*. Newark, NJ: Rutgers Center on Public Security, 2009. http://www.rutgerscps.org/docs/IntroToRTM_Brief.pdf.
- . *Risk Terrain Modeling Compendium*. Newark, NJ: Rutgers Center on Public Security, 2011. http://www.rutgerscps.org/rtm/RiskTerrainModelingCompendium_CaplanKennedy2011.pdf.
- Caplan, Joel, Leslie W. Kennedy, and Joel Miller. "Risk Terrain Modeling: Brokering Criminological Theory and GIS Methods for Crime Forecasting." *Justice Quarterly* 28, no. 2 (2011). <http://search.proquest.com/docview/863479648?accountid=12702>.
- Dahl, Erik J. *Intelligence and Surprise Attack—Failure and Success from Pearl Harbor to 9/11 and Beyond*. Washington, DC: Georgetown University Press, 2013.

- Dillon, Robin L., Robert M. Liebe, and Thomas Bestafka. "Risk-Based Decision Making for Terrorism Applications." *Risk Analysis* 29, no. 3 (March 2009). <http://online.library.wiley.com.libproxy.nps.edu/doi/10.1111/j.1539-6924.2008.01196.x/pdf>.
- Dolićanin, Ćemal, Ejub Kajan, Dragan Randjelović, and Boban Stojanović. *Handbook of Research on Democratic Strategies and Citizen-Centered E-Government Services*. Hershey, PA: IGI Global, 2014.
- Economist, The. "Don't Even Think about It." July 20, 2013. <http://www.economist.com/news/briefing/21582042-it-getting-easier-foresee-wrongdoing-and-spot-likely-wrongdoers-dont-even-think-about-it>.
- Eloy, Michell. "APD Rolls Out Crime Predicting Program." 90.1FM WABE—Atlanta's NPR Station, September 30, 2013. <http://news.wabe.org/post/apd-rolls-out-crime-predicting-program>.
- Ferguson, Andrew G. "Predictive Policing and Reasonable Suspicion." *Emory Law Journal* 62, no. 2 (2012). <http://law.emory.edu/elj/content/volume-62/issue-2/articles/predicting-policing-and-reasonable-suspicion.html>.
- Fletcher, Kenneth C. "Aviation Security: A Case for Risk-Based Passenger Screening." Master's thesis, Naval Postgraduate School, 2011. <https://calhoun.nps.edu/bitstream/handle/10945/10601/11Dec%255FFletcher.pdf?sequence=3&isAllowed=y>.
- Friend, Zach. "Predictive Policing: Using Technology to Reduce Crime." *FBI*, April 9, 2013. <https://leb.fbi.gov/2013/april/predictive-policing-using-technology-to-reduce-crime>.
- Friendly, Michael, and Nicolas de Sainte Agathe. "André-Michel Guerry's Ordonnateur Statistique: The First Statistical Calculator?" *The American Statistician* 66, no. 3 (August 1, 2012): 195–200, doi:10.1080/00031305.2012.714716.
- Gale Lucas, Matthew D. McCubbins, and Mark Turner. "Against Game Theory." In *Emerging Trends in the Social and Behavioral Sciences: An Interdisciplinary, Searchable, and Linkable Resource*, edited by Robert A. Scott and Stephen M. Kosslyn. Hoboken, NJ: John Wiley & Sons, Inc., 2015.
- Garrick, B. John, James E. Hall, Max Kilger, John C. McDonald, Tara O'Toole, Peter S. Probst, Elizabeth Rindskopf Parker, Robert Rosenthal, Alvin W. Trivelpiece, Lee A. Van Arsdale, and Edwin L. Zebroski. "Confronting the Risks of Terrorism: Making the Right Decisions." *Reliability Engineering & System Safety* 86, no. 2 (November 2004): 129–76.
- Goode, Erica. "Data-Crunching Program Guides Santa Cruz Police before a Crime." *The New York Times*, August 15, 2011. <http://www.nytimes.com/2011/08/16/us/16police.html>.

- Greenberg, Pam. "Privacy Protections in State Constitutions." National Conference of State Legislatures, 2015. <http://www.ncsl.org/research/telecommunications-and-information-technology/privacy-protections-in-state-constitutions.aspx>.
- Griffith, Samuel B. *The Art of War*. London: Oxford University Press, 1971.
- Hall, Howard B. "Data-Driven Approaches to Crime and Traffic Safety—Its Application to Public Safety and Accreditation." *CALEA Update*, no. 103, 2010. <http://www.calea.org/calea-update-magazine/issue-103/data-driven-approaches-crime-and-traffic-safety-its-application-publ>.
- Hargreaves-Heap, Shaun, and Yanis Varoufakis. *Game Theory: A Critical Introduction*. London: Routledge, 2004.
- Harries, Keith. *Mapping Crime: Principle and Practice*. Washington, DC: National Institute of Justice, 1999. <https://www.ncjrs.gov/html/nij/mapping/front.html>.
- Harris, David A. "Particularized Suspicion, Categorical Judgments: Supreme Court Rhetoric Versus Lower Court Reality Under *Terry v. Ohio*." *St. John's Law Review* 72, no. 3 (March 2012). <http://scholarship.law.stjohns.edu/lawreview/vol72/iss3/11>.
- Hollywood, John S., Susan C. Smith, Carter C. Price, Brian McInnis, and Walter L. Perry. "Predictive Policing: What It Is, What It Isn't, and Where It Can Be Useful." 2012 Law Enforcement Information Management Conference, Indianapolis, IN, May 22, 2012. <http://www.theiacp.org/portals/0/pdfs/leim/2012presentations/ops-predictivepolicing.pdf>.
- Huie, Marsha Cope, Stephen F. Larabee, and Stephen D. Hogan. "The Right to Privacy in Personal Data: The EU Prods the U.S. and Controversy Continues." *Tulsa Journal of Comparative and International Law* 9, no. 2 (2002). <http://digitalcommons.law.utulsa.edu/tjcil/vol9/iss2/2/>.
- James, Pita, Milind Tambe, Christopher Kiekintveld, Shane Cullen, and Erin Steigerwald. *GUARDS—Innovative Application of Game Theory for National Airport Security*. Los Angeles: USC Viterbi, Teamcore Research Group, University of Southern California, 2011. http://teamcore.usc.edu/papers/2011/GUARDS_Ind2.pdf.
- Johnson, Jeh C. "Statement by Secretary Jeh C. Johnson on Inspector General Findings on TSA Security Screening." U.S. Department of Homeland Security, June 1, 2015. <http://www.dhs.gov/news/2015/06/01/statement-secretary-jeh-c-johnson-inspector-general-findings-tsa-security-screening>.
- Kelion, Leo. "London Police Trial Gang Violence 'Predicting' Software." *BBC News*, October 29, 2014. <http://www.bbc.com/news/technology-29824854>.

- Kennedy, Leslie W., and Edmund F. McGarrell, ed. *Crime and Terrorism Risk: Studies in Criminology and Criminal Justice*. New York: Routledge, 2011.
- Kent Police. Corporate Services, Analysis Department. *PredPol Operational Review*. Kent, UK: Kent Police, 2014. <http://www.statewatch.org/docbin/uk-2014-kent-police-predpol-op-review.pdf>.
- . Corporate Services, Analysis Department. *PredPol Operational Review—Initial Findings*. Kent, UK: Kent Police, 2013. <http://www.statewatch.org/docbin/uk-2013-11-kent-police-pp-report.pdf>.
- Luna, Taryn. “Retailers Tap Software to Pick Best Locations for New Stores.” *Boston Globe*, August 29, 2013. <http://www.bostonglobe.com/business/2013/08/28/retailers-tap-software-programs-select-ideal-locations-for-new-stores/f6hsWesAX2NwrPXRPeUu4O/story.html>.
- McDougall, Kevin. “A Local-State Government Spatial Data Sharing Partnership Model to Facilitate SDI Development.” Ph.D. diss., The University of Melbourne, 2006. http://www.csdila.unimelb.edu.au/publication/theses/Kevin_Mcdougall_PhD_Thesis.pdf.
- McGrayne, Sharon Bertsch. *The Theory That Would Not Die: How Bayes’ Rule Cracked the Enigma Code, Hunted Down Russian Submarines, & Emerged Triumphant from Two Centuries of Controversy*. New Haven, CT: Yale University Press, 2011.
- Moreto, William D., and Joel Caplan. *Forecasting Global Maritime Piracy Utilizing the Risk Terrain Modeling (RTM) Approach*. Newark, NJ: Rutgers Center on Public Security, 2010. http://www.rutgerscps.org/publications/MaritimePiracy_Brief.pdf.
- Nassim Nicholas Taleb. *Foiled by Randomness: The Hidden Role of Chance in Life and in the Markets*. New York: Random House, 2005.
- National Archives. “The Constitution of the United States, Amendment IV.” Accessed June 6, 2015. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.
- . “The Constitution of the United States, Amendment V.” Accessed June 6, 2015. http://www.archives.gov/exhibits/charters/bill_of_rights_transcript.html.
- National Highway Traffic Safety Administration. “Data-Driven Approaches to Crime and Traffic Safety.” Accessed July 22, 2015. <http://www.nhtsa.gov/ddacts>.
- Neffenger, Peter. “Aviation Security Challenges: Is TSA Ready for the Threats of Today?” Transportation Security Administration, July 29, 2015. <https://www.tsa.gov/news/testimony/2015/07/29/testimony-tsa-aviation-security-challenges>.

- Office of Inspector General. *Transportation Security Administration's Deployment and Use of Advanced Imaging Technology* (OIG-13-120 (Revised)). Washington, DC: U.S. Department of Homeland Security, 2014. https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-120_Mar14.pdf.
- Pauly, Glenn A., J. Thomas McEwen, and Stephen J. Finch. *Computer Mapping—A New Technique in Crime Analysis*. Washington, DC: U.S. Department of Justice, Law Enforcement Assistance Administration, 1967. <https://www.ncjrs.gov/pdffiles1/Digitization/199NCJRS.pdf>.
- Peachey, Paul. "The Real Minority Report? Kent Constabulary Tests Computer Program to Predict Crime." *The Independent*, August 4, 2013. <http://www.independent.co.uk/news/uk/crime/the-real-minority-report-kent-constabulary-tests-computer-program-to-predict-crime-8744940.html>.
- Perry, Walter L., Brian McInnis, Carter C. Price, Susan C. Smith, and John S. Hollywood. *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*. Santa Monica, CA: RAND Corporation, 2013. http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.sum.pdf.
- Reifel, Christopher S. "Quantitative Risk Analysis for Homeland Security Resource Allocation." Master's thesis, Naval Postgraduate School, 2006. <https://www.hsdl.org/?view&did=469650>.
- Shannon-Missal, Larry. "Harris Interactive: Harris Polls > U.S. Mint & FAA Receive Highest Ratings of 17 Government Agencies; FBI, CDC, NIH, CIA and Office of the Surgeon General Also Well Regarded." *The Harris Poll*, February 26, 2015. <http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/1557/Default.aspx>.
- . "Who Screens the Screeners? American Opinions on the TSA." *The Harris Poll*, April 24, 2014. <http://www.harrisinteractive.com/NewsRoom/HarrisPolls/tabid/447/ctl/ReadCustom%20Default/mid/1508/ArticleId/1419/Default.aspx>.
- Shieh, Eric, Bo An, Rong Yang, Milind Tambe, Craig Baldwin, Joseph DiRenzo, Ben Maule, and Garrett Meyer. "PROTECT: A Deployed Game Theoretic System to Protect the Ports of the United States." In *Proceedings of the 11th International Conference on Autonomous Agents and Multiagent Systems—Volume 1*, AAMAS '12. Richland, SC: International Foundation for Autonomous Agents and Multiagent Systems, 2012. <http://teamcore.usc.edu/people/eshieh/AAMAS2012-protect.pdf>.
- Starbucks Corporation. "Q2—FY14 Earnings Release." April 24, 2014.

- Stroud, Matt. “The Minority Report: Chicago’s New Police Computer Predicts Crimes, but Is It Racist?” *The Verge*, February 19, 2014. <http://www.theverge.com/2014/2/19/5419854/the-minority-report-this-computer-predicts-crime-but-is-it-racist>.
- Tsai, Jason, Shyamsunder Rathi, Christopher Kiekintveld, Fernando Ordóñez, and Milind Tambe. *IRIS—A Tool for Strategic Security Allocation in Transportation Networks*. Los Angeles: USC Vitberbi, Teamcore Research Group, University of Southern California, 2009. <http://teamcore.usc.edu/papers/2009/aamas-09-industry.pdf>.
- U.S. Department of Homeland Security Office of Inspector General. *TSA’s National Deployment Force—FY 2012 Follow-Up*. Washington, DC: U.S. Department of Homeland Security Office of Inspector General, 2012. https://www.oig.dhs.gov/assets/Mgmt/2013/OIG_13-14_Dec12.pdf.
- U.S. Department of Homeland Security. *Budget-in-Brief Fiscal Year 2014*. Washington, DC: U.S. Department of Homeland Security, 2013. <http://www.dhs.gov/sites/default/files/publications/MGMT/FY%202014%20BIB%20-%20FINAL%20-508%20Formatted%20%284%29.pdf>.
- . *Budget-in-Brief Fiscal Year 2015*. Washington, DC: U.S. Department of Homeland Security, 2014. <http://www.dhs.gov/sites/default/files/publications/FY15BIB.pdf>.
- . *Budget-in-Brief Fiscal Year 2016*. Washington, DC: U.S. Department of Homeland Security, 2015. http://www.dhs.gov/sites/default/files/publications/FY_2016_DHS_Budget_in_Brief.pdf.
- . *Office of Inspector General, Efficiency and Effectiveness of TSA’s Visible Intermodal Prevention and Response Program Within Rail and Mass Transit Systems (Redacted)* (OIG-12-103). Washington, DC: U.S. Department of Homeland Security, 2012.
- . *Risk Steering Committee, DHS Risk Lexicon*. Washington, DC: U.S. Department of Homeland Security, 2010. <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>.
- U.S. Federal Aviation Administration. “Commercial Service Airports Based on Preliminary CY 2014 Enplanements.” June 29, 2015. http://www.faa.gov/airports/planning_capacity/passenger_allcargo_stats/passenger/media/cy14-commercial-service-enplanements.pdf.
- U.S. Government Accountability Office. *Report to Congressional Committees, Aviation Security: TSA’s Staffing Allocation Model Is Useful for Allocating Staff among Airports, but Its Assumptions Should Be Systematically Reassessed* (GAO-07-299). Washington, DC: Government Accountability Office, 2007. <http://www.gao.gov/assets/260/257256.pdf>.

- . *Report to Congressional Requesters, TSA Explosives Detection Canine Program—Actions Needed to Analyze Data and Ensure Canine Teams are Effectively Utilized* (GAO-13-239). Washington, DC: U.S. Government Accountability Office, 2013.
- . *Report to the Ranking Democratic Member, Committee on Transportation and Infrastructure, House of Representatives More Clarity on the Authority of Federal Security Directors Is Needed* (GAO-05-935). Washington, DC: Government Accountability Office, 2005. <http://www.gao.gov/assets/250/247917.pdf>.
- . *Report to the Ranking Member, Committee on Transportation and Infrastructure, House of Representatives, Aviation Security, Efforts to Validate TSA’s Passenger Screening Behavior Detection Program Underway, but Opportunities Exist to Strengthen Validation and Address Operational Challenges* (GAO-10-763). Washington, DC: U.S. Government Accountability Office, 2010).
- . *Streamlining Government—Key Practices from Select Efficiency Initiatives Should Be Shared Governmentwide* (GAO-11-908). Washington, DC: Government Accountability Office, 2011. <http://www.gao.gov/assets/590/585552.pdf>.
- . *Testimony, Before the Subcommittee on Aviation, Committee on Commerce, Science and Transportation, U.S. Senate, Aviation Security—Improvement Still Needed in Federal Aviation Security Efforts* (GAO-04-592T). Washington, DC; Government Accountability Office, 2004. <http://www.gao.gov/new.items/d04592t.pdf>.
- U.S. Senate Committee on Homeland Security & Governmental Affairs. “About Efficiency and Effectiveness of Federal Programs and the Federal Workforce.” Accessed July 29, 2015. <http://www.hsgac.senate.gov/subcommittees/fp/w/about>.
- U.S. Transportation Security Administration. “Mission.” July 23, 2014. <http://www.tsa.gov/about-tsa/mission>.
- . “Risk-Based Security: What This Means for You.” August 7, 2014. <http://www.tsa.gov/pressroom-channel/risk-based-security-what-means-you>.
- . “TSA Pre✓® Reaches Milestone with More than 1 Million Travelers Enrolled.” March 24, 2015. <https://www.tsa.gov/press/releases/2015/03/24/tsa-precheckR-reaches-milestone-more-1-million-travelers-enrolled>.
- . *Transportation Security: Are Our Airports Safe?*. Washington, DC: U.S. Transportation Security Administration, 2015. http://www.tsa.gov/sites/default/files/assets/pdf/tsa_testimony5-13-15.pdf.

- . *TSA at a Glance*. Washington, DC: U.S. Department of Homeland Security, n.d. https://www.tsa.gov/sites/default/files/assets/pdf/tsaatglance_final.pdf.
- . *TSA by the Numbers*. Washington, DC: U.S. Transportation Security Administration, 2015. http://www.tsa.gov/sites/default/files/publications/pdf/tsabythenumbers_final.pdf.
- Weiss, Alexander. *Data-Driven Approaches to Crime and Traffic Safety (DDACTS)—An Historical Overview*. Washington, DC: U.S. Department of Transportation, National Highway Safety Administration, 2013. <http://www.nhtsa.gov/static/files/nti/pdf/809689.pdf>.
- Wheatley, Malcom. “Data-Driven Location Choices Drive Latest Starbucks Surge.” January 10, 2013, DataInformed. <http://data-informed.com/data-driven-location-choices-drive-latest-starbucks-surge/>.
- Willis, Henry H. “Guiding Resource Allocations Based on Terrorism Risk.” *Risk Analysis* 27, no. 3 (June 2007): 597–606.
- Yahoo! Finance. “SBUX Historical Prices.” Accessed August 7, 2015. <http://finance.yahoo.com/q/hp?s=SBUX>.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, Virginia
2. Dudley Knox Library
Naval Postgraduate School
Monterey, California