



# **NAVAL POSTGRADUATE SCHOOL**

**MONTEREY, CALIFORNIA**

## **THESIS**

**AVIATION SECURITY: A CASE FOR RISK-BASED  
PASSENGER SCREENING**

by

Kenneth C. Fletcher

December 2011

Thesis Advisor:  
Second Reader:

Robert Bach  
John Rollins

**Approved for public release; distribution is unlimited**

THIS PAGE INTENTIONALLY LEFT BLANK

|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                 |                                                                |                                                            |  |
|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------|----------------------------------------------------------------|------------------------------------------------------------|--|
| <b>REPORT DOCUMENTATION PAGE</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |                                                                 |                                                                | <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.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                 |                                                                |                                                            |  |
| <b>1. AGENCY USE ONLY (Leave blank)</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                 | <b>2. REPORT DATE</b><br>December 2011                         | <b>3. REPORT TYPE AND DATES COVERED</b><br>Master's Thesis |  |
| <b>4. TITLE AND SUBTITLE</b> Aviation Security: A Case for Risk-Based Passenger Screening                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                 |                                                                | <b>5. FUNDING NUMBERS</b>                                  |  |
| <b>6. AUTHOR(S)</b> Kenneth C. Fletcher                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                 |                                                                |                                                            |  |
| <b>7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)</b><br>Naval Postgraduate School<br>Monterey, CA 93943-5000                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |                                                                 |                                                                | <b>8. PERFORMING ORGANIZATION REPORT NUMBER</b>            |  |
| <b>9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)</b><br>N/A                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |                                                                 |                                                                | <b>10. SPONSORING/MONITORING AGENCY REPORT NUMBER</b>      |  |
| <b>11. SUPPLEMENTARY NOTES</b> 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_____.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                                                                 |                                                                |                                                            |  |
| <b>12a. DISTRIBUTION / AVAILABILITY STATEMENT</b><br>Approved for public release; distribution is unlimited                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                                                                 |                                                                | <b>12b. DISTRIBUTION CODE</b>                              |  |
| <b>13. ABSTRACT (maximum 200 words)</b><br><br><p>Since September 11, 2001, the United States has invested considerable resources to improving aviation security. Despite technology and procedural improvements, passenger screening remains subject to much criticism. Challenges to the current approach include the assumption that all passengers pose a risk; the reactive responses to new threats that are applied broadly to all passengers; high levels of threat uncertainty; a focus on objects versus people; and time constraints on completing the screening process. Combined, these challenges adversely impact performance and result in poor public acceptance of government efforts to protect the commercial aviation sector from terrorist attacks. Questions persist regarding the long-term efficacy and sustainability of the current approach and the availability of a better model.</p> <p>The approach used by Israel and a risk-based approach that calibrates security measures to groups of passengers based on risk are two frequently offered alternative screening models. This thesis evaluates the current and alternative models using security effectiveness, risk mitigation, constitutional permissibility, social acceptance, and political feasibility as evaluation dimensions. This evaluation of policy options allows a side-by-side comparison of the three models and demonstrates that adopting a risk-based security approach to passenger screening is the best option for the U.S. government to pursue.</p> |                                                                 |                                                                |                                                            |  |
| <b>14. SUBJECT TERMS</b> Aviation Security, Risk-Based Security, Visual Search, Terrorism Deterrence, Passenger Screening, First Amendment, Fourth Amendment, Fifth Amendment, Risk Mitigation, Israeli Aviation Security, X-Ray Screening, Transportation Security                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                 |                                                                | <b>15. NUMBER OF PAGES</b><br>173                          |  |
|                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |                                                                 |                                                                | <b>16. PRICE CODE</b>                                      |  |
| <b>17. SECURITY CLASSIFICATION OF REPORT</b><br>Unclassified                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | <b>18. SECURITY CLASSIFICATION OF THIS PAGE</b><br>Unclassified | <b>19. SECURITY CLASSIFICATION OF ABSTRACT</b><br>Unclassified | <b>20. LIMITATION OF ABSTRACT</b><br>UU                    |  |

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)  
Prescribed by ANSI Std. Z39-18

THIS PAGE INTENTIONALLY LEFT BLANK

**Approved for public release; distribution is unlimited**

**AVIATION SECURITY: A CASE FOR RISK-BASED PASSENGER SCREENING**

Kenneth C. Fletcher  
Senior Executive, Transportation Security Administration  
B.S., Northern Illinois University, 2000

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 2011**

Author: Kenneth C. Fletcher

Approved by: Robert Bach  
Thesis Advisor

John Rollins  
Second Reader

Daniel Moran  
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

## **ABSTRACT**

Since September 11, 2001, the United States has invested considerable resources to improving aviation security. Despite technology and procedural improvements, passenger screening remains subject to much criticism. Challenges to the current approach include the assumption that all passengers pose a risk; the reactive responses to new threats that are applied broadly to all passengers; high levels of threat uncertainty; a focus on objects versus people; and time constraints on completing the screening process. Combined, these challenges adversely impact performance and result in poor public acceptance of government efforts to protect the commercial aviation sector from terrorist attacks. Questions persist regarding the long-term efficacy and sustainability of the current approach and the availability of a better model.

The approach used by Israel and a risk-based approach that calibrates security measures to groups of passengers based on risk are two frequently offered alternative screening models. This thesis evaluates the current and alternative models using security effectiveness, risk mitigation, constitutional permissibility, social acceptance, and political feasibility as evaluation dimensions. This evaluation of policy options allows a side-by-side comparison of the three models and demonstrates that adopting a risk-based security approach to passenger screening is the best option for the U.S. government to pursue.

THIS PAGE INTENTIONALLY LEFT BLANK

## TABLE OF CONTENTS

|      |                                                   |    |
|------|---------------------------------------------------|----|
| I.   | INTRODUCTION.....                                 | 1  |
| A.   | BACKGROUND .....                                  | 1  |
| B.   | PROBLEM STATEMENT .....                           | 3  |
|      | 1. Equal-Risk Assumption.....                     | 4  |
|      | 2. Reactive Security Measures .....               | 5  |
|      | 3. Threat Uncertainty .....                       | 7  |
|      | 4. Increased Risk and Cost.....                   | 7  |
|      | 5. Public Acceptance .....                        | 8  |
|      | 6. Summary.....                                   | 9  |
| C.   | RESEARCH QUESTIONS .....                          | 10 |
| D.   | ARGUMENT .....                                    | 10 |
| E.   | SIGNIFICANCE OF RESEARCH .....                    | 14 |
| II.  | LITERATURE REVIEW .....                           | 17 |
| A.   | INTRODUCTION.....                                 | 17 |
| B.   | RISK MANAGEMENT.....                              | 17 |
| C.   | CONSTITUTIONAL QUESTIONS .....                    | 21 |
|      | 1. Unreasonable Searches and Seizures .....       | 21 |
|      | 2. Due Process and Equal Protection .....         | 23 |
| D.   | OPERATIONS RESEARCH MODELS .....                  | 27 |
|      | 1. Unknown Threat Level.....                      | 27 |
|      | 2. Assigned Threat Level .....                    | 29 |
| E.   | RISK-BASED SCREENING .....                        | 33 |
| F.   | CONCLUSION .....                                  | 36 |
| III. | RESEARCH METHODOLOGY .....                        | 39 |
| A.   | POLICY OPTIONS ANALYSIS.....                      | 39 |
|      | 1. Policy Options.....                            | 39 |
|      | a. Option A—The Current U.S. Security Model.....  | 40 |
|      | b. Option B—The Israeli Security Model .....      | 40 |
|      | c. Option C—A New Risk-Based Security Model.....  | 41 |
|      | 2. Evaluative Criteria.....                       | 42 |
|      | a. Security Effectiveness .....                   | 42 |
|      | b. System Effectiveness .....                     | 42 |
|      | c. Probability of Deterring Terrorist Attack..... | 45 |
|      | 3. Risk Mitigation.....                           | 47 |
|      | a. Threat .....                                   | 47 |
|      | b. Vulnerability.....                             | 47 |
|      | c. Consequence.....                               | 48 |
|      | d. Constitutional Permissibility .....            | 49 |
|      | e. Social Acceptance .....                        | 50 |
|      | f. Political Feasibility .....                    | 50 |
|      | 4. Expected Outcomes.....                         | 50 |

|     |    |                                                              |     |
|-----|----|--------------------------------------------------------------|-----|
|     | a. | <i>Option A: The Current U.S. Model</i> .....                | 51  |
|     | b. | <i>Option B: The Israeli Model</i> .....                     | 51  |
|     | c. | <i>Option C: New Risk-Based Security Model</i> .....         | 51  |
| 5.  |    | <b>Outcome Likelihood</b> .....                              | 52  |
|     | a. | <i>Option A: The Current U.S. Model</i> .....                | 52  |
|     | b. | <i>Option B: The Israeli Model</i> .....                     | 53  |
|     | c. | <i>Option C: New Risk-Based Security Model</i> .....         | 53  |
| B.  |    | <b>COMPARISON OF OPTIONS AND EXPECTED OUTCOMES</b> .....     | 54  |
| C.  |    | <b>CONCLUSION</b> .....                                      | 54  |
| IV. |    | <b>OVERVIEW OF PASSENGER SECURITY SCREENING MODELS</b> ..... | 57  |
| A.  |    | <b>U.S. AVIATION SECURITY MODEL</b> .....                    | 57  |
| B.  |    | <b>ISRAELI AVIATION SECURITY MODEL</b> .....                 | 62  |
| C.  |    | <b>RISK-BASED PASSENGER SECURITY MODEL</b> .....             | 68  |
| V.  |    | <b>POLICY EVALUATION</b> .....                               | 75  |
| A.  |    | <b>INTRODUCTION</b> .....                                    | 75  |
| B.  |    | <b>QUANTITATIVE EVALUATION</b> .....                         | 76  |
|     | 1. | <b>Security Effectiveness</b> .....                          | 77  |
|     | a. | <i>System Effectiveness</i> .....                            | 80  |
|     | b. | <i>Probability of Deterring Terrorist Attack</i> .....       | 88  |
|     | 2. | <b>Risk Mitigation</b> .....                                 | 93  |
|     | a. | <i>Threat</i> .....                                          | 93  |
|     | b. | <i>Vulnerability</i> .....                                   | 94  |
|     | c. | <i>Consequence</i> .....                                     | 95  |
|     | d. | <i>Risk</i> .....                                            | 96  |
| C.  |    | <b>QUALITATIVE EVALUATION</b> .....                          | 98  |
|     | 1. | <b>Constitutional Permissibility</b> .....                   | 98  |
|     | a. | <i>First Amendment</i> .....                                 | 99  |
|     | b. | <i>Fourth Amendment</i> .....                                | 104 |
|     | c. | <i>Fifth Amendment</i> .....                                 | 109 |
|     | 2. | <b>Social Acceptance</b> .....                               | 114 |
|     | 3. | <b>Political Feasibility</b> .....                           | 117 |
| D.  |    | <b>CONCLUSION</b> .....                                      | 119 |
| VI. |    | <b>CONCLUSIONS AND RECOMMENDATIONS</b> .....                 | 121 |
| A.  |    | <b>INTRODUCTION</b> .....                                    | 121 |
| B.  |    | <b>FINDINGS AND CONCLUSIONS</b> .....                        | 122 |
|     | 1. | <b>Security Effectiveness</b> .....                          | 122 |
|     | 2. | <b>Risk Mitigation</b> .....                                 | 124 |
|     | 3. | <b>Constitutional Permissibility</b> .....                   | 124 |
|     | 4. | <b>Social Acceptance</b> .....                               | 127 |
|     | 5. | <b>Political Feasibility</b> .....                           | 128 |
|     | 6. | <b>Summary of Findings</b> .....                             | 130 |
| C.  |    | <b>IMPLEMENTATION CHALLENGES AND RECOMMENDATIONS</b> .....   | 131 |
|     | 1. | <b>Physical Changes to Airport Checkpoints</b> .....         | 131 |

|    |                                                              |     |
|----|--------------------------------------------------------------|-----|
| 2. | Technology Integration and Implementation Costs .....        | 131 |
| 3. | Background Investigations and Sustaining Program Costs ..... | 133 |
| D. | AREAS FOR FUTURE RESEARCH.....                               | 134 |
| 1. | Security Officer IED Detection Performance.....              | 134 |
| 2. | Security Interview.....                                      | 134 |
| 3. | Adapting to Different Airport Configurations.....            | 134 |
| 4. | Systems Alarm Impact .....                                   | 135 |
|    | LIST OF REFERENCES .....                                     | 137 |
|    | INITIAL DISTRIBUTION LIST .....                              | 153 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF FIGURES

|           |                                                                                          |    |
|-----------|------------------------------------------------------------------------------------------|----|
| Figure 1. | Layers of U.S. Aviation Security .....                                                   | 3  |
| Figure 2. | NIPP Risk Management Framework (from Chertoff, 2009, p. 27) .....                        | 18 |
| Figure 3. | DHS Risk Management Process (from DHS, n.d., p. 8).....                                  | 20 |
| Figure 4. | Terrorist Identification Event Diagram (adapted from Schneidewind,<br>2005, p. 44) ..... | 43 |
| Figure 5. | United States Aviation Security Model .....                                              | 61 |
| Figure 6. | Israeli Aviation Security Model.....                                                     | 66 |
| Figure 7. | Risk-Based Security Passenger Categories.....                                            | 69 |
| Figure 8. | Risk-Based Security Model .....                                                          | 71 |
| Figure 9. | Probability of Detection under Fixed Conditions (from Koopman, 1956,<br>p. 506) .....    | 84 |

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF TABLES

|           |                                                                                                    |     |
|-----------|----------------------------------------------------------------------------------------------------|-----|
| Table 1.  | Security Method Effectiveness .....                                                                | 44  |
| Table 2.  | Estimated Detection .....                                                                          | 45  |
| Table 3.  | Threat Values .....                                                                                | 47  |
| Table 4.  | Consequence Estimates .....                                                                        | 48  |
| Table 5.  | Policy Options Matrix .....                                                                        | 54  |
| Table 6.  | Primary Security Measures for Each Risk Group .....                                                | 73  |
| Table 7.  | Probability of Detection (adapted from Lewis, 2006, p. 206) .....                                  | 79  |
| Table 8.  | Probability of Terrorist Identification .....                                                      | 81  |
| Table 9.  | Probability of Explosive Device Detection .....                                                    | 83  |
| Table 10. | Conditional Probability of Detection Comparison .....                                              | 88  |
| Table 11. | Definitions and Values for Thwarting a Terrorist Attempt (from Martinosi<br>& Barnett, 2006) ..... | 90  |
| Table 12. | Risk Groups Threat Values .....                                                                    | 93  |
| Table 13. | Consequence Estimates .....                                                                        | 95  |
| Table 14. | Passenger Risk Category Percentages .....                                                          | 97  |
| Table 15. | Category Risk Scores .....                                                                         | 97  |
| Table 16. | Weighted Risk Score .....                                                                          | 98  |
| Table 17. | Side-by-Side Model Comparison .....                                                                | 130 |

THIS PAGE INTENTIONALLY LEFT BLANK

## **LIST OF ACRONYMS AND ABBREVIATIONS**

|          |                                                                 |
|----------|-----------------------------------------------------------------|
| ABG      | Automated and Bio-Metrics Supported Border Control              |
| AIT      | Advanced Imaging Technology                                     |
| ALPA     | Air Line Pilots Association                                     |
| ATSA     | Aviation and Transportation Security Act                        |
| BDO      | Behavior Detection Officer                                      |
| BGA      | Ben Gurion Airport                                              |
| C        | Consequence                                                     |
| CAPPS    | Computer Aided Passenger Prescreening System                    |
| CAPPS II | Computer Aided Passenger Prescreening System, Second Generation |
| CBP      | Customs and Border Protection                                   |
| CCTV     | Closed Circuit Television                                       |
| CIA      | Central Intelligence Agency                                     |
| CIKR     | Critical Infrastructure and Key Resources                       |
| CNN      | Cable News Network                                              |
| CRS      | Congressional Research Service                                  |
| DHS      | Department of Homeland Security                                 |
| DOJ      | Department of Justice                                           |
| DTC      | Dual Target Cost                                                |
| EDS      | Explosive Detections System                                     |
| EPIC     | Electronic Privacy Information Center                           |
| ETD      | Explosive Trace Detection                                       |
| FAA      | Federal Aviation Administration                                 |
| FAM      | Federal Air Marshal                                             |
| FAST     | Free and Secure Trade                                           |
| FBI      | Federal Bureau of Investigation                                 |
| FFDO     | Federal Flight Deck Officer                                     |
| GAO      | Government Accountability Office                                |
| HSMS     | Homeland Security Management System                             |
| HSPD     | Homeland Security Presidential Directive                        |
| IAA      | Israel Airports Authority                                       |

|        |                                                         |
|--------|---------------------------------------------------------|
| IDENT  | Automated Biometric Identity System                     |
| IED    | Improvised Explosive Device                             |
| JTTF   | Joint Terrorism Task Force                              |
| MAP    | Multi-Level Allocation Problem                          |
| MDP    | Markov Decision Process                                 |
| NIPP   | National Infrastructure Protection Plan                 |
| PAL    | Pre-enrolled Access Lane                                |
| R      | Risk                                                    |
| RBS    | Risk-Based Security                                     |
| SENTRI | Secure Electronic Network for Traveler Rapid Inspection |
| SF     | Secure Flight                                           |
| SOS    | Satisfaction of Search                                  |
| SPOT   | Screening Passengers by Observation Techniques          |
| SSPSP  | Sequential Stochastic Passenger Screening Problem       |
| T      | Threat                                                  |
| TDC    | Ticket Document Checker                                 |
| TSA    | Transportation Security Administration                  |
| TSO    | Transportation Security Officer                         |
| TWIC   | Transportation Workers Identity Card                    |
| U.S.C. | United States Code                                      |
| USTA   | United States Travel Association                        |
| V      | Vulnerability                                           |
| VBIED  | Vehicle Borne Improvised Explosive Device               |
| VOL    | Value of Life                                           |

## ACKNOWLEDGMENTS

The axiom that success has many fathers is certainly true with respect to this thesis, and its completion would not have been possible without the support and encouragement of many individuals. As many who preceded me through this program can attest, the successful completion of this journey would not have been possible without our families. It would be entirely wrong if I began by expressing my thanks and acknowledgement to anyone other than my wife, Peggy. This thesis would not have been completed without her unwavering support, encouragement, and sacrifice. After spending nearly two years keeping the cat from walking on my keyboard, reading through my drafts, taking care of the house while I was locked in my study doing school work, or packing up all of our belongings and moving us from Chicago to Maryland, Peggy, I am sure, is even happier than I am that my thesis is complete.

I am very grateful for the contribution and support of several TSA colleagues. Elise Crawford and Stephanie Blum patiently tried to provide a non-lawyer with a rudimentary understanding of constitutional law, and I am very grateful. The patience they showed in trying to help me grasp constitutional law concepts and their assistance in pointing me toward various court cases were invaluable to my research and informed my analysis and conclusions. Any errors in interpretation of constitutional case law as it applies to this thesis are entirely the result of my own lack of formal legal background and are not reflective of their efforts to help me understand the legal arguments. I am also very appreciative of the assistance of Sophia Hardee who reviewed my description of the Israeli security process and provided me with additional insight. I would also like to acknowledge the support and encouragement provided to me by Gale Rossides and Kathleen Petrowsky, my two immediate supervisors during this eighteen-month-long journey. It would have been impossible for me to balance the demands of work, family, and program requirements without their willingness to absorb my periodic two-week absences to attend in-residence classes and their concern for my academic success and wellbeing.

This thesis would not have come together without the guidance and feedback of my advisor, Bob Bach, and second reader, John Rollins. I could not have selected a better committee to guide me through this process, and I am eternally grateful for their advice, feedback, and perspective as each chapter came together. Nadav Morag on the NPS faculty was also instrumental in guiding me through the proposal and literature review process. Through his efforts, I had a solid foundation to build upon and a clear map of how I wanted to approach the research, which significantly reduced my stress level and kept me on track throughout the effort. I would also like to thank Professor Stephen Mitroff at Duke University for his quick response to my unsolicited request to use his unpublished research on visual search. His willingness to provide additional research results to assist my efforts and to review and comment on my proposed design of experimentation on IED detection was gracious and much appreciated.

Finally, I would like to acknowledge the thousands of Transportation Security Administration employees responsible for aviation security, and particularly the dedicated professionals with whom I had the distinct pleasure of working during my time at Baltimore-Washington Thurgood Marshall and Chicago O'Hare International airports. The challenges they encounter during the screening of airline passengers formed the genesis of my interest in this thesis topic. Their dedication to the aviation security mission in the face of near-constant change over the past decade is inspiring and started my questioning as to whether or not a different approach to passenger screening would provide an opportunity to improve the conditions under which they work to keep the traveling public safe. I hope this thesis provides some value to improving the nature of passenger screening and positively changing the dynamics at airport checkpoints to increase the level of security effectiveness and improving the support and appreciation shown by the traveling public for the efforts of the front-line TSA employees.

## **I. INTRODUCTION**

Over 90 percent of the nation's \$5.3 billion annual investment in the TSA goes to aviation—to fight the last war. The money has been spent mainly to meet congressional mandates to federalize the security checkpoint screeners and to deploy existing security methods and technologies at airports. The current efforts do not yet reflect a forward-looking strategic plan systematically analyzing assets, risks, costs, and benefits. Lacking such a plan, we are not convinced that our transportation security resources are being allocated to the greatest risk in a cost-effective way.

Kean et al., 2004, p. 391

### **A. BACKGROUND**

The overall effectiveness of airport security screening at passenger checkpoints, and the individual performance of employees performing this function, has been the subject of much criticism for nearly two decades. Reasons cited for poor performance include: 1) individual employee aptitude, 2) insufficient employee training, and 3) reduced vigilance due to job monotony (Dillingham, 2001, p. 7). Since al Qaeda attacked the United States on September 11, 2001, the U.S. government has invested considerable attention and resources to resolving these deficiencies. Immediately following the 9/11 attacks, Congress enacted and President Bush signed into law the Aviation and Transportation Security Act (ATSA) in an effort to address many of the problems previously identified with checkpoint screening effectiveness. The most fundamental change was the creation of the Transportation Security Agency (TSA) and the transfer of responsibility for aviation security screening from commercial air carriers to the federal government. ATSA also mandated several other changes to address causes of poor performance with the passenger security screening layer of the aviation security system. Among these changes were improved employment standards, preemployment aptitude testing, formalized initial training and certification, recurrent training, and annual proficiency evaluations (ATSA, sec. 111).

Despite these changes, continuing problems with checkpoint security performance were identified by the 9/11 Commission (Elias, 2005, p. 3). The commission's final report recommended that the TSA address the human factor issues at checkpoints that

inhibit performance and improve the ability to detect explosives (Kean et al., 2004, p. 393). In 2007, the former inspector general for the Department of Homeland Security (DHS) reported that checkpoint performance had essentially not increased since 2001 (Ervin, 2007). Although reports by the Government Accountability Office (GAO) state that considerable progress has been made in improving aviation security (Berrick, 2008, p. 21), an ever-growing list of prohibited items in response to new threats, combined with the on-going challenge of balancing passenger delays and long queues at airport checkpoints, presents an environment of increasing complexity for the TSA (Kutz & Cooney, 2007, p. 5). As recently as 2008, covert testing of checkpoint performance by GAO investigators found continuing deficits in identifying prohibited items hidden on passengers or in accessible property. GAO noted that these performance deficiencies existed even when transportation security officers (TSOs) followed established procedures and correctly used the security technology available to them at checkpoints (Kutz & Cooney, 2007, p. 4).

The National Commission on Terrorist Attacks upon the United States (9/11 Commission) recommended that the TSA employ a system of interconnected security layers to deter, detect, and prevent exploitation of commercial aviation by terrorists (Kean et al., 2004, p. 392). Since 9/11, the TSA has implemented an aviation security program that includes the 21 different layers shown in Figure 1.

As depicted in Figure 1, the ability of transportation security officers to detect explosive devices during the passenger screening process remains a critical link in this layered security approach (Dillingham, 2001, p. 6). Results of covert testing of transportation security officers demonstrate that achieving and sustaining high levels of performance in detecting explosive devices remains a concern (Ervin, 2007).

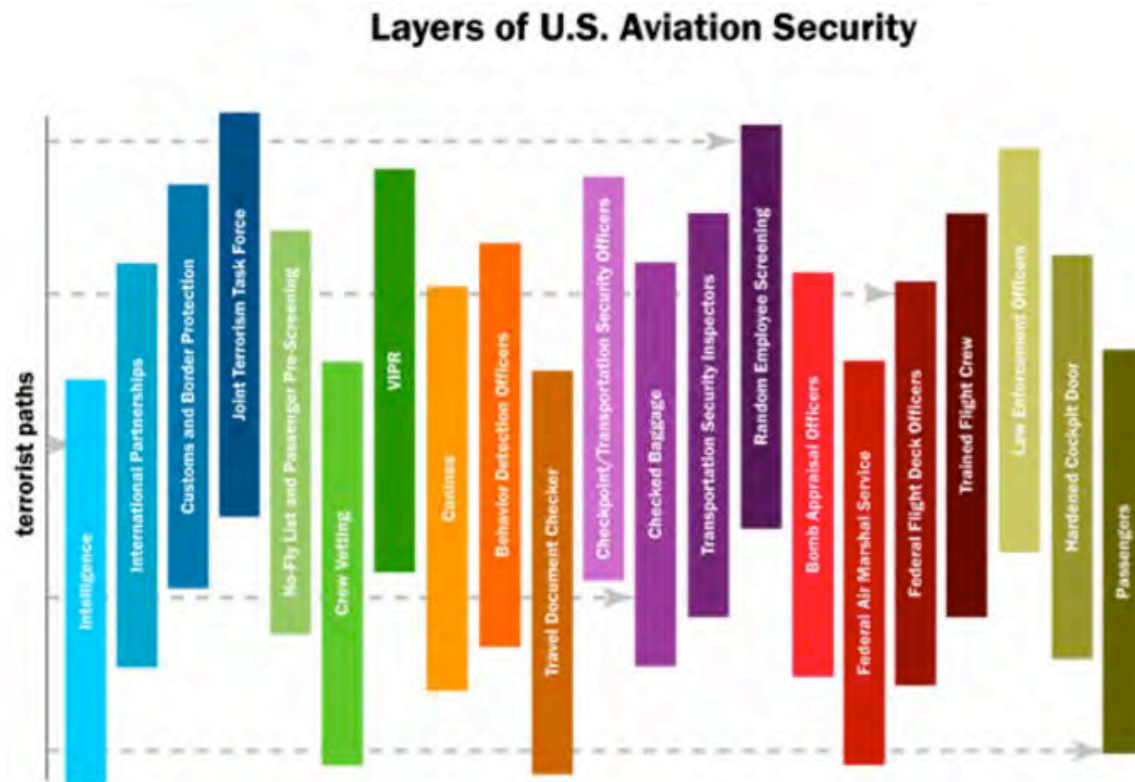


Figure 1. Layers of U.S. Aviation Security<sup>1</sup>

## B. PROBLEM STATEMENT

Several challenges associated with the current approach to passenger screening raise questions about the effectiveness and sustainability of this aspect of aviation security. These concerns include 1) an underlying assumption that *all* passengers pose risk, 2) changes to procedures and technology in response to specific threats or incidents, 3) a high level of threat uncertainty, and 4) the limited amount of time that transportation security officers (TSOs) have to screen passengers and property without creating unacceptably long wait times that would negatively impact the aviation system.

<sup>1</sup> Graphic, found at the TSA website [http://www.tsa.gov/what\\_we\\_do/layers/index.shtm](http://www.tsa.gov/what_we_do/layers/index.shtm), depicts the 21 layers that make up the aviation security approach used by the TSA (emphasis added). According to the TSA, “Each one of these layers alone is capable of stopping a terrorist attack. In combination their security value is multiplied, creating a much stronger, formidable system. A terrorist who has to overcome multiple security layers in order to carry out an attack is more likely to be pre-empted, deterred, or to fail during the attempt.”

Combined, these challenges adversely impact TSO performance and result in poor public acceptance of the government's efforts to protect the commercial aviation sector from terrorist attacks.

### **1. Equal-Risk Assumption**

Underlying the current TSA approach to aviation security screening of passengers, crew members, and airport workers is an assumption that every individual boarding a commercial aircraft poses a risk to aviation (Poole, 2006, p. 2). With very few exceptions, current TSA security regulations require that every individual who presents himself at a TSA checkpoint to board a commercial aircraft undergo primary physical security screening at screening checkpoints. In fact, the National Strategy to Combat Terrorist Travel reinforces this assumption and lists screening of all passengers and crew members as a critical element of denying terrorist entry into the aviation system (Redd, 2006, p. 31).

The equal-risk assumption drives checkpoint security screening to focus primarily on finding objects identified as prohibited for carriage aboard commercial aircraft and accessible in the passenger cabin. Reliance on the cognitive ability of security personnel to recognize and detect these objects in the face of increasingly sophisticated concealment techniques, or to recognize and react to something that experience indicates may be out of the ordinary, adds complexity to the passenger screening process that terrorists can exploit. Because all restrictions and primary screening measures are applied equally, and anyone can be subject to random additional measures to avoid profiling, the public views airport security screening and the TSA with derision.

The TSA states that, beginning in 2005, the agency has shifted the focus of airport security away from concentration on finding prohibited objects and toward a focus on intent and people, primarily through the Screening Passengers by Observation

Techniques (SPOT) program<sup>2</sup> (Simons, Brewer, & Szul, 2009). Despite this claim and the introduction of the SPOT program, checkpoint security screening has essentially not changed since 9/11 (Kutz & Cooney, 2007, p. 7). This is not to say that improvements in aviation security and checkpoint screening have not occurred. Changes in deployed technology, prohibited-items screening procedures, employee training, and covert testing have combined to improve overall passenger security screening effectiveness as compared to pre-9/11 (Berrick, 2008, p. 21). However, even when considering these improvements, it is the fundamental approach to checkpoint security screening that remains constant. All passengers are viewed as potential threats and subject to the same basic screening methods (including behavioral detection screening, X-ray screening of property, magnetometer screening for metallic objects) and secondary screening to resolve anomalies or alarms (Morgan, 2001, p. 2; Dillingham, 2001, p. 5). With the exception of behavioral detection screening, the focus of transportation security officers remains that of finding threat objects (Kutz & Cooney, 2007, p. 4).

## **2. Reactive Security Measures**

The TSA applies the professional experience of its employees to periodically reassess checkpoint screening procedures and to review the list of prohibited items. These reviews are driven by specific intelligence information, world-wide terrorist incidents targeting commercial aviation, passenger complaints, analysis of overall aviation risk, and efforts at harmonization with foreign governments (Kutz & Cooney, 2007, p. 6). Changes in terrorist tactics result in specific mitigation measures, including changes in procedure, additions to the prohibited-items list, focus areas for security personnel, or implementation of new screening technologies. Exceptions and alternative screening procedures adopted to address the concerns of specific stakeholder groups create exploitable vulnerabilities. Since the TSA assumed responsibility for aviation security

---

<sup>2</sup> The SPOT program is reflected in Figure 1, as the “behavior detection officer” layer. According to TSA, “The Behavior Detection Officer (BDO) program utilizes non-intrusive behavior observation and analysis techniques to identify potentially high-risk passengers. ... BDO-trained security officers are screening travelers for involuntary physical and physiological reactions that people exhibit in response to a fear of being discovered.” [http://www.tsa.gov/what\\_we\\_do/layers/bdo/index.shtm](http://www.tsa.gov/what_we_do/layers/bdo/index.shtm)

screening in 2002, a number of reactive adjustments to checkpoint screening procedures and prohibited items have been implemented in response to these pressures.

- Shoes: Following the unsuccessful shoe bombing attempt by Richard Reid in December 2002, the agency required that passengers remove their shoes prior to undergoing security screening. Following passenger complaints, the TSA relaxed the 100 percent removal policy and suggested that passengers remove shoes. In 2008, the agency reverted to requiring removal of all shoes, and in May 2009, it shifted to having shoes placed directly on the X-ray belt to remove clutter and improve prohibited-item detection by security officers (Transportation Security Administration [TSA], 2011a).
- Jackets and coats: In response to the simultaneous destruction of two Russian aircraft by suicide bombers in August 2004, the TSA required the removal of all outer garments prior to checkpoint screening in November 2004 (Croft, 2004, p. 1).
- Scissors: In December 2005, the TSA removed from its prohibited-items listing small scissors and tools to improve the focus of security personnel on finding improvised explosive devices (Kutz & Cooney, 2007, p. 6).
- Liquids: Immediately after British authorities foiled a plot to destroy U.S. commercial aircraft using peroxide-based liquid explosives disguised as sports drink, the TSA banned all liquids, aerosols, and gels from passing through security checkpoints. This total ban was subsequently relaxed to the current 3-1-1 policy.<sup>3</sup>
- Advanced imaging technology: Following the failed attempt to detonate an explosive charge sewn into the underwear of a suicide bomber on December 25, 2009, the TSA immediately accelerated the deployment of advanced imaging technology equipment to detect nonmetallic threats hidden beneath clothing.
- Toner and ink cartridges: When the plot to destroy cargo aircraft using printer cartridges concealing explosive devices surfaced in November, 2010, the TSA banned large-size printer and ink cartridges from all commercial passenger flights (Lipton, 2010).

---

<sup>3</sup> The TSA's 3-1-1 policy now permits containers of 3 ounces or less in a 1-quart, clear, zip-top plastic bag, one bag per passenger, with the bag removed from carry-on luggage and placed separately for x-ray inspection. Additional exemptions of medicines, infant-care needs, and personal hygiene were also implemented (TSA, 2011f).

Regularly implementing new security layers, adding items to the prohibited list, and educating transportation security officers on new concealment techniques result in a process highly susceptible to threat uncertainty,<sup>4</sup> with institutionalized vulnerabilities; it is an unsustainable strategy over time (Jackson, 2008, p. 7).

### **3. Threat Uncertainty**

As the terrorist threat evolves and new tactics are discovered, the TSA provides that information to checkpoint personnel to be alert for and detect these additional items. This reactive approach—expanding the list of items and concealment techniques that checkpoint security personnel must be cognizant of, without causing additional delays to all travelers—is not sustainable (Jackson, 2008, p. 6). Jackson refers to this concept as a “hyper-vigilant approach,” where each threat results in a specific prevention response that is applied to all individuals. The end result is overall disruption to existing security measures and potential discredit to the DHS and the TSA (Jackson & Frelinger, 2009, p. 4). Furthermore, the level of performance required by this reactive approach is not achievable within the limitations imposed by current technology and the U.S. Constitution, privacy and civil liberties concerns, and social norms. Terrorists and criminals have a significant advantage in their attempts to defeat existing checkpoint detection methods by disguising prohibited items so that they appear as innocent or ordinary objects to security personnel (Jackson, 2008, p. 5). The overall effect of changes to checkpoint security since 9/11 represents what some critics call “security theater” (Schneier, 2007).<sup>5</sup>

### **4. Increased Risk and Cost**

Another real concern about the current checkpoint screening process is the attractiveness of large crowds of passengers waiting for security screening as targets for terrorists (Poole, 2006, p. 22). Three events highlight the concern about the vulnerability

---

<sup>4</sup> Threat uncertainty refers to the fact that it is difficult to distinguish through X-ray screening everyday benign objects from similar items concealing improvised explosive devices.

<sup>5</sup> Security consultant Bruce Schneier defines “security theater” as cost-ineffective measures that look good and create an impression of security without actually improving it.

of passengers in public areas at airports. In June 2007, al Qaeda-linked operatives crashed into the front of the airport terminal in Glasgow Scotland and attempted to detonate a vehicle-borne improvised explosive device (VBIED). In November 2008, terrorists from Lashkar-e-Taiba attacked several commercial buildings in Mumbai India, including the crowded central railway terminal. More recently, a suicide bomb attack in the lobby of Domodedova Airport in Moscow on January 24, 2011, killed 35 and wounded another 168 individuals waiting for arriving passengers (Barry, 2011). The current checkpoint screening approach increases the risk of a suicide bomb attack aimed at the large queues of passengers waiting for checkpoint screening (Poole, 2006, p. 22).

Beyond creating additional vulnerabilities and adding complexity to the security process, the current passenger screening process creates significant opportunity costs. The resources required to screen every passenger and X-ray every carry-on bag, shoes, coat, and electronic device for possible threat objects pulls resources away from addressing other airport or transportation security vulnerabilities (Jackson, 2008, p. 7). The approach also limits the amount of time that can be spent evaluating each X-ray image for possible threat items without creating excessive wait times and even larger queues. In 2008, when many air carriers began charging fees for checked baggage, the TSA experienced a near immediate impact. Not only were more items of accessible property being brought through passenger screening checkpoints, the carry-on baggage was more densely packed, and X-ray images were significantly more cluttered. This combined effect creates an even greater challenge to the transportation security officer, who must spend more time evaluating images and must encounter more images per passenger. This situation raises the overall risk that a prohibited item will be missed or that large queues will become more attractive targets for Mumbai-, Glasgow-, or Moscow-style terrorist attacks.

## **5. Public Acceptance**

In addition to baseline security measures applied to all passengers, TSA employs a concept of randomness to create unpredictability in the process in an effort to hamper terrorist preoperational planning and surveillance. While randomness provides greater

unpredictability, it also creates frustration in frequent travelers who want to know what to expect and what to do to get through checkpoint screening as quickly as possible. Additionally, the random process for selecting who receives additional security also results in the TSA's being the subject of derision and ridicule when grandmothers are required to stand spread-eagle in secondary screening booths at checkpoints while undergoing handheld metal-detector screening and physical pat down (Jackson, 2008, p. 7). Public sentiment and opposition to TSA screening methods intensified when more invasive physical search procedures were introduced in November 2010 (Kravitz, 2010).

## **6. Summary**

A study of airport security effectiveness completed in 2005 used probability statistics to model the likelihood that a terrorist would go undetected and successfully get aboard an aircraft. The study recommended several measures to enhance overall airport security: 1) improved effectiveness of checkpoint security personnel, 2) improved performance of checkpoint technology, and 3) positive identification of passengers at various steps in the process from ticket counter to boarding gate (Schneidewind, 2005, p. 36). This study was not the first analysis of aviation security to conclude that there was a need for these improvements. The 9/11 Commission reached the same conclusions, and GAO reports from before 9/11 urged the FAA to improve personnel selection and training, raise performance of the process in detecting explosives, and improve passenger identification.

Since 9/11, the TSA has implemented a number of changes and additional layers to improve the overall security of commercial aviation. Although significant emphasis has been placed on improving the three recommendations identified by Schneidewind, many of the changes are intended to improve performance of a process largely unchanged since before 9/11. Checkpoint security personnel remain primarily focused on finding threat objects. As Poole pointed out in 2006, the underlying assumption that all passengers pose a risk to aviation security remains the cornerstone of the current passenger screening approach (Poole, 2006, p. 2). As a result, all passengers are subject to the same primary security measures. This approach is susceptible to threat uncertainty,

is highly reactive to changes in threats and tactics, is inefficient in its use of limited personnel and technology resources, and is poorly accepted by the American people. The existing approach also results in large crowds queued in front of security checkpoints, vulnerable to attack by a suicide bomber. Under the current passenger screening strategy, terrorists retain a decided advantage by devising more clever concealment and innovative devices designed to circumvent security procedures.<sup>6</sup> The combined challenges and continuing problems with passenger security screening raise questions about the long-term efficacy and sustainability of the current approach.

### **C. RESEARCH QUESTIONS**

#### Primary Research Question

What passenger screening model for commercial aviation might be best to address aviation security needs with respect to security effectiveness, risk mitigation, constitutional permissibility, social acceptance, and political feasibility?

#### Secondary Research Questions

What screening models are used in other domains that could provide the basis for a different model to apply to the aviation passenger screening process?

What legal, social, and civil liberty concerns might inhibit the adoption of a different model for passenger screening in the aviation security domain?

### **D. ARGUMENT**

The Transportation Security Administration (TSA) is charged with the daunting mission of protecting commercial aviation from terrorist attack. Executing the TSA mission requires front line transportation security officers to interact with and effectively screen between 1.7 million and 2 million airline passengers each day. Built upon the premise that every airline passenger and flight crew member poses some level of risk of perpetrating a terrorist attack, the current process focuses on finding prohibited items and

---

<sup>6</sup> The attempted destruction of Delta Airlines flight 263, on December 25, 2009, over Detroit provides a recent example of this point. The device sewn into the underwear of Umar Farouk Abdulmulltalab was purposely constructed and concealed to avoid detection by technology and procedures used during passenger screening.

broadly applies security screening procedures to nearly every individual who boards an aircraft (Poole, 2006, p. 2). The many changes to technology, procedures, and prohibited items implemented by the TSA in the intervening years since 9/11 reflect the highly reactive nature of the current security regime (Jackson & Frelinger, 2009, p. 4).

Separating passengers into four basic risk categories can improve overall aviation security while operating within the time and resource constraints of the total passenger security screening process. Implementing this type of risk-based screening system is not only possible; adopting such a system is imperative to protecting commercial aviation from terrorist attack over the foreseeable future. There are several potential benefits to the TSA's consideration of an improved risk-based passenger security model.

The primary reason for adopting a risk-based security approach is that such an approach can improve overall security effectiveness of passenger screening. Improved security results from shifting the focus of TSO personnel from broadly searching for objects to focusing more intently on people assessed as unknown or high risk. Categorizing passengers into four risk groups allows an increased level of scrutiny to be applied to individuals in higher risk groups. Several mathematic models demonstrate that even random categorization of passengers results in an improved overall security level of the system (Babu, Batta, & Lin, 2006, pp. 640–43; McLay, Jacobson, & Kobza, 2005, pp. 189, 194). Advancing these models to the next logical step by applying what we know about the individual to determine the category to which they are assigned allows the TSA to better determine the appropriate mix of security measures needed to maximize the probability of detecting threats from these individuals. This approach also minimizes false positive and false negative rates while reducing the ability of terrorists to defeat the system.

A second reason arguing for risk-based passenger screening is that such a system will improve TSO performance. Covert testing results made public in the past few years continue to demonstrate TSO performance deficits in detecting explosive devices. Reports by the Government Accountability Office and the DHS inspector general both conclude that aptitude, training, and vigilance are the root causes of this performance deficiency (Kean et al., 2004, p. 393; Elias, 2005, p. 3; Dillingham, 2009, p. 7). With

each passenger viewed as a potential threat, and faced with increasingly sophisticated concealment techniques, the TSO focus on finding prohibited objects increases job complexity, creates fatigue, adds time pressures to completing the screening process, and results in diminished vigilance (Kutz & Cooney, pp. 4, 5). TSO performance will not improve while system constraints remain constant or become more constrained and job complexity increases. This outcome is true even with better TSO aptitude assessments and improved training. Grouping passengers by risk allows low-risk passengers to be removed from many security measures, reduces TSO job complexity, and provides additional time to complete the screening of passengers categorized as unknown or high risk. The fact that the TSO knows that these individuals present an elevated risk will enhance their vigilance during the screening process. With more time available to thoroughly screen these individuals and their accessible property, and the knowledge that these passengers present an elevated risk to aviation security, TSO performance in detecting threats will improve.

A third reason why TSA should begin grouping passengers into risk categories is that this security process is less susceptible to negative impacts resulting from changes to airline business practices. This higher level of resilience results from fewer passengers being required to undergo the full spectrum of security measures at the airport. A recent example of negative impact as a result of airline decisions is the implementation of checked baggage fees by most carriers because they are exempt from the 7.5 percent excise tax. While this business decision generated \$2.5 billion in increased revenue during 2009, it had collateral consequences on TSA checkpoint security operations (Dillingham, 2010, p. 5). A significant negative impact was the decrease in hourly screening lane throughput as a result of more passengers bringing bags through the checkpoint to avoid these fees. In addition, passenger-accessible property is now more densely packed, presenting more complex X-ray images for security officers to evaluate and requiring more time to complete bag searches. Because security equipment and personnel resources are finite, the amount of time available for X-ray image interpretation has decreased, making detection of prohibited items more difficult. Another consequence of this decision is increased passenger wait times during peak hours and

extended peak operational periods throughout the day. The time pressure exerted on the process is also greater as queuing lines have become longer and these larger crowds are more attractive targets for suicide bombers.

Another reason that TSA should consider grouping passengers into four risk categories is the cost savings possible for overall passenger screening. As most passengers present no true threat to aviation, the many alarms that must be resolved throughout the system each day are in fact false alarms that drive costs to create capacity needed to resolve these alarms (McLay, Jacobson, & Kobza, 2008, p. 5). Broadly implementing new technology throughout all 450 commercial airports requires a significant financial investment to modify checkpoints and to purchase and install equipment. As an example, the TSA plans to deploy 1,800 advanced imaging technology (AIT) units over the next four years. The estimated cost to purchase, install, staff, and maintain these units is expected to reach \$700 million (Aviation Security Market, 2010). Even if categorizing passengers by risk permitted reducing this deployment plan by just 10 percent, DHS would save \$70 million. Spreading this same reduction across other checkpoint technologies could result in direct savings exceeding \$100 million. Reductions in TSO staffing at checkpoints is also possible as other security measures no longer need to be applied to every passenger, thus reducing the resources required to resolve false alarms on passengers posing no credible threat.

A final potential reason for adopting this approach is that it may be more constitutionally acceptable within the framework of the special-needs search exception carved out by the courts. Applying the same primary security measures to all passengers not only raises questions regarding the necessity of this approach but its constitutionality as well (Kraus, 1973, pp. 402, 409, 410). In various rulings on the constitutionality of warrantless special-needs airport searches, the courts have asserted that the level of intrusiveness should be minimal and only conducted to the extent necessary to combat the present danger (Power, 2006, p. 56). As categorizing passengers into groups based on risk appears possible, applying intrusive searches to every passenger becomes

unnecessary. Subjecting passengers who can be determined to pose less risk to more intrusive search measures than are necessary to address that risk may well be in conflict with the courts “minimally intrusive” standard.

Terrorist plots revealed since 9/11 demonstrate the persistence of al Qaeda and its affiliate organizations in targeting commercial aviation, and the sector remains a high-priority target. These plots also show that al Qaeda is highly innovative in devising explosive-device concealment methods specifically designed to circumvent existing aviation security measures. The underlying assumption of the existing aviation security process is that every passenger is considered to pose a threat (Poole, 2006, p. 2). This assumption drives a focus on finding objects versus the more risk-based approach of focusing on individuals. Since 9/11, aviation security has been largely reactive in response to the latest terrorist methodology. Reacting to changes in tactics and methods with new technology and more intrusive procedures creates a costly and unsustainable security model fraught with institutionalized vulnerabilities and frustrating to the traveling public. By adopting a system that groups passengers into four risk categories and tailoring security measures to the risk associated with each category, the TSA can more effectively and efficiently apply resources to address the intent component of threat and to avoid the costs and threat uncertainty attendant to the current approach. Adopting a risk-based security approach raises the overall security level of the system while improving TSO performance. Such a system is also more resilient to changes in airline practices, less expensive overall, and more constitutionally supportable.

#### **E. SIGNIFICANCE OF RESEARCH**

The significance of this research is that it provides an evaluation of different policy options for passenger screening in the aviation domain. Since the formation of the TSA in November 2002, several different approaches to passenger screening have surfaced. The most common call is for the United States to adopt the Israeli model—often heralded as the “gold standard” of aviation security. Several groups, including the Airline Pilots Association and the 9/11 Commission, have called for the United States to adopt a risk-based approach to aviation security screening (Kean et al., 2004, p. 391; Air

Line Pilots Association [ALPA], 2010). Arguments supporting both these options have been largely based on anecdotal evidence and supposition. Nothing in the literature contains an analytical comparison between these alternative policy options and the current passenger screening approach. The literature on aviation security deals broadly with matters of constitutionality, criticisms regarding the effectiveness of the current system, and several risk-based mathematic models. However, the literature is devoid of analytical comparison between the various options. This thesis seeks to fill that gap by analyzing the three approach options—the status quo, the Israeli model, and a proposed risk-based passenger security model—to assess whether an alternative approach would better address the criticisms discussed in the problem statement above. Since the TSA recently announced the intent to shift to a risk-based security approach for passenger screening, this research will provide some empirical basis to support that decision and potentially identify specific elements that the agency should consider adopting as part of the design of that model.

THIS PAGE INTENTIONALLY LEFT BLANK

## **II. LITERATURE REVIEW**

We must find ways of reconciling security with liberty, since the success of one protects the other.

Hamilton & Gorton, 2004

### **A. INTRODUCTION**

Since al Qaeda attacked the United States on September 11, 2001, the effectiveness of airport security processes has garnered a great deal of public, academic, and political attention. An array of literature exists regarding how the federal government should approach aviation security to protect the nation from terrorism. Similarly, a vast amount of literature is devoted to related topics of privacy, government surveillance, civil liberties, and technology to enable better security. The scope of this literature review is limited to four topics with potential to impact any decision to change the current passenger screening approach: 1) risk management, 2) constitutional questions, 3) operations research modeling, and 4) risk-based screening approaches. Sources include federal policy documents, congressional research papers, scholarly journal articles, academic research, and papers from think tanks.

### **B. RISK MANAGEMENT**

The DHS Risk Lexicon defines “risk management” as a “process of identifying, analyzing, assessing, and communicating risk and accepting, avoiding, transferring or controlling it to an acceptable level at an acceptable cost” (Schwien & Jamison, 2008, p. 27). This closed-loop process provides policy makers with the ability to weigh tradeoffs between accepting the risk or implementing specific measures to reduce or “buy down” risk. Two important factors in this tradeoff consideration are the potential effectiveness of the measure to reduce the risk and the cost effectiveness of the reduction measure being considered (Jamison, 2009, p. 9).

Risk management influences security decisions for two reasons: 1) the cost-prohibitive nature of equally securing all assets and 2) the need to balance security with individual civil rights and liberties. Federal methods for evaluating risk provide an objective approach to address these realities when allocating limited resources. The National Strategy for Homeland Security explicitly states that uncertainty and risk of another terrorist attack will persist and outlines measures to manage that risk by prioritizing resources and broadening responsibilities for protecting critical assets (Bush, 2002, p. 25). The principles of deterring terrorist attacks, reducing vulnerabilities, and mitigating the consequences form the foundation of the Homeland Security Management System (HSMS) (Bush, 2002, pp. 25–30, 44–46).

Building on these risk management principles, the National Infrastructure Protection Plan (NIPP) provides a six-step model to protect critical physical and cyber assets.

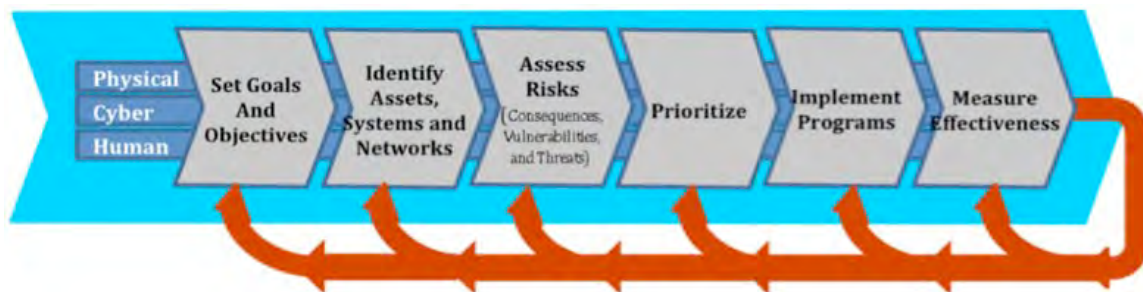


Figure 2. NIPP Risk Management Framework (from Chertoff, 2009, p. 27)

Defining risk as the product of threat, vulnerability, and consequence, the model recognizes that risk results from the interaction of these factors (Chertoff, 2009, p. 27; Masse, O’Neil, & Rollins, 2007, p. CRS-6). The NIPP requires federal departments to use this common method to enable “cross-sector” comparisons to determine where and how to apply limited homeland security resources (Chertoff, 2009, p. 27). Broad guidance for using the methodology recognizes unique differences between critical infrastructure and key resource (CIKR) sectors dominated by “physical assets” and those with more “accessible and distributed systems.” For asset-heavy sectors, the NIPP

recommends a “bottom-up, asset by asset” method, where assets are ranked based on risk. More open sectors should use a “top-down” continuity approach that considers critical system nodes and interdependencies to determine risk (Chertoff, 2009, p. 28).

Building on the NIPP model, in January 2009, DHS published an Interim Integrated Risk Management Framework, the model reflected in Figure 3. This guidance again emphasized the need for “a common and consistent approach to risk management” that united and standardized the efforts of all “organizations responsible for homeland security” (Jamison, 2009, p. 1). The intent of the risk-management framework was that it would be compatible with other approaches, including the NIPP, recommendations by the Government Accountability Office (GAO), and the method used in the Target Capabilities List. This risk-management framework provides a general model that can be adapted to many different risk-management applications across the DHS enterprise (Jamison, 2009, p. 9). Comparing the NIPP and risk-management models in Figures 2 and 3 shows that, while they use slightly different terminology, both models contain essentially the same six components.

What both of the federal risk-management models lack are the specific details on how to apply these models to open systems like transportation and how to adapt these methods to reflect the top-down continuity approach identified as appropriate for these distributed networks. This lack of implementation detail provides significant latitude to alter the risk-management approach that threatens to undercut the benefits of a common framework. Without consistent application of these principles, it becomes impossible to compare risk across sectors and systems and to determine the appropriate policies to reduce risk where it is greatest.



Figure 3. DHS Risk Management Process (from DHS, n.d., p. 8)

Critics of the federal risk management approach note that the classified nature of threat and consequence information prevents transparency, and federal grants funds prioritize buying down risk in major urban areas, which leaves state and local governments to address other vulnerabilities. (Masse, O’Neil, & Rollins, 2007, pp. CRS-9–10). These criticisms reflect the distinction between “asset-based” and “geographic-based” risk and create partisan political positioning for limited grant funds (Masse, O’Neil, & Rollins, 2007, p. CRS-20). Masse, O’Neil, and Rollins argue that, without a “cohesive risk strategy” and common terminology, the nation will be maladapted to “changing threats” and subject to greater impact from “political influence” and uncertain future funding (Masse, O’Neil, & Rollins, 2007, p. CRS-25).

## **C. CONSTITUTIONAL QUESTIONS**

The escalating intrusiveness of increased aviation security measures continues to raise questions about the appropriate balance between security effectiveness and erosion of civil liberties. Rather than remaining a unique post-9/11 phenomenon, the debate over where this balance point should be set has been going on for several decades. Literature on this subject comes primarily from several types of sources: 1) law review articles that provide interpretation of various court decisions regarding constitutional protections, 2) analysis of constitutional provisions and their impact on security initiatives by think tanks, and 3) the judicial decisions themselves. Additional information is found in targeted academic research, including dissertations and theses for postgraduate and doctoral degree work. The two sections of the U.S. Constitution that primarily impact permissible security measures in the aviation security environment are the Fourth and Fifth Amendments.

### **1. Unreasonable Searches and Seizures**

The Fourth Amendment to the United States Constitution guards against unreasonable search and seizure by the government, and holds that

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

A good body of literature exists on the impact of the Fourth Amendment on aviation security practices, and most of this literature asserts that the idea of “reasonableness” evolves over time and is highly dependent on how seriously the courts and public perceive the threat. The evolution of various court cases supports the idea that reasonableness of government searches is highly situational, dependent and subject to three varying levels of court review. A report by the Markle Foundation in 2002 outlined these levels in an analysis of legal constraints on profiling and government watch lists. According to the report’s authors, the legal hurdle is easiest to overcome when the search involves no “individualized suspicion” (Breverman & Ortiz, 2002, p. 150). In general, the

courts have included in this category routine administrative searches, such as those currently occurring at airport security checkpoints or international border searches. The next higher hurdle involves searches following reasonable suspicion. Searches of individuals stopped and detained by police officers and searched for weapons, commonly referred to as “Terry stops,” fall into the category of reasonable-suspicion searches.<sup>7</sup> The most significant hurdle involves probable cause searches. These searches invoke the highest burden of proof by government officials and usually require a warrant as specified in the Fourth Amendment (Breverman & Ortiz, 2002, pp. 151, 154).

Following 9/11, Viscusi and Zeckhauser’s survey of Harvard law students in 2002 reflects this valuation of liberty in balance with perceived risk and personal impact on public attitudes. Their hypothesis regarding civil liberties was not whether searches of aviation passengers was appropriate but rather how individuals perceived the erosion of civil liberties if these searches targeted specific groups of passengers. Analysis of the survey results led the authors to the conclusion that by and large U.S. citizens do not view “many legal rights and liberties” as inviolate, but rather attitudes change depending on perceptions of risk and individual impact (Viscusi & Zeckhauser, 2003, pp. 101–102, 105). In a *Widner Law Journal* article, Power makes the similar point that Fourth Amendment protections are changeable based on how “society expect[s] government to respond to terrorism” (Power, 2006, p. 43). Similar to the findings in the Harvard study, Power concluded that, as public perceptions of risk change, expectations of privacy also change “with the result that the Fourth Amendment no longer applies to some very intrusive governmental actions” (Power, 2006, p. 48). As an example of how court and public perceptions of reasonableness have altered interpretations of the Fourth Amendment, Power notes that prior to the ruling in *United States v. Bell*, 464 F.2d 667 (2d Cir. 1972), even magnetometer searches were perceived as “unreasonable” intrusions and justified only by the wave of hijackings occurring throughout the world (Power, 2006, p. 56). Minert, in a *Brigham Young University Law Review* article, also cites the

---

<sup>7</sup> In *Terry v. Ohio*, 392 U.S. 1 (1968), the United States Supreme Court ruled that “a police officer is entitled, for the protection of himself and others in the area, to conduct a carefully limited search of the outer clothing of individuals in an attempt to discover weapons which might be used to assault the officer, and such a search is a reasonable search under the Fourth Amendment.”

*Bell* ruling and notes that in *United States v. Epperson*, 454 F.2d 769 (4th Cir. 1972), the Fourth Circuit ruled that a “warrantless search” using magnetometers was essentially not, unlike a *Terry* search, an exception to the requirement to obtain a search warrant (Minert, 2006, p. 1642).

A *University of Chicago Law Review* article written shortly after the *Bell* decision, analyzed the constitutionality of airport searches. Citing the U.S. Supreme Court decision in *Dunn v. Blumstein*, 405 U.S. 330 (1972), Kraus notes that “the Supreme Court has protected the right of persons to travel from state to state and overseas” and asserts that it is “constitutionally impermissible” to place a “double burden” on airline passengers by forcing passengers to choose between their right against unreasonable search or their right to travel. Krause further asserts that requiring every passenger to submit to even the minimally invasive magnetometer search is “constitutionally suspect” (Krause, 1973, pp. 409–10). While acknowledging that *Terry* permits warrantless searches to address immediate danger, Krause argues that extending the officer safety exception to any warrantless search beyond that need is a violation of constitutionally protected rights (Krause, 1973, p. 402). Referencing *Bell* three decades later, the Fourth Circuit reinforced the warrantless special-needs searches at airports, ruling in *Epperson* that these searches are essentially no different than officer safety searches of subjects permitted under *Terry* (Minert, 2006, p. 1642).

## **2. Due Process and Equal Protection**

Constitutional arguments against profiling for security or law enforcement purposes by federal officials stem from the implied guarantee of equal protection under the law contained in the Fifth Amendment to the U.S. Constitution, which states:

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of War or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Despite constitutionality questions, under certain circumstances profiling is permissible. In *United States v. Brignoni-Ponce*, 422 U.S. 873 (1975), the U.S. Supreme Court ruled that the use of appearance, including one's race, can be a permissible factor for police officers to consider in a reasonable-suspicion search when the officers "are aware of specific articulable facts, together with rational inferences from those facts." Most recently, the First Circuit ruled in *United States v. Ramos*, 629 F.3d 60 (1st Cir. 2010), that "in a reasonable suspicion inquiry, a person's appearance is not per se an impermissible or irrelevant consideration." The *Ramos* ruling further found that circumstances including apparent race do not "forbid the officers' consideration of the information that at least two of the van's occupants appeared to be Middle Eastern. Groups claiming to be affiliated with Middle Eastern terrorist groups had made a specific threat to the United States just weeks earlier ... and concern about terrorism was intense."

The Department of Justice (DOJ) believes profiling—including the use of race—is permissible by federal employees involved in law enforcement or aviation security duties to address "national security" or border integrity concerns. (United States Department of Justice [DOJ], 2003, p. 12). Justifying this position, the DOJ asserts that "no governmental interest is more compelling than the security of the Nation," a rationale that permits federal personnel to use profiling to prevent "catastrophic events." This national-security exception must be within the boundaries established by law and cannot be a "pretext for invidious discrimination" (DOJ, 2003, pp. 12–13).

Department of Justice guidelines regarding profiling do permit the use of race by federal personnel involved in law enforcement or aviation security duties when involved in "threats to national security or the integrity of the nation's borders" (DOJ 2003, p. 12). The stated justification for this exception is that "it is obvious and unarguable that no governmental interest is more compelling than the security of the Nation," (*Haig v. Agee*, 453 U.S. 280 (1981); *Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964)). This guidance provides authorization for federal personnel to use all means permitted by law to prevent "catastrophic events" but cautions that the claim of a national security compelling interest must not be a "pretext for invidious discrimination" (DOJ, 2003, pp. 12–13).

The DOJ position is supported by several studies. Markle Foundation researchers similarly conclude that profiling is constitutionally permissible and that neither Fourth Amendment hurdles of “reasonableness” nor Fifth Amendment equal protection considerations constrain profiling to any great extent except in limited situations (Breverman & Ortiz, 2002, p. 153). In their analysis, the authors concluded that none of the three hurdles of “reasonableness” under the Fourth Amendment “imposes meaningful constraints on profiling” except in limited situations (Breverman & Ortiz, 2002, p. 153). Citing the unanimous Supreme Court ruling in *Whren v. United States*, 517 U.S. 806, 813–18 (1996), the analysis notes that the intent of the individual engaged in profiling does not violate the Fourth Amendment. What does impact the potential constitutionality of profiling is the equal protection clause of the Fifth Amendment (Breverman & Ortiz, 2002, p. 152). Herzog, in the *Florida Coastal Law Review*, also concludes that profiling is constitutionally permissible when “the profiled person is more likely to cause harm” and when profiling meets the “compelling government interest” to protect the nation from terrorist attacks (Herzog, 2005, p. 386).

In a *Yale Law Review* analysis of the constitutionality of the federal government’s “no-fly list,” Florence identifies three individual liberty areas of judicial concern with respect to the due process clause of the Fifth Amendment. These constitutional concerns involve impacts on an individual’s travel, occupation, and personal reputation (Florence, 2006, p. 2159). With respect to aviation passenger screening, the freedom to travel and personal reputation are applicable. Florence asserts that, while the constitution does not specifically guarantee freedom of travel, this freedom is a “fundamental right” within the commerce clause in Article IV; he references *United States v. Guest*, 383 U.S. 745 (1966), in which the court presented the idea that “a right so elementary was conceived from the beginning to be a necessary concomitant of the stronger Union the Constitution created” (Florence, 2006, p. 1160). He also cites the ruling in *Kent v. Dulles*, 357 U.S. 116 (1958), in which the court ruled that “the right to travel is a part of the ‘liberty’ of which the citizen cannot be deprived without due process of law” (Florence, 2006, p. 2161). Herzog argues a similar position, citing *Kent* and the majority opinion in *Zemel v. Rusk*, 381 U.S. 1 (1965), wherein the Supreme Court noted that “the right to travel within

the United States is of course also constitutionally protected” but can be limited by the government when there is an overriding and compelling national interest that warrants restrictions. (Herzog, 2005, p. 386).

Power and Herzog both provide substantive analyses of profiling. Power notes that the courts by and large “pretend” that the negative impacts on society as a result of profiling “do not exist.” To bolster that claim, Power cites the Supreme Court decision in *United States v. Sokolov*, 486 U.S. 1005 (1988), in which the court took a neutral stance regarding whether or not the use of racial profiling helped or hindered the determination of reasonable suspicion (Power, 2006, p. 63). Herzog posited a similar argument that profiling is not inherently in conflict with the equal protection clause if airport searches are “analogous to boarder searches” because the Supreme Court in *United States v. Montoya De Hernandez*, 473 U.S. 531 (1985), had ruled that such searches are permissible “without individualized suspicion even if the stop is based largely on ethnicity” (Herzog, 2006 p. 390). Breverman and Ortiz support this same contention and note that in *United States v. Weaver*, 966 F.2d 392 (8th Cir. 1992), the court found that, even when race was the predominate reason for stopping a suspect, this profiling did not find any conflict with guarantees of equal protection (Breverman & Ortiz, 2002, p. 155).

Although this literature supports the contention that Fourth Amendment rights are not inviolate and that Fifth Amendment guarantees of equal protection can be diminished in the face of compelling national security interests, it does not address the limits of government action when exercising special-needs searches. Since 9/11, the level of intrusiveness for special-needs searches has increased substantially, and the literature fails to address whether it is appropriate to apply these intrusive warrantless search methods broadly to individuals without any suspicion that they pose a threat. Similarly, the literature does not discuss how alternative methods to determine the level of risk posed by an individual passenger and the application of varying levels of intrusive search to mitigate that risk could be impacted by the Fourth and Fifth Amendments. Finally, the literature fails to address how the Fifth Amendment’s due process clause impacts the government’s power to engage in profiling and to place restrictions on air travel for compelling national security reasons.

## **D. OPERATIONS RESEARCH MODELS**

In the intervening years since 9/11, several mathematic models have emerged from the fields of operational research and industrial engineering to improve passenger screening methods. These models can be grouped into two basic categories: 1) those that assume that the threat posed by an individual passenger is unknown and 2) those that attempt to classify passengers into categories by risk. The objective of both approaches is to maximize the security level<sup>8</sup> of the entire passenger screening system. This overarching objective is achieved by maximizing the overall system probability of detecting threats while minimizing false positives and false clears.<sup>9</sup> Underlying both approaches is the premise that security methods are divided into primary screening measures applied to all passengers and secondary measures applied in various combinations to classes of passengers generally reflecting risk.

### **1. Unknown Threat Level**

Models that assume that the threat posed by individual passengers is unknown mirror the current TSA screening process. Like the current TSA practice, these models randomly assign passengers to some level of secondary screening, based on an underlying premise that a random and unpredictable process improves the deterrent effect of passenger screening. Where these models differ from the current U.S. approach is in their focus on improving process efficiency by reducing the percentage of false positive alarms while maximizing the security level of the system.

An example of the unknown or constant threat probability model approach was published by researchers from the Institute for Safety and Security in Transportation at the University of Buffalo. Under this model, passengers are randomly grouped into different subcategories based on an assessment of the overall threat probability, while

---

<sup>8</sup> For the purposes of this thesis, “security level” is defined as the probability of detecting a threat object when the threat object is actually present. The security level is dependent on the capability of security equipment to detect various threat objects and assumes that there is an equal likelihood that the threat object will be present in the property carried aboard the aircraft by the passenger or is on the passenger proper.

<sup>9</sup> A false positive is a threat alarm when no threat is present. A false clear is no threat alarm when a threat is present.

factoring in the probability of detection and the probability of false alarm of the equipment used for each screening method (Babu, Batta, & Lin, 2006, pp. 643–44). The authors hypothesize that it is possible to improve the overall efficiency of the process without sacrificing security effectiveness by treating passengers as if they pose different degrees of threat even when that difference is not known (Babu, Batta, & Lin, 2004, p. 643). The random selection process used in the model avoids profiling passengers based on any specific categorization, thereby minimizing civil rights and liberties concerns.

The researchers base their model on the following assumptions: 1) all passengers pose an equal threat; 2) a maximum of 30 minutes is available to screen the passenger; 3) the total time required to pass through all stations is under 30 minutes; 4) space is sufficient for required security equipment; 5) primary methods apply to all passengers with random assignment to secondary measures; and 6) an alarm at any station in the system is considered a system alarm (Babu, Batta, & Lin, 2004, pp. 634, 638, 641, 644). The model uses eight check stations, four stations as primary and the remaining four as optional for secondary searches. Primary stations include 1) check in, 2) checked baggage screening with X-ray, 3) passenger screening with imaging or metal detector, and 4) X-ray screening of accessible property. Optional measures are 1) physical search of checked baggage, 2) thorough search of passenger, 3) physical search of accessible property, and 4) gate search of passenger and property (Babu, Batta, & Lin, 2004, p. 640). Threats are broken down into four broad types—false identification, explosive in checked baggage, weapons on person, and weapons in accessible property.

Using nominal detection values derived from open sources and a 0.1% probability that a passenger possesses a threat item, the model was run for an estimated 1,000 passengers to determine an optimal percentage of passengers that should be assigned to a varying number of groups (from one to four) (Babu, Batta, & Lin, 2004, p. 641). The authors concluded that efficiency of the process is improved when four random groupings are used and assigned to different combinations of the optional secondary screening methods. This result achieves a system security level between 0.94 and 0.99 with the lowest false alarm value (Babu, Batta, & Lin, 2004, pp. 641, 643). The authors postulate

that the sensitivity of the model solution can be altered to reflect desired reductions in false clear rate limits during higher threat conditions by altering equipment sensitivity and TSO attention levels (Babu, Batta, & Lin, 2004, p. 640–42).

Unlike the current U.S. approach, maximizing efficiency and effectiveness under the equal-threat model results in a significant increase in the percentage of passengers assigned to secondary screening for reasons other than alarm resolution. The model results reflect just 22.9 percent of passengers processing through only the four primary screening stations. Nearly 30 percent of all passengers would be subject to hand searches at the checkpoint, with an additional 30 percent selected for random searches of their accessible property and their body during gate screening. These percentages represent dramatic increases above current resource levels and would require additional capacity and personnel to achieve an optimum security level for the entire system. What the results of this model do show is that the current TSA approach to implementing the equal-risk assumption philosophy is inadequate to achieve optimum security effectiveness through random and unpredictable assignment to secondary screening methods.

## **2. Assigned Threat Level**

Models that assign passengers to different threat levels based on assessed risk are formulated as system optimization models. Two such models are the Multi-level Allocation Problem (MAP) and the Sequential Stochastic Passenger Screening Problem (SSPSP). Under the MAP methodology, passengers are grouped by threat level scores assigned prior to their arrival at the airport. The model then optimizes the screening process based on fixed and variable costs (McLay, Jacobson, & Kobza, 2006, p. 184) In the SSPSP model, the threat level for a passenger is not assigned until they check in for their flight; the Markov Decision Process<sup>10</sup> is used to assign passengers to different screening measures based on the remaining capacity in the system at the time of

---

<sup>10</sup> Markov Decision Process is a random process where the outcome is dependent on the current state of the process.

assignment (McLay, Jacobson, & Nikolaev, 2008, p. 577). In both models, the objective is to maximize the security level for the system while concurrently maximizing the efficiency level of the process by using all search positions to maximum capacity.

Both models are structured as discrete optimization or knapsack problems<sup>11</sup> and have several common assumptions (McLay, Jacobson, & Kobza, 2006, p. 185; McLay, Jacobson, & Nikolaev, 2008, p. 577). These common assumptions include 1) that adequate procedures and capacity exist to resolve system alarms; 2) that adequate space exists to install the necessary quantity of security equipment at all search positions; 3) that a method such as CAPPS<sup>12</sup> or Secure Flight<sup>13</sup> exists to identify and assign individual passenger threat levels; and 4) that all passengers arrive in sufficient time to clear the screening process (nominally 60 minutes prior to departure) (McLay, Jacobson, & Kobza, 2006, pp. 184, 185; McLay, Jacobson, & Nikolaev, 2008, p. 578).

Unique aspects of the MAP model include independent threat-level assignment prior to the passenger's arriving at the airport, variable number of passenger threat groupings (3, 5, and 8), and the assumption that all passengers have exactly one checked bag and one item of accessible property (McLay, Jacobson, & Kobza, 2006, pp. 185–88). The unique assumptions in the SSPSP model are that all passengers check in sequentially, are assigned a threat value at check-in resulting in their being placed into either the selectee or non-selectee group, more screening measures are applied and equipment allocated to the selectee group, and sufficient non-selectee capacity exists for all passengers (McLay, Jacobson, & Nikolaev, 2008, p. 578).

---

<sup>11</sup> A knapsack optimization problem looks at the capacity existing in the system and assigns reward values to each item about to enter the system so that the maximum total reward is attained while using as much system capacity as possible. For security screening, the capacity constraint is the capacity of the selectee class, and the reward is the assigned risk level for each passenger. Maximum reward is determined by the highest overall security level for the system.

<sup>12</sup> CAPPS is a Computer Aided Passenger Prescreening System used by the airlines to identify higher risk passengers based on a number of preset profile criteria.

<sup>13</sup> Secure Flight is the replacement process for CAPPS operated by the Transportation Security Administration and is used for vetting passengers against terrorist watch lists and no-fly lists.

The MAP model seeks to maximize total security while satisfying budget and capacity constraints. MAP assumes that 80 percent of passengers are assessed as low risk. Assignment of N passengers to M security classes is determined by the budget allocation for each class of passengers based on the fixed and marginal costs<sup>14</sup> associated with the screening method used for that group of passenger (McLay, Jacobson, & Kobza, 2006, pp. 185, 186). The authors use seven security methods for the MAP model and designate metal detector passenger screening and X-ray accessible property screening as primary measures applied to all passengers. The remaining five security methods are grouped in various combinations depending on the number of threat classes selected (McLay, Jacobson, & Kobza, 2006, p. 189).

The researchers show the results of running the MAP model using the 3, 5, and 8 threat groupings for three different projections of passenger volume. The authors conclude that fewer threat classes are better since they produce the highest security level at the lowest total cost. The security level for higher risk passenger groups is between 0.927 and 0.964 with the false clear level below the FAA established level and the total cost for each class optimized (McLay, Jacobson, & Kobza, 2006, pp. 189, 194). This result suggests that by differentiating passengers according to threat level and applying varying security methods based on the assessed threat, it is possible to improve both the effectiveness and the efficiency of the passenger screening process as opposed to the current TSA approach that assumes each passenger represents an equal threat and applies the same level of screening to all.

Although another discrete optimization problem, the SSPSP model differs from the MAP approach in several important ways. While MAP optimizes security levels while minimizing costs, the goal of SSPSP is to optimize security levels by maximizing the assignment of passengers to the selectee group while not exceeding the capacity constraints of the associated selectee screening methods. SSPSP achieves this goal by assigning the passenger to either the selectee or non-selectee groups as he checks in at the

---

<sup>14</sup> Fixed costs equal the purchase cost of each component associated with the class. Marginal costs reflect the direct cost to screen each passenger or bag through the equipment assigned to each class and include salary, consumables, and other noncapital expenses that can be allocated on a per capita basis.

airport. SSPSP uses a real time Markov Decision Process (MDP) for assignment to the selectee group depending on the high-risk capacity remaining in the system at the time of assignment and the expected number of arrivals in the future (McLay, Jacobson, & Nikolaev, 2008, pp. 577, 578). The overall screening system security level is determined by the conditional probability of a true alarm and the conditional probability of detecting a threat item on a passenger irrespective of their assigned risk level (McLay, Jacobson, & Nikolaev, 2008, p. 578). Running the SSPSP model with an expected 1,000 passenger arrivals resulted in a total security level score of between 0.71 and 0.74 (McLay, Jacobson, & Nikolaev, 2008, p. 586).

The SSPSP model biases passengers into the selectee category at the beginning of the cycle as the method of maximizing the overall security level. This approach maximizes the use of designated selectee screening methods but drives resource requirements upward because several search methods are used continuously instead of solely for alarm resolution. Two aspects of the SSPSP model leave the approach vulnerable to gaming the system by terrorist groups. First, a known high-risk passenger may be assigned to the non-selectee group when a high number of future arrivals is expected as some selectee capacity is reserved for these future arrivals. Second, the model is vulnerable to a large number of high-risk passengers all arriving at the same time late in the cycle when most selectee capacity is already in use (McLay, Jacobson, & Nikolaev, 2008, pp. 581, 582). An example would be the large number of terrorists similar to the 9/11 attacks arriving simultaneously at the end of any designated cycle, resulting in some likely being assigned to the non-selectee group even though the intelligence information indicates that they present a higher risk.

Several problems arise in the practical application of risk-based screening models not addressed in this literature. Some models appear to drive a requirement for more resources than currently required as larger numbers of passengers are screened by methods currently used for alarm resolution only. Additionally, the literature shows that some of these approaches are susceptible to “gaming” by terrorists timing their arrival at an airport or arriving in larger groups, which can increase the probability that some will be designated as low risk even though their actual risk level may be elevated. Finally, any

risk-based passenger screening approach requires security and airline personnel to be able to identify and track passengers from check-in to boarding to ensure that they undergo the appropriate level of screening. The literature is devoid of any review of risk evaluation, methods to identify and track passengers at airports, or the costs associated with the implementation and operation of such systems.

## **E. RISK-BASED SCREENING**

The expectation that all passengers and their property will be screened prior to boarding commercial aircraft stems from the Aviation and Transportation Security Act (ATSA), P.L. 107-71, Sec. 101. However, the legislation recognizes the potential benefits of “trusted passenger programs” that apply varying levels of scrutiny to passengers based on the risk they may pose to aviation ATSA, Sec. 109. Despite this latitude, 100 percent screening is firmly entrenched in our aviation security strategy, with the National Strategy for Combating Terrorist Travel citing screening of “all passengers, operators, crew members, and baggage” as critical to strengthening transportation security (Redd, 2006, p. 31).

Several studies note that applying the same level of screening to all passengers results in “substantial costs” and the approach is likely unsustainable over time. Cost considerations include direct costs for equipment and personnel and indirect costs associated with passenger delays and opportunity costs where resources are not available to address “other security measures” (Jackson, 2008, p. 7). The opportunity cost consideration is important when determining how to allocate scarce resources across competing homeland security demands—even within the transportation sector alone (Jackson & Frelinger, 2009, p.1). To provide a more efficient and cost-effective screening model, several risk-based passenger screening concepts have surfaced based on the idea that passengers should be separated into different risk categories with different screening requirements applied to each category.

Since the late 1990s, the United States has used some version of an automated profiling system to improve aviation security. The initial system was recommended in the White House Commission on Aviation Safety and Security report, which called for

“developing an automated profiling system tailored to aviation security ... and implementation of such a system” (Gore, 1997, Sec. 3.19). This recommendation became the Computer Assisted Passenger Pre-Screening System (CAPPS), implemented in 1998, which was used to identify passengers believed to pose a higher risk to aviation. While the exact listing of the 40 or so characteristics from which suspicious travelers are identified for increased screening is classified, the criteria is believed to include travel history, cash or credit purchase, one-way purchase, date of purchase and departure, and address (Fiske, 2010, pp. 180–81). Although viewed as a significant improvement in pre-screening passengers as a means of identifying individuals who would be subject to greater security scrutiny, the CAPPS system relied entirely on the passenger’s providing accurate information and avoiding patterns that could indicate abnormal traveler behavior (Fiske, 2010, p. 181). The CAPPS program did successfully identify half of the 9/11 hijackers, but the program at that time required only increased screening of checked baggage and not the passengers themselves (Kean et al., 2004, p. 392).

To strengthen the pre-screening process, the Aviation and Transportation Security Act (ATSA) required the newly established TSA to improve CAPPS (ATSA, Sec. 136). The enhanced passenger pre-screening system was named CAPPS II and represented several improvements over the original CAPPS approach. These improvements included validating the identity of every passenger during the reservation/ticketing process and conducting an individual risk assessment of every passenger using a combination of information from commercial and government databases (Kite, 2004, p. 1391). This combination of identity verification and assigning a risk score to every passenger was intended to change the equal-risk assumption underlying the current passenger screening regime (Von Rochow-Leuschner, 2004, p. 144). The output of the CAPPS II process provided the air carrier with the passenger’s risk score and color code, which would place the passenger into one of three risk categories for appropriate screening. While the specific details behind the risk algorithm were classified, the program reportedly created the passenger’s risk profile based on factors other than race, religion, or ethnicity (DeGrave, 2004, p. 131). Early opposition to CAPPS II came from civil rights groups, who were fearful that the program would infringe upon the civil rights and liberties of

many American citizens and resident aliens. These groups were also concerned about the vague reference to using CAPPs II information for “other purposes” contained in the January 15, 2003, Notice to Amend a System of Records (Kite, 2004, p. 1396; DeGrave, 2004, p. 132). In the end, the TSA scrapped the CAPPs II program and implemented a scaled-down version called Secure Flight that validates passenger identity and conducts checks against the government’s no-fly and selectee screening lists. Secure Flight operates in conjunction with the original CAPPs program to identify passengers for more security screening.

Risk-based screening programs are already used in several other areas. Within the aviation domain overseas, even the much heralded Israeli aviation security program contains a registered traveler component, where registered travelers receive “less cumbersome security” methods and clear security nearly eight times faster than other passengers (Poole & Passantino, 2003, p. 8). The former head of security for the Israeli Airport Authority noted that the difference between the U.S. and Israeli approaches is that the United States focuses on finding objects while Israel focuses on individuals with ill intent (Ran, 2002, p. 2). The Israeli approach focuses on people and applies a level of search commensurate with the risk category of the passenger. This approach avoids “wasting our attention on the ‘low risk’ passenger” so that more resources and time are available for screening ‘high risk’ passengers” (Ran, 2002, p. 4). An early risk-based proposal asserted the futility of inspecting “the entire ‘haystack’ of passengers ... [to] search for the proverbial needle” (Golaszewski and Levine, 2001, p. 1). In January 2010, Israel started to implement a biometric-based identity system for passengers called Unipass Airport Management System, which is intended to speed enrolled passengers through security screening processes (Hellman, 2010, p. 2). Amsterdam also uses a registered traveler program, called Privium, at Schiphol Airport to speed enrolled passengers to their flights. Like the Israeli program, Privium uses biometric-based identity verification and provides expedited movement through check-in and screening processes (Poole and Passantino, 2003, p. 9).

Risk-based screening is also employed in programs such as the DHS Global Entry initiative. Under this program, approved participants “considered low risk” are allowed to proceed directly to claim their baggage and avoid primary customs screening after fingerprint-based identity verification (United States Customs and Border Protection [CBP], 2009). Beyond accommodating “low risk” U.S. citizens, Global Entry now includes participants in foreign “trusted traveler” programs such as Privium and Germany’s Automated and Biometrics-Supported Border Controls (ABG) program.” (DHS, 2010b). DHS also employs risk-based methods in other border-entry programs like Free and Secure Trade (FAST), Pre-enrolled Access Lane (PAL), and Secure Electronic Network for Travelers Rapid Inspection (SENTRI). (DHS, 2006, p. 19).

## **F. CONCLUSION**

Federal risk-management guidance provides a standardized method to manage the need to balance security with civil liberty concerns in a cost-effective manner. The NIPP requires federal departments to use this common framework to enable cross-sector comparisons and policy decisions regarding the allocation of scarce resources to areas of greatest risk. While adopting a common framework is a sound approach with many potential benefits, the literature lacks specific implementing detail, which threatens to undercut these benefits.

Since 9/11, a body of literature from various disciplines has discussed the application of the risk-management framework to passenger screening within the aviation domain. The literature points to the use of risk-based screening principles in other applications and in foreign countries that are potentially more cost effective and sustainable over time. These risk-based screening approaches are supported by several mathematic models that demonstrate that it is possible to improve the overall security level of the process by dividing passengers into three or four different risk categories and applying varying combinations of optional screening methods to these different groups. Primary gaps in this literature include how to prevent terrorists from gaming a risk-based

system and the need to track individual passengers from the time of check-in until they have boarded their flight to ensure that they receive the designated level of optional security screening.

Adopting a risk-based approach to the passenger screening process will raise questions regarding unreasonable government searches and the equal protection guaranteed by the Fourth and Fifth Amendments. However, the literature demonstrates that a foundation for accepting such changes is in place in previous court decisions. The literature shows that both the courts and the general public view the definition of reasonableness as changeable, based on perceptions of the risk and the individual impact of more intrusive government search methods. Arguments that airport passenger screening methods create a situation where individuals must choose between their right to freedom from unreasonable government search and their right to air travel have generally been rejected by the courts, which have sustained warrantless searches as constitutional and necessary. Similarly, the literature supports subjecting groups of passengers to different screening procedures as appropriate when certain individuals or groups of individuals are more likely than others to cause harm. Two areas that the literature does not address are the limits on the government when devising special-needs search procedures, and the impact of profiling passengers according to risk on the guarantee of the equal protection clause under the Fifth Amendment.

In the intervening years, several mathematic models have emerged from the fields of operational research and industrial engineering to improve passenger screening methods. These models can be grouped into two basic categories: 1) those that assume that the threat posed by an individual passenger is unknown and 2) those that attempt to classify passengers into categories by risk. The aim of both approaches is to maximize the security level of the entire passenger screening system. This overarching objective is achieved by maximizing the overall system probability of detecting threats while minimizing false positives and false clears. Underlying both approaches is the premise that security screening methods are divided into primary screening measures applied to all passengers and secondary measures applied in various combinations to classes of passengers, generally reflecting risk. While these models demonstrate the utility of

assigning passengers into different risk groups, some approaches drive an increase in resources and others create an opportunity for a terrorist group to defeat the system by timing arrival at the screening checkpoint to increase the likelihood of being assigned to a low-risk group.

From the information gleaned during this literature review, several specific criteria are defined that will be used to compare and evaluate the three different policy options available to address passenger security screening needs within the United States. The five criteria identified as most applicable to this analysis are 1) security effectiveness, 2) risk mitigation, 3) constitutional permissibility, 4) social acceptance, and 5) political feasibility. Chapter III provides an overview of the methodology to be used during the evaluation.

### **III. RESEARCH METHODOLOGY**

Hard choices must be made in allocating limited resources. The U.S. Government should identify and evaluate transportation assets that need to be protected and set risk-based priorities for defending them, select the most practical and cost effective ways of doing so, and then develop a plan budget and funding to implement the effort.

Kean et al., 2004, p. 391

#### **A. POLICY OPTIONS ANALYSIS**

Regardless of the approach taken to ensure the security of commercial aviation, the challenge that must be addressed remains constant: preventing terrorists from smuggling explosives and other prohibited items aboard passenger aircraft. While some level of risk is inherent in the passenger screening environment, the degree of risk we are willing to accept can be varied depending on 1) the level of resources we are willing to devote to the issue, including funding, personnel, and technology; 2) the level of inconvenience and delay that we as travelers are willing to endure; 3) the location of the balance point between security on the one hand and privacy and civil liberties on the other; and 4) the philosophical underpinnings of the passenger screening system. This challenge must be addressed without sacrificing the fundamental principles that define us as a nation and in a way that the American people will accept and support. The primary research method for this thesis is the policy options analysis approach, which supports an objective evaluation of the current U.S. approach, the Israeli security model, and a proposed new risk-based security (RBS) method against a common set of criteria.

##### **1. Policy Options**

The following provides a brief description of the three policy options being evaluated in this thesis. A more detailed overview of each approach is provided in Chapter IV.

**a.      *Option A—The Current U.S. Security Model***

Option A reflects the status quo assumption that all passengers pose roughly an equal risk to aviation security. Passenger screening is one of 21 different layers of security that comprise the aviation security regime. With few exceptions, all passengers traveling aboard commercial aircraft are required to submit to security screening. This approach supports the underlying assumption that *all* passengers pose a potential risk to aviation security. As a result, a basic set of security measures is applied to these individuals at the checkpoint, including identity and boarding pass verification, magnetometer screening, and X-ray inspection of all accessible property. To facilitate the search for prohibited items, passengers are required to remove their shoes, hats, and outerwear (coats and jackets), as well as many electronic items from their accessible property. Restrictions on liquids apply to all passengers, and they must be removed for separate inspection. Passengers are also subject to random selection for additional security measures including screening passengers by observation techniques, advanced imaging technology, explosive trace detection of property or individuals, and physical pat down. The list of prohibited items generally applies to all passengers, as does alarm resolution procedures. Transportation security officers concentrate on searching for prohibited items hidden either on the passenger or in their accessible property, which drives the focus of recurrent training, including X-ray image interpretation, procedural compliance, and concealment techniques. Passenger processing requirements and process efficiency standards require screening of more than two passengers per minute.

**b.      *Option B—The Israeli Security Model***

Option B involves some use of demographic profiling to identify high-risk passengers, who are subject to extensive security interviews and screening procedures. The long-term success of Israel's aviation security approach has resulted in recurring calls to adopt this model from various U.S. government policy makers. A primary difference between the methods of the two countries is Israel's focus on people versus a search for objects. In the Israeli model, every passenger is subject to an interview by security personnel trained to detect suspicious behaviors and physical indicators of

deception. Passenger identity is verified, and each passenger is checked against a variety of intelligence and law enforcement databases. Profiling of passengers based on their nationality, religion, national origin, and/or travel patterns is used to identify individuals who may be considered a security concern. Passengers of concern are subject to extensive security screening and additional interviews by security personnel that can last up to two hours. All other passengers are subject to standard magnetometer screening and X-ray inspection of their accessible property, and luggage is sent through a barometric chamber to simulate altitude pressures that could trigger an explosive device. Screening of passengers not deemed suspicious can take up to 15 minutes each, whereas the time to complete the screening process for the typical passenger traveling in the U.S. aviation system is less than 5 minutes.

***c. Option C—A New Risk-Based Security Model***

Option C proposes a new passenger security approach that assigns each passenger into one of four risk groups, based on what the government knows or does not know about the individual, and then calibrates security measures to address the risk level associated with each group. Some passengers would be categorized as no risk and would receive no security screening beyond identity verification. Low-risk passengers would voluntarily provide the personal information necessary to allow the U.S. government to complete a security background investigation. Once categorized as low risk, these passengers would undergo minimal X-ray and magnetometer screening but would be permitted to keep all items in their accessible property and would not be required to remove shoes, hats, or outer garments. Additionally, low risk passengers would be exempt from many prohibited-item restrictions. Passengers categorized as high risk would undergo far more extensive security screening than currently applied to individuals identified by the government as selectees. This level of screening would include physical bag search, X-ray inspection of all electronics separately from other items, inspection and testing of all medically necessary liquids, interview by security personnel trained to identify suspicious behavior and signs of deception, advanced imaging technology or equivalent physical search of their person, and explosive trace detection screening of both the passenger and his property. Any passenger who could not be placed in one of these

three categories would be assessed as an unknown risk passenger and would undergo the same level of primary screening as currently applied to all passengers. Transportation security officers would not be time constrained in completing the screening process for any passenger assigned to the unknown or high risk categories.

## **2. Evaluative Criteria**

This thesis will evaluate each of these policy options against the following five criteria: 1) security effectiveness, 2) risk mitigation; 3) constitutional permissibility; 4) social acceptance; and 5) political feasibility. The specific components of each of these evaluative criteria are detailed below.

### ***a. Security Effectiveness***

Security effectiveness assesses the probability of finding an object capable of damaging or destroying an aircraft when such an object is actually present or in deterring a terrorist attack. Effectiveness is determined by the security level of the screening process, whether or not a terrorist operative is identified for secondary screening, and considers the number of false positives and false negatives. Two models are used to determine the effectiveness of the passenger screening process.

### ***b. System Effectiveness***

Estimating the probability of detecting the explosive charge or detonator during primary and/or secondary screening, or of detecting a terrorist, is critical to defining the  $P_1$  and  $P_2$  parameters above. This probability is conditioned on several factors. The first factor is the number of opportunities to identify the potential terrorist and direct him to both primary and secondary screening. A second factor considers the effectiveness of primary screening methods in detecting an explosive device concealed in a passenger's accessible property or hidden beneath their clothes. The final factor is the effectiveness of finding the explosive during the required secondary screening, either because the passenger was identified as a higher risk or because of an alarm at a previously identified screening station. For the purposes of this thesis, under both the Israeli and proposed RBS models, any alarm during the screening process is considered a

system alarm, and the effectiveness of secondary screening methods are considered equal, regardless of why the individual was processed through secondary screening measures. Figure 4 depicts the opportunities to identify a potential terrorist during the various primary screening measures and direct that individual to secondary screening.

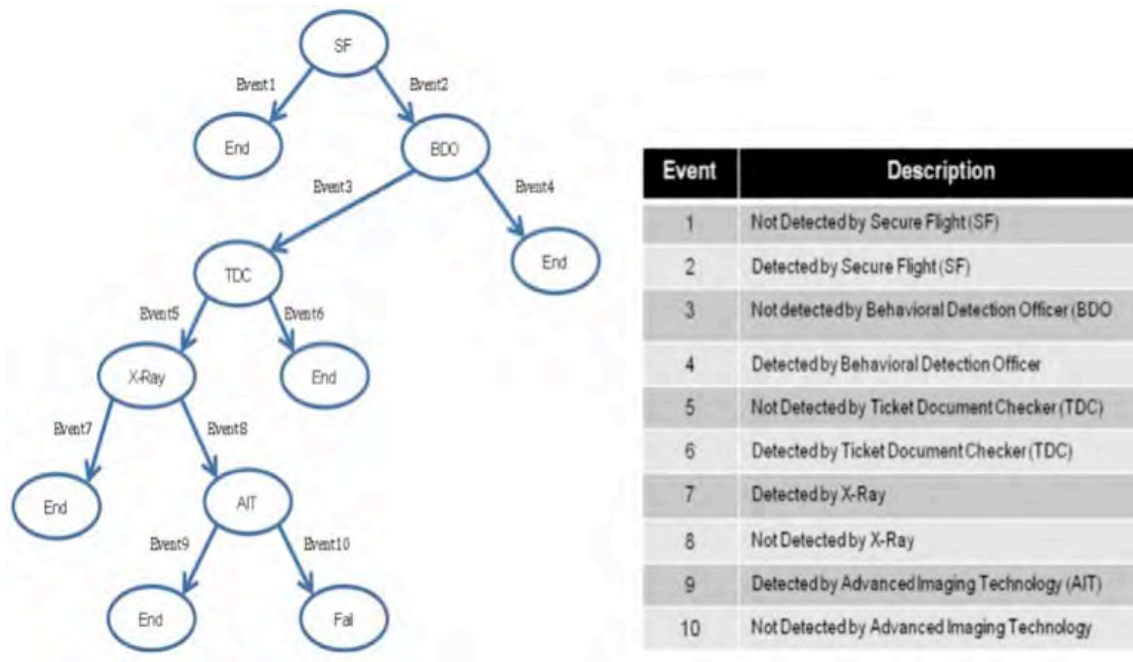


Figure 4. Terrorist Identification Event Diagram (adapted from Schneidewind, 2005, p. 44)

This model uses the following parameters and definitions:

- $P_1$  = Conditional probability of identifying a terrorist operative during screening;
- $P_2$  = Conditional probability of detection an explosive device during screening;
- $1 - P_1$  = Probability of not detecting the terrorist.

Information regarding the estimated probability of detecting a threat when a threat is actually present is contained in Table 1 for both primary and secondary security screening methods. The probability of detection for each security device or

method has been set at the unknown level of 0.5 for illustrative purposes. This value will be adjusted upward or downward as appropriate during the detailed evaluation provided in Chapter V, which also provides an explanation as to the rationale for how these values were set.

| <b>Purpose</b>           | <b>Primary<br/>or<br/>Secondary</b> | <b>Device/Method</b>      | <b><math>p_1</math> Detection</b> |
|--------------------------|-------------------------------------|---------------------------|-----------------------------------|
| Terrorist Identification | Primary                             | Secure Flight             | 0.5                               |
|                          | Primary                             | Behavior Detection        | 0.5                               |
|                          | Primary                             | Ticket Document Check     | 0.5                               |
| Explosive Detection      | Secondary                           | Physical Bag Search       | 0.5                               |
|                          | Secondary                           | Explosive Trace Detection | 0.5                               |
|                          | Primary                             | X-ray                     | 0.5                               |
|                          | Primary                             | Advanced Imaging          | 0.5                               |
|                          | Secondary                           | Physical Pat Down Search  | 0.5                               |

Table 1. Security Method Effectiveness

Table 2 reflects the representational data set that will be used for estimating the detection level of the security device or method.

When the security process is predicated on any alarm, being a system alarm that triggers the full extent of screening of both the person and their property, the overall system effectiveness increases as more security measures are applied to the individual and their property. Under this criteria, it is possible to compute the conditional probability of the overall security level of terrorist identification ( $P_1$ ) and explosive

| <b>Description</b>   | <b>Probability</b> |
|----------------------|--------------------|
| Almost Certain       | 0.95               |
| Highly Probable      | 0.85               |
| Probable             | 0.75               |
| More Likely Than Not | 0.6                |
| About Even           | 0.5                |
| Less Likely Than Not | 0.4                |
| Probably Not         | 0.25               |
| Highly Improbable    | 0.15               |
| Almost Certainly Not | 0.05               |
| Impossible           | 0.0                |

Table 2. Estimated Detection

Using this formula and the representational data sets contained in Tables 1 and 2, the computed security levels for and are as follows:

$$P_1 = [1.0 - [(1.0 - 0.5) (1.0 - 0.5) (1.0 - 0.5)]] = 0.875$$

$$P_2 = [1.0 - [(1.0 - 0.5) (1.0 - 0.5)]] = 0.75$$

Where alarms at any given screening station are not viewed as system alarms, and therefore do not result in full secondary screening of both the individual and his property, the maximum security effectiveness of the overall process is limited to the highest level of security effectiveness of the individual component methods. As an example, if the probability of detecting an IED using explosive trace detection is 50 percent and using X-ray inspection is 60 percent, then the overall system security level is 60 percent.

### ***c. Probability of Deterring Terrorist Attack***

As noted in Chapter II, operations researchers have published a model to calculate the probability that a terrorist attempt would be deterred by the passenger screening process (Martonosi & Barnett, 2006, pp. 1–8). The model holds that the probability of deterring a terrorist attempt “Q” is determined by:  $Q = [P_1 + (C + (1 - C)r) e]$  and uses the following parameter definitions (Martonosi & Barnett, 2006, pp. 2, 6):

**Q =** The probability that a terrorist attempt is stopped by the screening process.

- C** = The a priori probability that an actual terrorist is classified as a high-risk passenger by the passenger screening process.
- r** = The proportion of passengers categorized as low risk who are selected at random for secondary security screening measures.
- P<sub>1</sub>** = The conditional probability of detecting an explosive device during primary security screening of passengers, given that the passenger undergoes only primary security measures.
- P<sub>2</sub>** = The conditional probability of detecting an explosive device during secondary security screening of passengers, given the passenger also completed primary screening.
- e** = The opportunity of sending a terrorist operative to secondary security screening by correctly identifying him through a risk assessment process and reflected as the difference between P<sub>2</sub> and P<sub>1</sub> (P<sub>2</sub> – P<sub>1</sub>).

The authors provide the following example: If the probability of identifying a terrorist during prescreening is 50 percent (C = 0.5); and the conditional probability that an explosive device will be detected during primary screening is 20 percent (P<sub>1</sub> = 0.2); and the probability of detecting the explosive device during secondary screening is 50 percent (P<sub>2</sub> = 0.5); where e = 0.3 (P<sub>2</sub> – P<sub>1</sub>); and the proportion of low risk passengers sent to primary screening only is 0 (r = 0); then the probability of deterring a terrorist attack is 35% (Q = 0.35), as follows (Martonosi & Barnett, 2006, p. 7):

$$Q = [0.2 + (0.5 + (1 - 0.5) 0) 0.3] = 0.35$$

As noted by the authors, as “C” gets closer to 1, the more likely it is that the terrorist will be sent to secondary screening. Increasing “C” by improving the identification of terrorist operatives during the prescreening process is one of three ways to increase the probability of deterring a terrorist attack. The other ways are 1) to increase P<sub>1</sub> by improving the effectiveness of primary screening processes for potential terrorists; and 2) to increase P<sub>2</sub> by improving the effectiveness of secondary screening applied to high-risk potential terrorist subjects (Martonosi & Barnett, 2006, pp. 3, 7).

### 3. Risk Mitigation

Risk mitigation assesses the reduction likelihood that an attack is attempted using an improvised explosive device (IED) brought on board a commercial passenger aircraft and hidden in a passenger's accessible property or on their person and that the IED was successfully detonated, destroying the aircraft in flight. This criterion uses the standard DHS definition of risk, where  $\text{Risk} = \text{Threat} * \text{Vulnerability} * \text{Consequence}$ .

#### a. Threat

Threat [T] is determined by assessing the intent [I] and capability [C] of a terrorist organization to attack a commercial passenger aircraft using an IED (DHS, 2010a, p.36). Threat will be calculated by  $T = [I * C]$ , using the values in the following table.

|                      | Intent | Capability | Threat Score |
|----------------------|--------|------------|--------------|
| T <sub>HIGH</sub>    | 0.95   | 0.95       | 0.903        |
| T <sub>UNKNOWN</sub> | 0.5    | 0.95       | 0.475        |
| T <sub>LOW</sub>     | 0.15   | 0.95       | 0.143        |
| T <sub>NO</sub>      | 0.05   | 0.95       | 0.048        |

Table 3. Threat Values

Since this method of attack has already been demonstrated in several attacks on commercial aircraft, both the intent and the capability components are assessed as “almost certain,” using the scale from Table 2, and the corresponding value of 0.95 will be used for high-threat passengers. This assessment results in a computed threat score for passengers assigned to the high-risk group of 0.903.

#### b. Vulnerability

Vulnerability is defined as the likelihood that the security system will fail and allow the attack to succeed (DHS, 2010a, p. 38). When calculating risk throughout this thesis, the vulnerability of a passenger aircraft to attack by an IED will be set at 0.25, assuming that each of the three policy options is “probably not” going to fail and applies the corresponding value from Table 2.

### c. *Consequence*

For the purpose of this thesis, consequences are defined as the direct financial impact of the catastrophic loss of a commercial aircraft resulting in the death of all on board, and a 10 percent decrease in commercial air travel over a two-year time span. Financial consequences not considered include the impact of any legislative, policy, or regulatory changes that increase the funding appropriated to aviation security programs by Congress, increase the costs to commercial air carriers, or increase security fees imposed on individual passengers. This thesis will use both direct and indirect economic impact. Direct consequences include loss of life and loss of property impact. The direct impact estimates are computed using standard program management estimation techniques, using the formula  $C_N = [C_H + C_L + (4 \cdot C_E)]/6$  where C = Nominal Consequence;  $C_H$  = High Estimate;  $C_L$  = Low Estimate; and  $C_E$  = Expected Consequence. The total direct consequence estimate is \$1,615 (million) based on the preliminary estimates reflected in Table 4 (all dollar values shown are in millions).

|                             | Low Estimate | High Estimate | Expected | Nominal  |
|-----------------------------|--------------|---------------|----------|----------|
| Aircraft <sup>15</sup>      | \$72.85      | \$261.98      | \$164.18 | \$165.26 |
| Deaths <sup>16</sup>        | 189          | 550           | 270      | 303      |
| Value of Life <sup>17</sup> | \$2          | \$10          | \$5      | \$5.33   |

Table 4. Consequence Estimates

Indirect consequences reflect the economic impact of a 10 percent drop in air travel for two years following a successful terrorist attack and the financial impacts across the 20 business sectors identified by the U.S. Department of Commerce that have direct dependence on the commercial air transportation sector. This value is estimated at

---

<sup>15</sup> Aircraft replacement cost estimates are based on the average replacement costs of \$72.85M for a B737; \$261.98M for an B777; and \$164.18 for a B767. Retrieved on March 25, 2011, from <http://www.boeing.com/commercial/prices/index.html>

<sup>16</sup> Estimates on the number of deaths resulting from the destruction of a passenger aircraft while in flight are based on the following: a low estimate equals the capacity of a B737 aircraft; a high estimate equals the capacity of a B777 aircraft; and the expected figure is based on the number of actual deaths in the Pan Am 103 attack over Lockerbie Scotland (Schneidewind, 2005, p. 40, and <http://archives.syr.edu/panam/>).

<sup>17</sup> Value-of-life estimates found in von Winterfeldt and O'Sullivan, 2006, p.67.

\$42,064 million (Von Winterfeldt and O’Sullivan, 2006, p. 67). The combined consequence impact of a successful IED attack aboard a commercial passenger aircraft is estimated at \$43,679 million.

A weighted average of risk will be used when computing total risk based on the individual risk assessed for various combinations of passengers. As an example, assuming that 3 percent of all passengers are considered high threat, and the remaining 97 percent are an unknown risk, the total risk for this passenger group is computed as:

$$\text{High Risk Group: } R = [0.903 \times 0.25 \times 43,679] = 9860.53$$

$$\text{Unknown Risk Group: } R = [0.475 \times 0.25 \times 43,679] = 5186.88$$

$$\text{Total Weighted Risk} = [(9860.53 \times 0.03) + (5186.88 \times 0.97)] = 5327.09$$

#### ***d. Constitutional Permissibility***

Both the Fourth and Fifth Amendments to the U.S. Constitution have a potential impact on any approach to passenger screening. Under the Fourth Amendment, citizens are guaranteed freedom from unwarranted searches by the government, whereas the Fifth Amendment implies a guarantee of equal protection under the law for all individuals. This criterion assesses how well the policy options conform to both amendments. As discussed in the literature review, the following elements will be used to evaluate this criterion:

- Is the measure minimally invasive, as needed to address the threat and prevent a catastrophic event?
- Are individuals more likely to cause harm subject to higher levels of scrutiny?
- Which of the categories that govern Fourth Amendment searches is the measure based upon: no individualized suspicion, reasonable suspicion, or probable cause?
- Does the measure implicate the liberty concerns associated with 1) undue restrictions on travel; 2) impacts on occupational choice; or 3) impacts on an individual’s reputation?

***e. Social Acceptance***

The traveling public interacts with the TSA more frequently than any other government agency, and passenger screening is viewed as an inconvenience and a delay to many. The social-acceptance criterion assesses the degree to which the American people will accept the security approaches associated with each policy option.

- Does the screening program make sense to the average passenger, or do the measures seem arbitrary and unnecessary?
- Is the screening program a cost effective approach to aviation security?
- Does the program minimize the inconvenience for the vast majority of passengers, who are in fact at low risk of committing a terrorist act?
- Do travelers understand what to expect in the screening process?

***f. Political Feasibility***

Because security screening directly impacts so many citizens and private sector entities alike, this topic is politically charged. Any approach to passenger screening must be approved and funded by Congress and the administration. This criterion assesses how difficult it would be, from a purely political perspective, to implement any passenger screening option.

- Is the screening process resource neutral, or does it require greater or fewer resources (e.g., funding, equipment, staffing)?
- Is the screening process likely to increase performance in detecting explosives as the nature of the explosive and methods of concealment change?
- Does the screening process achieve the objectives behind the recommendations contained in the 9/11 Commission report?

**4. Expected Outcomes**

Based on an understanding of the five evaluation criteria from review of the applicable literature and the brief description of the various policy options, the following

reflects the initial evaluation of the expected outcomes for each model. A more precise and detailed analysis is provided in Chapters V and VI.

**a.      *Option A: The Current U.S. Model***

Absent changes in technology or screening procedures, the current status quo approach will result in no change in overall security effectiveness or additional risk mitigation. While some court cases have challenged the constitutionality of recent advanced imaging technology and enhanced pat down procedure changes, the courts have carved out a special-needs exception to the Fourth Amendment for aviation security, and the overall constitutionality of the current process is well established. Social acceptance of additional security measures is likely to become more difficult and resistance to these measures more vocal. Political support for passenger screening exists, and while philosophical differences between the political parties is present, these differences focus on technology and privatization and not the underlying equal-risk approach.

**b.      *Option B: The Israeli Model***

The Israeli security model would improve the security effectiveness of the passenger screening process because more time would be provided to complete primary screening. This option would also effectively mitigate risk from the current threat stemming from Islamic terrorists by profiling passengers for additional security measures. However, this approach would create significant constitutional problems and would result in the courts' rejecting the measures. Social acceptance would be mixed, with some advocating profiling and others objecting on civil rights grounds. Political support would not be present for two primary reasons: first, the public backlash against profiling would prevent bipartisan consensus for adopting this method; second, full implementation would increase the overall cost of passenger screening.

**c.      *Option C: New Risk-Based Security Model***

Using risk-assessment information to determine the level of security measures applied to individual passengers would raise the security effectiveness of the screening process. Similarly, by concentrating more security scrutiny on passengers

evaluated as higher risks, the level of risk mitigation as compared with the current process is expected to improve. The risk-based approach is constitutionally permissible for two reasons: first, it applies the minimal level of intrusiveness to mitigate the threat that the courts have held as the standard for the special-needs exception to the Fourth Amendment, but it does so in a more targeted manner; second, the fact that individuals voluntarily provide the information needed to categorize them as no- or low-risk passengers, overcomes the equal protection concerns of the Fifth Amendment. Because passengers will have the option of getting a background check to be placed in the low-risk category and less intrusive security measures can be applied to a large group of travelers, this option is expected to be well accepted by the public. The expected broad level of public support for this option is also expected to make implementing this model politically feasible.

## **5. Outcome Likelihood**

Based on the preliminary expected outcomes of each policy option, the information below provides an assessment regarding the likelihood that those outcomes would materialize.

### ***a. Option A: The Current U.S. Model***

Although additional procedures and technology are anticipated as the government reacts to changes in threat and terrorist tactics, the overall effectiveness of the process is unlikely to change. Similarly, the broad application of security measures to all passengers absent consideration of risk will not improve the ability of the process to further mitigate risk. The courts have consistently upheld the constitutionality of passenger screening under the special-needs exception to the Fourth Amendment, and the fact that measures are broadly applied to all passengers meets the equal protection requirements of the Fifth Amendment. These interpretations are unlikely to change and undermine the constitutional permissibility of passenger screening. As security measures continue to become more thorough in response to terrorist tactics and methods and these measures are broadly applied to all passengers, the social acceptance for aviation security is likely to continue to decline. Fundamental political support for passenger screening in

general is unlikely to change, although politically imposed restrictions on technology and procedures may occur as public acceptance becomes more vocal.

***b. Option B: The Israeli Model***

Overall, the constitutionality of this option and its lack of social acceptance make the approach politically infeasible. Although this option is expected to provide the greatest level of security, with the best risk mitigation, it is not expected to be accepted by the American people. This likely outcome is based on the lack of acceptance of current procedures that are less disruptive and intrusive on the traveling public than those entailed in the Israeli approach.

***c. Option C: New Risk-Based Security Model***

As several mathematic models demonstrate improved security effectiveness through even random assignment of passengers into risk categories, this expected outcome is highly likely. Absent time constraints during screening of passengers categorized as high or unknown risk, shifting the focus of transportation security officers from finding objects to concentrating on people will effectively mitigate overall risk. This approach is likely to withstand constitutional challenge due to the voluntary feature of the program (absent intelligence or law enforcement information to the contrary, passengers can decide to remain in the unknown-risk category). Further, government officials can articulate the case for the level of intrusiveness of screening measures to address the specific risk posed by each category of passenger, which may be overall more acceptable to the courts under the special-needs exception. Varying the nature of screening measures based on risk at the individual passenger level is likely to gain better social acceptance and support for passenger screening overall. Similarly, the increased security effectiveness and greater social acceptance, combined with the potential to free resources to address other transportation security vulnerabilities, are expected to gain bipartisan political support.

## **B. COMPARISON OF OPTIONS AND EXPECTED OUTCOMES**

Table 5 reflects the expected outcomes of the five evaluative criteria against each of the three options.

Each criterion is assigned a relative ranking against the three policy options, where 1 reflects the best option for achieving the desired evaluative criteria outcome and 3 reflects the least attractive option to achieve this outcome. For example, under the social acceptance criteria, option C is considered the most socially acceptable choice and is assigned a value of 1. Conversely, option B is the least socially acceptable and is assigned a relative value of 3.

|                 | <b>Security Effectiveness</b> | <b>Risk Mitigation</b> | <b>Constitutionally Permissible</b> | <b>Social Acceptance</b> | <b>Political Feasibility</b> |
|-----------------|-------------------------------|------------------------|-------------------------------------|--------------------------|------------------------------|
| <b>OPTION A</b> | 3                             | 3                      | 2                                   | 2                        | 1                            |
| <b>OPTION B</b> | 1                             | 1                      | 3                                   | 3                        | 3                            |
| <b>OPTION C</b> | 2                             | 2                      | 1                                   | 1                        | 2                            |

Table 5. Policy Options Matrix

This use of relative rankings permits comparison of each option against the evaluative criteria by adding the respective numbers, where the option with the lowest total score is potentially the best policy choice. For Table 5, the total score for option A is 11; for option B, 11; and for option C, 8. Although options A and B have identical relative ranking scores, questions regarding the constitutional permissibility of option B make this the least preferred choice, even though the approach is expected to result in the greatest improvement in security effectiveness and best overall risk mitigation.

## **C. CONCLUSION**

Based on the projected outcomes of the selected evaluative criterion, the best option appears to be to adopt a risk-categorization screening system. Although this option may not provide the greatest improvement in security effectiveness or risk mitigation, it is projected to be the most acceptable to the American people and potentially more constitutionally supportable than either the status quo or the Israeli model.

A more detailed analysis of the three passenger screening models is necessary to validate the preliminary judgments and conclusions. In order to support that level of evaluation, a more descriptive overview of each of the policy options is necessary. Those descriptions are provided in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

## **IV. OVERVIEW OF PASSENGER SECURITY SCREENING MODELS**

What the tragic security failures of September 11 reveal is that the continual piecemeal imposition of new technologies, rules, and processes can compromise security and erode public confidence in the government's ability to ensure it.

Downey and Menzies, 2002

### **A. U.S. AVIATION SECURITY MODEL**

The layered-security concept employed by the Transportation Security Administration (TSA) to secure commercial aviation from attack by terrorist groups consists of 21 different measures. Underpinning these measures is the belief that any one of the measures is sufficient to deter or disrupt a terrorist plot, and when interleaved, the totality of these measures provides a resilient and robust defense in depth. According to the TSA, "in combination their security value is multiplied, creating a much stronger, formidable system" (Transportation Security Administration [TSA], 2011a). These measures can generally be grouped into categories based in general by type or location of the security steps. Categories include 1) intelligence; 2) checkpoint screening of passengers and accessible property; 3) checked-baggage screening; 4) random security measures; and 5) security measures on board the aircraft.

Aviation security begins with intelligence information collected by the intelligence community, information provided to the United States by foreign intelligence partners, and counterterrorism investigations conducted by the FBI and their Joint Terrorism Task Forces (JTTFs). This information feeds the Secure Flight system. At the time a passenger makes a flight reservation with an air carrier, he is required to provide some personal information that is used to conduct a comparison of the passenger's identity against intelligence databases, including the no-fly and selectee lists. Depending on the results of this intelligence database check, the passenger is currently placed into one of three categories: 1) passengers identified as "no-fly" individuals will be denied a boarding pass and restricted from passing through security screening and boarding an

aircraft; 2) individuals identified as “selectee” passengers will be required to undergo additional primary screening measures prior to entering the sterile area and being allowed aboard an aircraft; and 3) normal passengers are subject to just primary screening measures that apply to all passengers but may be subject to a variety of random security measures while at the airport. In addition to Secure Flight, the airline-operated Computer Assisted Passenger Pre-screening Systems (CAPPS) also reviews several unspecified passenger criteria to designate certain passengers for additional screening by adding them to the “selectee” category.

In addition to intelligence checks through Secure Flight, several primary screening measures are applied to all passengers and their property. The first primary measure is the ticket document checking (TDC) process. The TSA added this security layer when the agency assumed responsibility for travel document verification from the airlines in an effort to reduce the possibility of a terrorist’s using another individual’s identification or boarding pass to gain access to an aircraft. Since the TDC measure was added in June 2007, all passengers over the age of 18 are required to provide both their airline-issued boarding pass plus one government-issued photo identification to a transportation security officer for inspection. The TSA does provide an alternate means of validating passenger identity for individuals who have lost or misplaced their identification. If the TSA is unable to validate the passenger’s identity, then the individual will not be permitted to process through checkpoint security screening or to board an aircraft.<sup>18</sup> All checked baggage is subject to screening for explosives using either explosive detection system (EDS) equipment or through explosives trace detection (ETD) technology.

Following the TDC security measures, passengers proceed to the familiar passenger screening checkpoint. During checkpoint screening, all accessible property must be submitted for inspection by X-ray screening equipment, and all passengers are subject to screening by either walking through a magnetometer or through advanced

---

<sup>18</sup> A list of acceptable government-issued photo identification can be found at [http://www.tsa.gov/travelers/airtravel/acceptable\\_documents.shtml](http://www.tsa.gov/travelers/airtravel/acceptable_documents.shtml)

imaging technology.<sup>19</sup> An array of technologies and procedures is also available at passenger screening checkpoints to address either unique screening situations or to resolve alarms or anomalies, based on established TSA procedures. These technologies include bottle liquid scanners, used to screen liquids exempt from the current 3-1-1 restrictions (primarily medical and infant/child-care liquids), and cast scopes, which support the noninvasive screening of casts and prosthetic devices to ensure that they are not concealing weapons or explosives. In addition, all checkpoints are configured with explosive trace detection (ETD) equipment, which is used to screen both property and individuals for the presence of trace amounts of explosive residue. Beyond this technology, checkpoints use both physical inspections of property and people to search for weapons and explosives, and the TSA deploys explosives security specialists to assist with response and evaluation of suspect items and equipment alarms.<sup>20</sup>

During checkpoint security screening, the focus of the transportation security officer is on finding prohibited objects, and primary screening measures are applied broadly to all passengers under the assumption that all passengers pose some level of risk to commercial aviation. As noted in Chapter I, the success of this methodology depends heavily on the capabilities of available screening technology and the TSOs who operate this equipment. In particular, X-ray image interpretation, which requires the TSO to search for a host of dissimilar prohibited object types (liquids, knives, firearms, explosives) among significant clutter and distracting items of everyday use, increases reliance on the cognitive abilities of the TSO workforce. Factors such as the time constraints to evaluate each X-ray image, the impacts of satisfaction of search (SOS) and dual target cost (DTC) phenomena, high levels of object ambiguity, and the susceptibility of X-ray screening to threat uncertainty combine to impact performance. The overall security level of the passenger screening process is also impacted by the fact that all

---

<sup>19</sup> The TSA has made the use of AIT technology optional. Passengers selected for AIT screening who do not want to proceed through this screening technology will be subject to equivalent alternative screening including physical pat-down. <http://www.tsa.gov/approach/tech/ait/privacy.shtm>

<sup>20</sup> For a brief overview of this technology and its primary application, see [http://www.tsa.gov/approach/tech2/sec\\_tech.shtm#eds](http://www.tsa.gov/approach/tech2/sec_tech.shtm#eds)

alarms are not viewed as a system alarm that triggers the full scope of security measures and technology applied to both the passenger and all of his property. As a result, alarm resolution measures are generally focused on resolving only the specific alarm at hand.

A variety of random and unpredictable security measures are employed throughout U.S. airports. Passengers may begin to encounter these measures when first arriving at the airport. These measures include 1) visible law enforcement presence in the public areas of the airport, including explosive detection canine teams; 2) behavior detection officers conducting observations of passengers and looking for suspicious activities; 3) random security screening measures, such as requests for consent searches of property away from screening checkpoints or ETD screening of passengers' hands while in the queuing area prior to the TDC position; and 4) closed-circuit television coverage. These measures may be encountered both in the public areas of the airport, including curbside, outside of the terminals, in the ticketing or baggage claim lobbies, and past security checkpoints, within the concourse areas and at departure gate areas.

The final security measures occur aboard the aircraft themselves. These measures consist of 1) pilots trained and armed under the Federal Flight Deck Officer program;<sup>21</sup> 2) hardened cockpit doors; 3) federal air marshals aboard selected aircraft; 4) flight crew members trained to handle security incidents on board an aircraft, and some who have volunteered to receive self-defense training; and 5) fellow passengers who have in the past assisted with subduing threatening passengers and are likely to resist any attempted repeat of a 9/11-type attempt to turn the aircraft into a weapon of mass destruction.

As new search technologies and capabilities become available to improve detection performance, the TSA incorporates them within this process and develops the associated standard operating procedures used by the TSOs to employ these capabilities. Procedural changes are also made to address newly identified threats, methods to further improve detection performance, or risk assessments that indicate changes in risk levels for certain individuals. As example, the TSA recently announced two changes to better

---

<sup>21</sup> Federal flight deck officers are deputized and armed federal law enforcement officials within the limited jurisdiction of the flight deck; they are authorized to defend the flight deck from acts of criminal violence or hijacking. The program was established by 49 U.S.C. § 44921. [http://www.law.cornell.edu/uscode/49/usc\\_sec\\_49\\_00044921----000-.html](http://www.law.cornell.edu/uscode/49/usc_sec_49_00044921----000-.html)

address risk and minimize unnecessary procedures for certain groups of individuals processing through security checkpoints. One of these changes, titled “Known Crew Member,” changes the manner in which certain airline pilots and co-pilots are screened.<sup>22</sup> The other change involves procedures for screening children 12 and under.<sup>23</sup> The various security measures used by the current U.S. model to screen passengers and their property are shown in Figure 5.



Figure 5. United States Aviation Security Model

Random measures that may or may not be used for passenger screening and security purposes are noted in red, while static measures that apply to all passengers and their property are reflected in blue. These measures are:

<sup>22</sup> Known Crew Member is a program sponsored by the Air Line Pilots Association (ALPA) and Air Transport Association (ATA), implemented in partnership with the TSA. For information on this program, see <http://www.knowncrewmember.org/Pages/Home.aspx>

<sup>23</sup> See TSA statement on this change at [http://www.tsa.gov/what\\_we\\_do/screening\\_under12.shtm](http://www.tsa.gov/what_we_do/screening_under12.shtm)

1. Secure Flight;
2. Armed law enforcement, including explosive detection canine teams;
3. Random TSA security measures including behavior detection officer screening;
4. Ticket document checking;
5. Walk-through magnetometer;
6. Advanced imaging technology;
7. X-ray screening of accessible property;
8. Bottle liquid scanners and CastScope technology;
9. Explosive trace detection;
10. Explosive detection systems;
11. Random gate screening;
12. Hardened cockpit doors;
13. Federal flight deck officers and trained crew members;
14. Federal air marshals.

## **B. ISRAELI AVIATION SECURITY MODEL**

Although similar in nature to the U.S. layered-security approach, the Israeli model relies on concentric rings of security, with significant emphasis placed on personal interaction with passengers, beginning from the perimeter of the airport to the aircraft. It is this focus on personal interaction, including an interview of every passenger by at least one security staff member, that provides the most striking difference in comparison to the approach adopted by the United States and most other Western countries. Rather than concentrating resources and technology to broadly screen all passengers and property in a search for weapons, the goal of the Israeli method is identifying individuals with ill intent and subjecting those individuals to more intense security scrutiny. Other prominent features of the Israeli model are the continuous monitoring of everything happening throughout the airport terminal and security screening technology that checks for explosives and weapons, including placing some cargo in a decompression chamber to screen for altitude initiated explosive devices (Hellman, 2010, p. 2). According to Raphael Ron, “You must look at the problem of security from 360 degrees and develop

procedures that go beyond looking for weapons” (quoting Ron in Ficks, 2003, p. 1). While many of the specific measures employed by Israel for aviation security are classified, sufficient details are available in open sources to create a reasonable understanding of the elements that make up the entire aviation security regime.

Passengers encounter the first visible layer of security at the perimeter of the airport. All automobile traffic entering the airport must come to a complete stop at a vehicle checkpoint on either of the two roads leading to the airport, located approximately a mile from the terminal. These checkpoints are configured with license plate recognition systems and armed security personnel and are monitored by a closed-circuit television camera (CCTV) system. Each vehicle is examined, its license plate checked against a national database, and the driver and occupants may be asked several simple questions while the security personnel look for suspicious indicators or reactions. If the security personnel see or sense something suspicious, the driver and/or passengers are questioned further, and the vehicle may be searched, including screening for explosives using under-vehicle cameras. The commuter rail line that serves the airport also has armed security personnel on each train who are looking for suspicious individuals, and explosive detection canine teams are used throughout the airport rail station.

Perimeter security at BGA also includes a five-meter-high fence equipped with motion detection sensors, fence integrity detectors, and buried fence. Closed circuit pan-tilt-zoom cameras are placed approximately every 300 meters around the entire perimeter and are synched to the alarm sensors to automatically shift the camera’s aim point to the spot of the alarming sensor. Behind this outer fence is a second layer of fencing outfitted with razor wire outcroppings. The physical barrier provided by the perimeter fencing is augmented by armed security personnel who patrol the fence line and respond to breach alarms, with plans to field unmanned ground vehicles to enhance surveillance (Lowery, 2010, p. 1; Hellman, 2010, p. 2; Fried, 2008, p.1; Tucker, 2003, p. 6; Kelly, 2009, p. 1–2; Ficks, 2003, p. 2).

Upon reaching the parking garage, bus debarkation point, or BGA train station, travelers encounter the next layers of security. Armed security guards roam throughout the public and exterior areas of the terminal buildings, scrutinizing individuals for suspicious behavior as they approach the terminal entrances. Stationed at each terminal entrance is a second layer of armed security personnel, who conduct a brief check of documents, continue to observe individuals for suspicious behavior, and may randomly select some for magnetometer screening. Armed plainclothes security personnel are also present (Hellman, 2010, p. 1–2; Kelly, 2009, p. 2; Lowrey, 2010, p. 1; Tucker, 2003, p. 2; Fried, 2008, p. 1).

As previously noted, the most significant difference between the U.S. and Israeli systems is the intense focus that Israel places on identifying people with ill intent rather than the search for prohibited objects that dominates the U.S. system (St. John, 1991, p. 85; Walker, 2010, p. 2; Hellman, 2010, p. 2; Tucker, 2003, p. 6; Lowrey, 2010; CNN, 2011). The backbone of the process is the personal interview of every individual and an assessment of risk based on that interview and any information from intelligence agencies “because it is impractical to subject every passenger to a high level of security” according to David Harel, a former member of Shin Bet<sup>24</sup> (quoting Harel in Tucker, 2003, p. 6). Passengers encounter this fifth layer immediately after entering the passenger terminal.

Similar to the U.S. system, passengers are screened against a variety of intelligence databases, and individuals with suspect ties to terrorist organizations are identified prior to their arrival at the airport. Documents and passports are checked for travel trends and visits to countries of interest, and this information is used to assist with developing the line of questioning used by the highly trained interviewers. Items in the passenger’s possession can be checked against the responses provided to the interview questions, and throughout the interview process, the security personnel are assessing the passenger for suspicious behaviors and physical indicators of deception. It is not uncommon for some passengers to be interviewed by more than one security personnel in

---

<sup>24</sup> Shin Bet, or Shabak, is the Israeli Security Agency (ISA). It is one of three agencies that make up Israel’s intelligence community. The ISA is responsible for internal state security, counterterrorism, and counterintelligence. <http://www.shabak.gov.il/english/pages/default.aspx>

order to check for consistency in responses. These interviews can take as little as a few minutes or can extend to more than an hour for passengers selected for more security scrutiny (Lowrey, 2010; Tucker, 2003, p. 6–7; Hellman, 2010, p. 2; Kelly, 2009, p. 2; Passenger Screening Israelis, 2001; St. John, 1991, p. 88).

Although profiling based on race, religion, and nationality has been denied by Rafael Ron as being “professionally stupid” (quoting Ron in Ficks, 2003, p. 3), subjecting Arab passengers to greater security scrutiny is a common practice acknowledged by Israel’s transportation minister when announcing that the practice of placing different colored stickers on the luggage of Arab travelers would shift to assigning a unique number that would flag the luggage for enhanced security checks (Hellmann, 2010, p. 2; Lowrey, 2010; Blumenkrantz & Stern, 2007, p. 1; Passenger Screening Israelis, 2001). In addition to profiling using unspecified demographic criteria, the interview process is used to profile passengers based on behavior, signs of stress, and other indicators of deception (Pickett, 2008). Passengers of concern are subject to extensive security screening and additional interviews by security personnel that can last up to two hours. Baggage carried by these individuals is opened for hand search and the bag and contents tested for explosives (Lowrey, 2010). The fact that passenger interviews are conducted while they are still in possession of all of their property allows the security personnel to review the content of the bags to verify that they are consistent with the passenger’s responses (Pickett, 2008).<sup>25</sup>

On completion of the interview process, passengers proceed to the ticket counter for check-in and to receive their boarding passes. This stage in the passenger process includes luggage scanning in specially designed areas outfitted with blast containment boxes capable of withstanding an explosion from up to 100 kilos of explosives. Security personnel are trained to quickly place a suspect explosive device inside the container to reduce the risk of death and injury to individuals nearby (Fried, 2008, p. 2). Following

---

<sup>25</sup> The success of non-demographic profiling was demonstrated on April 17, 1986, when a bomb hidden in the luggage of Ann Marie Murphy was discovered prior to boarding an El Al flight from London to Tel Aviv. The bomb was planted by Ms. Murphy’s boyfriend, later identified as a PLFP member attempting to destroy the aircraft. See <http://www.shabak.gov.il/English/History/Affairs/Pages/Anne-MarieMurphyCase.aspx>

the scanning of luggage, passengers are issued their boarding passes, tender their checked baggage to the airlines, and then proceed to the security checkpoint, where they are subject to standard magnetometer screening and X-ray inspection of their accessible property (Kelly, 2009, p. 3).

The next step in the security process is submitting checked baggage to explosive detection system screening and placing some luggage in a barometric chamber to simulate at altitude pressures that could trigger an explosive device (Weiss, 2010, p. 2). Prior to entering the concourse leading to the departure gates, international passengers proceed through passport control; all passengers go through a final inspection of boarding documents and passports to verify that they have the appropriate markings indicating that they have cleared through all security measures. The final security measures within the passenger terminal are the presence of both overt and covert armed security personnel who constantly monitor passengers, looking for individuals who are exhibiting suspicious behaviors and who are then subjected to additional security scrutiny (Hellman, 2010, p. 4).

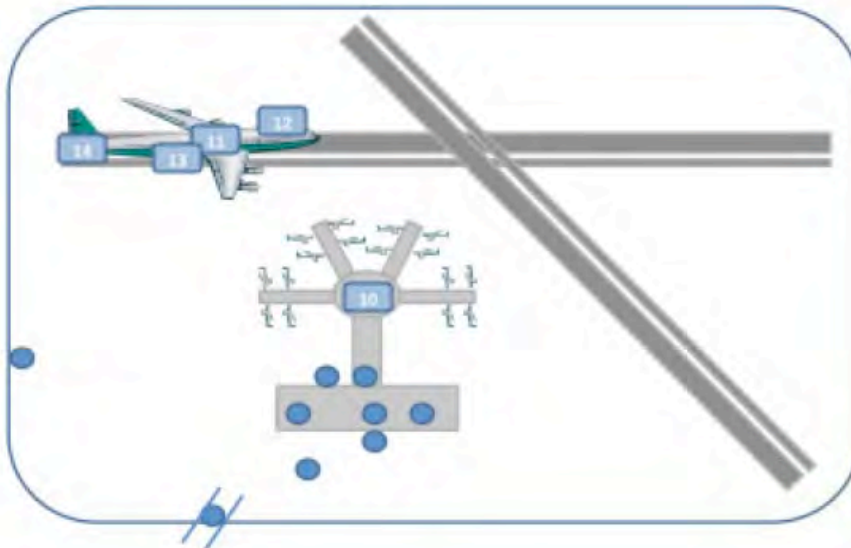


Figure 6. Israeli Aviation Security Model

The visible security layers are shown in Figure 6 as:

1. Vehicle inspection checkpoint;
2. Airport perimeter security;
3. Exterior security guards;
4. Terminal entrance guard and magnetometers;
5. Document review, security interview, and behavioral observations;
6. Luggage scanning and check-in;
7. Security checkpoint X-ray and magnetometer;
8. Passport control (for travelers leaving the country);
9. Passport and boarding pass check prior to entering the concourse;
10. Overt and covert interior armed security guards.

Four additional measures complete the system and extend to the aircraft itself. Each El Al flight has undercover armed sky marshal personnel on board (measure 11) (Walker, 2010, p. 2; Tucker, 2003, p. 7; Weiss, 2010, p. 2; St. John, 1991, p. 71). All aircraft are modified to provide hardened cockpit doors to prevent a breach of the flight deck and fortified cargo hold areas to minimize damage in the event of an onboard explosion from checked baggage (measures 12 and 13) (Weiss, 2010, p. 2; Passenger Screening Israelis, 2001, p. 1). El Al aircraft are also outfitted with an anti-missile system called “flight guard” to defeat anti-aircraft missiles (measure 14) (Walker, 2010, p. 2; St. John, 1991, p. 71).

In January 2010, the Israel Airports Authority (IAA) implemented a biometric-based security enhancement program called UNIPASS to speed cleared passengers through the security process. At each stage in the security process, enrolled travelers enter their issued smart card into a kiosk and are processed through that stage in the process under the watchful eye of security personnel who are ready to assist and are looking for signs of suspicious behavior. Although UNIPASS automates several steps in the process and continuously verifies the traveler’s identity at each step, according to the IAA, Israel is “not giving up on human interaction,” which provides the undergirding of the Israeli security approach (Lappin, 2010, p. 1–2).

### **C. RISK-BASED PASSENGER SECURITY MODEL**

Two basic approaches to implementing a risk-based passenger screening program have regularly surfaced since 9/11. The first approach reflects the Israeli model, which applies more screening measures above a predetermined baseline of measures to passengers identified as posing an elevated risk to aviation security. As noted in the description of the Israeli model above, this approach places a great deal of emphasis and devotes significant resources to identifying higher-risk travelers so that they can be singled out for increased security. A second option regularly proposed is to identify individual travelers who pose less risk and apply lower levels of primary screening to these individuals (Jackson, Chan, & Latourette, 2011, p. 1). Variations of this second approach have generally been referred to as “trusted traveler” programs. The proposed third option evaluated in the thesis represents a combination of these two approaches, where passengers are categorized by risk to receive either less or more security screening from a notional baseline applied to any passenger with unknown risk, and is referred to as risk-based passenger security. The proposed risk-based passenger security entails grouping passengers into four risk categories, based on what we know or don’t know about them as depicted in Figure 7.

Under this proposal, travelers assigned to either of the first two groups—trusted and low risk—would be subject to reduced screening, based on the thoroughness of the associated background investigation. In order to be allowed into the “trusted traveler” group, passengers would be required to undergo and successfully complete an extensive background investigation. This comprehensive background investigation would include a face-to-face interview; checks on immediate family members, friends and neighbors; and fingerprint-based criminal records checks, along with checks against terrorism data bases. Beyond this background check and a periodic reinvestigation, travelers assigned to the trusted traveler group would undergo only two other security measures when traveling aboard a domestic commercial flight. These measures would consist of checks via the Secure Flight system and identity-based security checks at the airport. This final security measure would validate the identity of the traveler using some method of biometric identification card and verify that their travel documentation was valid and a match to

their identity. Passengers assigned as a trusted traveler would generally include individuals with top secret security clearances granted by the U.S. government (both government and contractor personnel), sitting members of Congress, airline pilots, and other flight deck personnel.

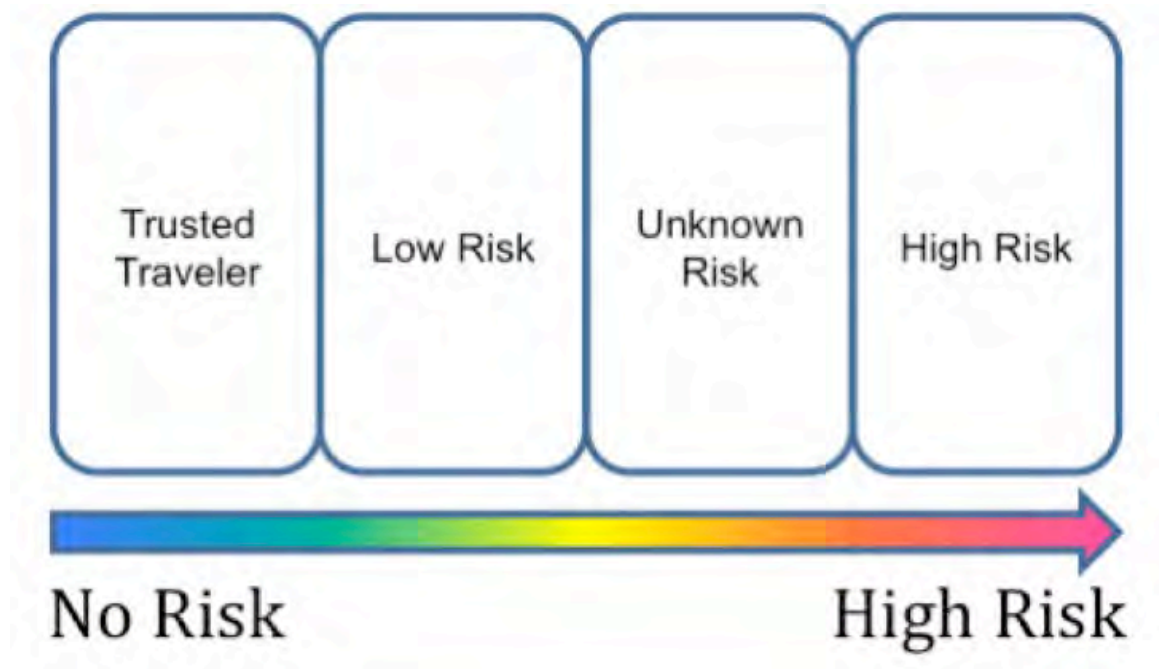


Figure 7. Risk-Based Security Passenger Categories

Individual allowed into the “low risk” group would also be allowed to undergo less security scrutiny from the established baseline measures following successful completion of a less comprehensive background investigation than that required for the trusted traveler group. Passengers seeking approval as low risk would be required to voluntarily provide personal information necessary for the purposes of completing a security background investigation that could be similar in nature to the type of information and background checks currently implemented under the Global Entry program operated by Customs and Border Protection. In addition to the background investigation, Secure Flight systems check, and identity-based security measures, passengers approved as low-risk travelers would be subject to behavior detection screening, would be required to submit to walkthrough metal detector screening and X-

ray of their accessible property, but they would be permitted to keep all items in their accessible property and would not be required to remove shoes, hats, or outer garments. Additionally, low-risk passengers could be exempt from many prohibited-item restrictions, such as liquids in excess of the 3-1-1 rule. In order to guard against the risk of coercion or threats that could induce a trusted traveler to carry an explosive device aboard the aircraft, low-risk passengers would be subject to additional periodic random security measures such as explosive trace detection screening of the passenger's hands or property. As a further safeguard, any alarm during the security screening process (i.e., a possible weapon or explosive identified during X-ray screening, or an alarm at the walkthrough metal detector) would trigger the full scope of security screening measures defined for high-risk passengers.

At the upper boundary of the risk spectrum are passengers categorized as high risk due to identified or suspect ties to terrorist organizations or individual terrorists. Under this risk-based passenger security screening proposal, high-risk passengers would undergo far more extensive security screening than is currently applied to individuals identified by the government as selectees. This level of screening would begin with Secure Flight, which would identify the individual as high risk. Upon arrival at the airport, the high-risk passenger would process through the ticket and identity document check. Once travel documents were confirmed, the passenger would proceed to the security interview and physical bag search position. This measure would function very similarly to the passenger interview process used by Israel, and the interview would occur while the passenger was still in possession of his accessible property to allow the interviewer to review the contents of the bags to validate the responses to security questions. All electronic items would be removed from the passenger's property at this stage and submitted for X-ray inspection, searching for explosives. All other contents of the individual's accessible property would be submitted for X-ray inspection.

Following these security steps, the passenger would proceed for screening of their person using advanced imaging technology (AIT) to screen for explosives and weapons hidden beneath the passenger's clothing. AIT screening would be followed by an ETD of the passenger's hands, looking for explosive residue, and a physical pat down of the

individual to ensure that no weapons or explosives were undetected during primary AIT screening. The final step in the high-risk passenger screening process is the ETD of all electronics to detect trace amounts of explosive particles that would trigger closer examination of these items. Similar to the Israeli model, transportation security officers would not be time constrained in completing the screening process for any passenger assigned to the unknown or high-risk categories, and they would be aware that the property they were inspecting belonged to individuals identified as high risk.

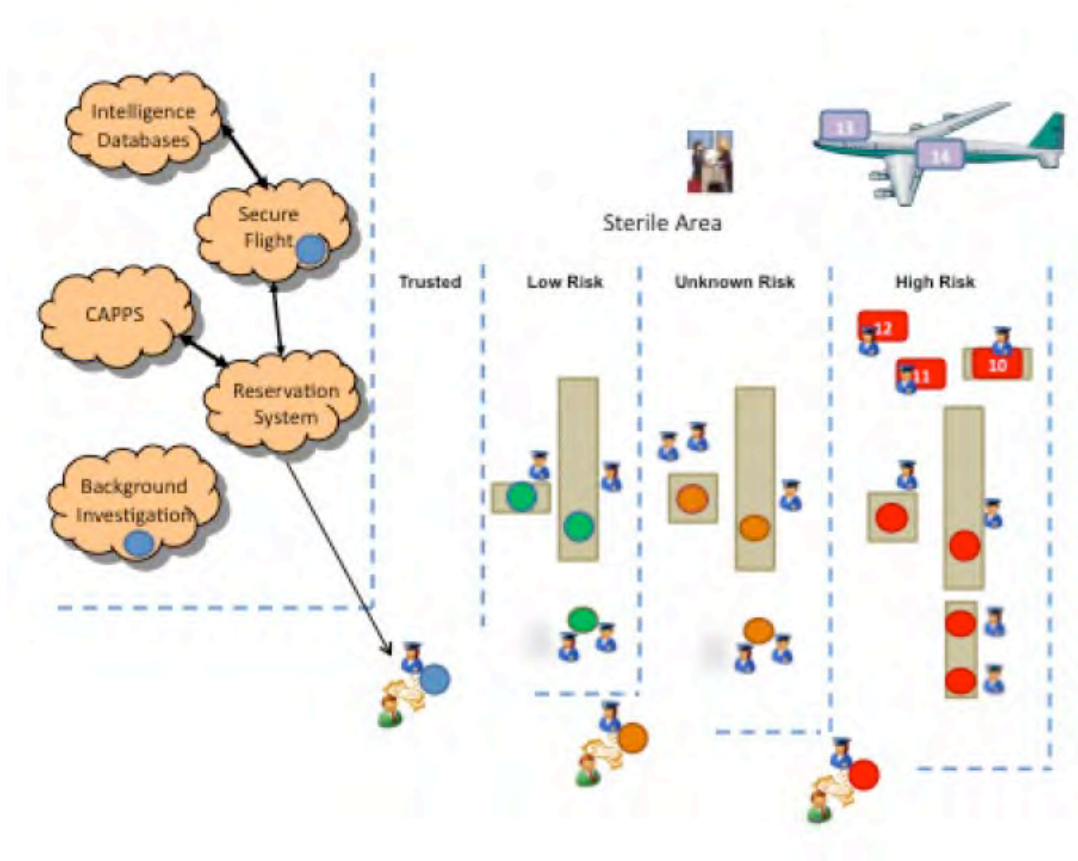


Figure 8. Risk-Based Security Model

Any passenger who could not be placed in one of these three categories would be assessed as an unknown-risk passenger and would undergo the same level of primary screening as currently applied to all passengers and described above. Three fundamental changes would be introduced to improve the security effectiveness of the screening

process in two ways. First, all unknown passengers would be subject to passive screening for suspicious behaviors by trained behavior detection officers. This measure improves the ability of the security process to identify individuals with ill intent. The second improvement over the current U.S. approach would be a shift to a systems alarm philosophy and away from mere alarm resolution.

As noted in the Israeli model, treating every alarm as a systems alarm improves the overall security effectiveness of the process by subjecting passengers who alarm for any reason to the full measure of secondary screening methods. Primary screening methods applied to passengers in the unknown-risk category form the baseline security approach and consist of Secure Flight, behavior detection officer screening, travel document checks; X-ray screening of accessible property, screening of the passenger through AIT equipment (or equivalent physical pat down if the passenger refuses AIT screening), and ETD screening of electronic items. Passengers in the unknown-risk category would also be subject to additional random security screening methods, such as ETD of hands, footwear, or property, and physical search of accessible property.

The security processes applied to the passengers assigned to the various risk-based security categories are depicted in Figure 8 and Table 6. In addition to the passenger checkpoint screening processes, other security measures include explosive detection system screening of checked baggage, federal flight deck officers (item 13), and federal air marshals aboard certain unspecified flights (measure 14).

The risk-based passenger security screening model seeks to strike an appropriate balance between the emphasis on identifying individuals with ill intent inherent in the Israeli model and broadly applied searches for weapons and other prohibited items inherent in the current U.S. approach. This approach also seeks to combine the elements of the two broad methods for developing trusted-traveler-type programs by simultaneously reducing primary screening measures for individuals assessed as lower risk and applying greater security measures to passengers identified as high risk. By adopting the systems alarm philosophy embedded in Israel's approach to aviation

security, the risk-based security approach should increase the overall security level of the passenger screening process while providing acceptable risk reduction to the domestic aviation sector.

Understanding each of the three security models at this high level allows evaluation of the models against the five criteria identified in Chapter III. This evaluation is provided in the following chapter, along with a side-by-side comparison of these policy options.

| <b>Primary Security Measure</b>              | <b>No Risk Group</b> | <b>Trusted Group</b> | <b>Unknown Risk Group</b> | <b>High Risk Group</b> |
|----------------------------------------------|----------------------|----------------------|---------------------------|------------------------|
| 1. Background Investigation                  | Yes                  | Yes                  | No                        | No                     |
| 2. Secure Flight                             | Yes                  | Yes                  | Yes                       | Yes                    |
| 3. Identity and Travel Document Verification | Yes                  | Yes                  | Yes                       | Yes                    |
| 4. X-ray Property Screening                  | No                   | Yes <sup>26</sup>    | Yes                       | Yes <sup>27</sup>      |
| 5. Walk Through Metal Detector               | No                   | Yes                  | No                        | No                     |
| 6. Advanced Imaging                          | No                   | No                   | Yes                       | Yes                    |
| 7. Behavior Detection Screening              | No                   | Yes                  | Yes                       | No                     |
| 8. Physical Property Search                  | No                   | No                   | No                        | Yes                    |
| 9. Security Interview                        | No                   | No                   | No                        | Yes                    |
| 10. Explosive Trace Detection of Property    | No                   | No                   | Yes                       | Yes                    |
| 11. Explosive Trace Detection of Passenger   | No                   | No                   | No                        | Yes                    |
| 12. Physical Pat Down                        | No                   | No                   | No                        | Yes                    |

Table 6. Primary Security Measures for Each Risk Group

<sup>26</sup> All items would be left in the accessible property.

<sup>27</sup> All electronic items would be removed and x-rayed separately.

THIS PAGE INTENTIONALLY LEFT BLANK

## **V. POLICY EVALUATION**

One cannot live free if one lives in fear because people are more able to exercise their freedoms if they feel safe. But the need to be safe, the need to be free from fear should not be used, as it sometimes has been, to justify policies or actions that ignore our rights. It does not mean that our efforts to secure civil rights, liberties, and privacy must be partially rooted in the need to secure our nation.

Janet Napolitano, 2010

### **A. INTRODUCTION**

This chapter evaluates a selection of quantitative and qualitative criteria with direct application to each of the three passenger screening approaches described in Chapter IV. Within the broad category of quantitative criteria, the two areas of relevance chosen for evaluation are security effectiveness and risk mitigation. These measures are selected because they provide an effective gauge of the efficacy of the three policy options and allow for some direct comparison and relative ranking of the models. This section takes several arithmetic formulas from the field of operations research and shifts their application from theoretical to practical, using the primary and secondary security measures contained in each of the proposed approaches. Some assumptions regarding security measures will be made in order to support a viable comparison, and the rationale behind these assumptions will be explained. Additional information regarding any supporting research, where available, is provided along with an explanation of how that research informed these assumptions.

Following the quantitative analysis, the evaluation moves to several key qualitative criteria that have the potential to enable or inhibit the successful implementation and sustainability of any policy decision. This qualitative analysis addresses just three criteria that are arguably the most fundamentally important to evaluating any aviation security policy option. These criteria are constitutional permissibility, social acceptance, and political feasibility. Each subsection contains an

overview of the pertinent information identified during the research, followed by a discussion of how each policy option under consideration in this thesis is potentially impacted by that information.

## **B. QUANTITATIVE EVALUATION**

One constant throughout human history is that no defensive security program is impenetrable. This reality is certainly true in the commercial aviation passenger screening context. Security policy within U.S. commercial aviation seeks to strike a balance between the efficacy of the program and the efficiency of the system, while simultaneously safeguarding the civil rights of passengers. This balance is reflected in how the TSA defines its mission to “protect the Nation’s transportation systems to ensure freedom of movement for people and commerce (TSA, 2011b). The two quantitative measures used in this thesis—security effectiveness and risk mitigation—are intended to determine where this balance point is set with respect to these individual policy options so that they can be arranged in a relative rank ordering. Once the notional effectiveness of the three models is determined using a common methodology, it is then possible for policy makers to assess these security benefits against more qualitative factors.

Although the models used in this analysis are straightforward, the values used for each of the factors are not. It is important to stress that this analysis does not attempt to develop a pinpoint value of effectiveness or risk score for any of the policy options because it is not a definitive computed value that is most important to the conclusions. Rather, it is the relative ranking and the differences between the computed values for the different models that are important, as these differences illuminate how the policy options compare against each other with respect to security effectiveness. It is also important to understand that this analysis is approached in a manner that avoids direct disclosure of security sensitive information regarding the actual effectiveness of specific security measures or technologies employed in the current U.S. passenger screening approach that could be exploited by terrorist groups. To meet academic objectives and to allow this thesis to be broadly available, actual values are not used; unless otherwise noted, assigned values used in this analysis are representational. In some instances, the values

used are adopted from academic literature, and the source of this data is noted where applicable. Where representational values were not found in open source literature, they are derived from the author's direct experience in aviation security but have been adjusted either upwards or downwards and then aligned with the scale presented in Table 7 so as not to reveal actual system performance.<sup>28</sup> The reader should not conclude that the computational results from this use of representational data reflect actual security effectiveness or performance characteristics, and any depiction of actual performance is accidental and unintentional.

## **1. Security Effectiveness**

This section begins with assessing the overall security effectiveness of the three passenger screening approaches. It is divided into two major categories—detection and deterrence. Detection is computed by determining the conditional probabilities of locating the targeted object through the combination of primary and secondary security measures used in each approach. This section will lay out the conditional probabilities for each model and then apply those probabilities to assessing the deterrence value of the respective options.

Throughout this analysis, security effectiveness is limited to just two areas. The first component is a determination of how effective the system is in detecting a threat. For the purposes of this evaluation, threat is narrowly defined as either a potential terrorist operative with intent to commit a terrorist act aboard a commercial aircraft or an improvised explosive device concealed on the individual or within the property he is carrying through the passenger security screening checkpoint. The second component explored is the deterrence effect of the security process—in other words, how the effectiveness of the system might be perceived by the terrorist as a means of dissuading him from attempting to penetrate the checkpoint to commit a terrorist act. In essence, successful deterrence represents a lack of attempt to breach the passenger security process to attack a commercial aircraft using an explosive device carried onboard the

---

<sup>28</sup> The author has nearly nine years' direct experience in the field of aviation security since 9/11, with more than six years in leadership positions as the assistant federal security director for screening operations and deputy federal security director at two of the nation's largest commercial airports.

passenger cabin of an aircraft.<sup>29</sup> The computed security effectiveness will then be used as an input for determining the deterrence value for each of the policy options.

With respect to system effectiveness, it is possible to disrupt and prevent an attempted terrorist attack during passenger screening by one of two means—by detecting the operative and preventing him from entering the aviation system or by detecting the object intended to be used as a weapon during the screening process. Although there are a variety of objects that could be used as weapons and which pose a risk to individual passengers or the aircraft as a whole, the most significant threat object is an explosive device. For this reason, and because the many security layers implemented since 9/11 have reduced the number of objects that can result in catastrophic failure of the aircraft and the death of all on board, the conditional probability of object detection is limited to just explosive devices. Therefore, the detection component of security effectiveness is assessed separately for these two sub-elements—detecting people with intent to commit a terrorist act against the aircraft and detection of an explosive device. Because an explosive device can be hidden either on the passenger or within his accessible property, these two concealment methods provide two additional sub-components of this aspect of effectiveness. The overall effectiveness of the security process is reflected by the conditional probabilities of detection and the response of the security program to alarms that indicate the potential presence of a true threat.

Conditional probabilities are aligned to the ten-point probability scale reflected in Table 7 below. This table provides both a qualitative description and assigned detection probability value. The approach taken to assign a specific value to any individual security measure in the process was first to assess the qualitative descriptor based on judgment. This process requires some reasonable conclusions to be drawn with respect to both the probability of deterring a terrorist attack and the probability of identifying a terrorist operative or explosive device during the security process. For example, open source

---

<sup>29</sup> Success in the deterrence realm includes 1) a terrorist arriving at the airport and then departing because of fear of discovery during security screening; 2) a suicide bomber electing to detonate an explosive device prior to or during checkpoint because of fear of discovery; 3) a suicide bomber prematurely detonating his explosive device during the security screening process when on the cusp of discovery; and 4) a terrorist shifting his plot to attack a non-aircraft target due to the perceived difficulty in defeating security measures.

reporting highlighted in Chapters I and III regarding the effectiveness of X-ray operators in finding prohibited objects indicates that, while detecting prohibited objects during X-ray screening is not impossible, neither is their detection almost certain. However, it is reasonable to expect that finding sophisticated and well-concealed explosive devices during X-ray inspection is highly probable, or this method would not be used; therefore a probability of detection of 0.85 is assigned to this security step.

| <b>Description</b>   | <b>Probability</b> |
|----------------------|--------------------|
| Almost Certain       | 0.95               |
| Highly Probable      | 0.85               |
| Probable             | 0.75               |
| More Likely Than Not | 0.6                |
| About Even           | 0.5                |
| Less Likely Than Not | 0.4                |
| Probably Not         | 0.25               |
| Highly Improbable    | 0.15               |
| Almost Certainly Not | 0.05               |
| Impossible           | 0.0                |

Table 7. Probability of Detection (adapted from Lewis, 2006, p. 206)<sup>30</sup>

In order to effectively compare the relative effectiveness of the three policy options, the assigned descriptors and associated detection probabilities from Table 7 are generally held constant for security measures that are common across the three policy options under evaluation. Where different values are used for a like process, an explanation of the rationale used to arrive at these differences is provided. As an example, not all security measures are used in the same way under each model, with some applied broadly to every passenger in one approach and randomly to some passengers in another option. These differences in how the security measures are applied leads to the judgment

---

<sup>30</sup> This table is adapted from a scale by Lewis used to illustrate the probability of a successful attack. The descriptive labels and corresponding probability value are those of the author.

that the probability of detection should be different when computing the security effectiveness of those different models.

***a. System Effectiveness***

As noted above, system effectiveness is one of two elements that make up overall security effectiveness. System effectiveness represents the overall effectiveness of the passenger security screening system and is defined as the probability of either identifying a terrorist operative or detecting the explosive charge or detonator from an explosive device during primary and/or secondary screening of the passenger or his property when such a device is actually present. System effectiveness is conditioned by several factors: 1) the number of opportunities to identify the potential terrorist and direct him to secondary screening; 2) the probability of detection of an explosive device when such a device is actually present; 3) the rate of false clear when a terrorist operative in possession of an explosive device is not successfully detected and is allowed to pass into the sterile airport area still in possession of the device; and 4) the condition of whether or not the policy views every alarm as a systems alarm that triggers the full measure of security processes being applied to both the passenger and his property.

Table 8 provides a listing of the various security measures detailed in Chapter IV that are used to identify terrorist operatives and assigns each measure an estimate of their detection probability from Table 7. It is important to emphasize that the probability of detection estimates is reflective of that security measure's operation as a stand-alone function in identifying a terrorist operative. These detection probabilities do not reflect the increased effectiveness of security measures when applied in combination. When multiple security measures are combined, the overall effectiveness of the systems increases. This amplifying effect is particularly true when these measures are combined to form a system of primary security screening, as will be demonstrated in the explanation below.

| Security Measure                    | Detection Probability |         |            |
|-------------------------------------|-----------------------|---------|------------|
|                                     | Current U.S.          | Israeli | Risk Based |
| Passenger Background Investigation  | NA                    | NA      | 0.85       |
| Intelligence Databases              | 0.85                  | 0.85    | 0.85       |
| Vehicle Checkpoint                  | NA                    | 0.5     | NA         |
| Exterior Surveillance               | NA                    | 0.5     | NA         |
| Security Interview                  | NA                    | 0.75    | 0.75       |
| Behavior Observation                | 0.4                   | 0.6     | 0.6        |
| Overt/Covert Surveillance           | 0.4                   | 0.6     | 0.4        |
| Identity and Travel Document Checks | 0.15                  | 0.15    | 0.15       |

Table 8. Probability of Terrorist Identification

As noted in Table 8, the estimated probability of detection for behavior observation and overt/covert surveillance measures is not consistent across the three policy options, even though the underlying assumption is that performance is equal when considered at the individual level of the personnel performing these duties. The rationale for this difference stems from the fact that under the existing U.S. process both of these security measures are applied in a random and unpredictable manner as detailed in Chapter IV. Deploying security measures randomly and unpredictably does not reduce the basic effectiveness of the measures operating in isolation, nor does it reduce their overall deterrence value,<sup>31</sup> the approach simply limits the percentage of passengers subject to those measures. In other words, when all passengers are subject to these measures, the security technique is more likely than not able to pick out a terrorist operative in a crowd of passengers based on the behavior of that individual (60% probability of detection). However, when the technique is randomly applied to just one-third of all passengers, the overall system-wide probability of detection is reduced to less likely than not, while the ability to identify a terrorist operative within the crowd of

---

<sup>31</sup> When security measures are used in a truly random and unpredictable way, their deterrence value remains the same because the terrorist operative cannot predict whether or not he will be subject to those measures when on arrival at the airport for passenger screening.

passengers subject to these measures remains at the more-likely-than-not level. Because surveillance and behavior observation measures are not applied to every passenger or at every checkpoint, the overall effectiveness of these measures is decreased when viewed from the macrosystems perspective, and these measures are less likely than not able (40% probability of detection) to identify a terrorist operative within the system, as compared with consistent and non-random use of these measures. Using this same reasoning, the estimated effectiveness of overt/covert surveillance under the risk-based security process is also reduced. Each of the measures listed in Table 8 is considered a primary screening measure.

Table 9 reflects the various security measures used to detect explosive devices and their representational probability of detecting such a device on a person or in their property when the device is actually present. Again, as was the case for the security measures listed in Table 8, the probability of detection reflects the security measure employed as a stand-alone function and not in combination with any other measure. For example, the analysis assumes that it is highly probable that using explosive trace detection will detect the presence of an explosive device, and the corresponding value of 85 percent is assigned from Table 7. Whether or not the security measure is used predominately as a primary or secondary measure under each model is reflected by the parenthetical notation of P for primary and S for secondary. Items listed as secondary measures are principally used for alarm resolution but may also be applied randomly to passengers as primary screening steps. Whether or not the measure is used as a primary security requirement impacts the overall security effectiveness of the process as these measures are combined.

As reflected in Table 9, advanced imaging technology is not used by Israel but is employed in both the current U.S. and proposed risk-based passenger security screening approaches as a primary security measure. Under the current U.S. model, any passenger is subject to random selection to undergo advanced imaging technology

screening. According to the TSA, passengers who do not wish to be screened using advanced imaging technology can elect alternative screening that will include a physical pat down (TSA, 2011c).<sup>32</sup>

| Security Measure                          | Detection Probability |          |            |
|-------------------------------------------|-----------------------|----------|------------|
|                                           | Current U.S.          | Israeli  | Risk Based |
| Physical Bag Search                       | 0.75 (S)              | 0.75 (P) | 0.75 (P)   |
| Explosive Trace Detection                 | 0.85 (S)              | 0.85 (P) | 0.85 (P)   |
| X-ray Screening                           | 0.6 (P)               | 0.85 (P) | 0.85 (P)   |
| Advanced Imaging Technology <sup>33</sup> | 0.85 (P)              | NA       | 0.85 (P)   |
| Physical Pat Down                         | 0.85 (S)              | 0.85 (S) | 0.85 (S)   |

Table 9. Probability of Explosive Device Detection

The assigned detection probability for X-ray screening under the current U.S. model, as reflected in Table 8, is lower than for the other two policy options. The author's rationale for assigning different detection probabilities is based on findings that the longer an individual has to search a complex image for prohibited objects (such as guns, knives, and explosive devices), combined with frequency of exposure to the target objects that build recognition, the greater the accuracy in detecting the presence of these objects, even when they are well camouflaged (McCarley et al., 2004, pp. 302, 306). Several factors identified in the literature diminish detection performance, including 1) the amount of time the operator has to complete a visual search of the X-ray image to identify threat objects; 2) the frequency with which the target threat object is presented to the operator—how often the operator encounters the specific object impacts his ability to quickly recognize that object during visual search; 3) the dual target cost (DTC) phenomenon, which decreases operator performance in finding all anomalous target

<sup>32</sup> See <http://www.tsa.gov/approach/tech/ait/faqs.shtml>

<sup>33</sup> At present advanced imaging technology is not deployed across the entire domestic aviation system and does not support all passengers being screened with this technology. As a result, passengers are randomly selected for AIT screening, which decreases the system-wide probability of detection, similar to behavior detection officer screening conducted on a random and unpredictable manner under the current U.S. approach.

objects when more than one is present and they are dissimilar in appearance (e.g., a handgun versus an explosive mass); and 4) the satisfaction of search (SOS) phenomenon, which results in operators discontinuing their visual search upon finding some other anomalous object in the image. A brief overview of each of these factors is provided below.

In the aviation security environment, X-ray images of carry-on property present complex and densely cluttered images that must be visually searched for prohibited objects under time constraints. A variety of research studies demonstrate that providing more time to complete the visual search increases performance accuracy in detecting the presence of explosive device components and other weapons (Bruner & Postman, 1949, p. 210; Menneer et al., 2006, p. 930; Jackson, Chan, & Latourette, 2011, p. 4; Fleck, Samei, & Mitroff, 2010, p. 64). The relationship between accuracy and time is logarithmic, not linear, where detection error decreases exponentially as search time increases (Menneer et al., 2010, p. 917). Figure 9 provides a visual depiction of this logarithmic relationship using the equation  $P(t) = 1 - e^{-yt}$  where  $y$  represents detection error and  $t$  reflects the time available to search the X-ray image (Jackson, Chan, & Latourette, 2011, p. 4).

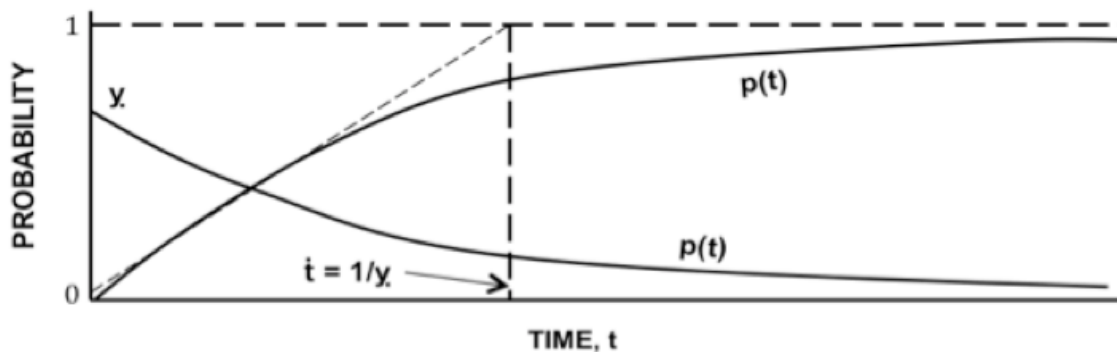


Figure 9. Probability of Detection under Fixed Conditions (from Koopman, 1956, p. 506)

Visual search performance also increases with frequency of exposure to images of the target objects as increased prevalence builds recognition proficiency, with

recognition error rates of low prevalence target objects at nearly twice the level as high prevalence objects (Wolfe, Horowitz, & Kenner, 2005, p. 439).

Dual target cost (DTC) and satisfaction of search (SOS) phenomena also impact the time to complete the visual search and accuracy in finding target objects when the same image must be searched for multiple threat objects. This type of environment is characteristic of aviation security needs. The dual target cost (DTC) impact is particularly prevalent when the target objects are dissimilar (e.g., metallic threats, like guns and knives, and organic threat objects, like explosives) and is present even when using color enhanced X-ray images to display different object types as different colors (e.g., metal objects are displayed in a different color from organic objects). Satisfaction of search (SOS) reflects the fact that individuals conducting visual searches of images become satisfied after finding one such object and discontinue their search efforts as a result (Goodwin et al., 2010, p. 79; Menneer et al., 2007, p. 930; Fleck, Samei, & Mitroff, 2010, p. 60; Berbaum et al., 2001, p. 304). Several measures can minimize performance impacts stemming from SOS and DTC during critical visual search tasks for multiple objects in critical applications such as the aviation security environment. Research shows that increased operator alertness will serve to decrease the impacts of SOS and DTC on overall performance (Babu, Batta, & Lin, 2006, p. 634). Research also supports the need to provide sufficient search time, and high levels of object exposure are also necessary (McCarley et al., 2004, pp. 302, 306; Fleck, Samei, & Mitroff, 2010, p. 64).

Simply stated, when the operator is aware that an individual passenger (or group of passengers) is more likely to present a threat by carrying an explosive device, he or she is more alert to the presence of such a device during X-ray screening. Because of the equal-risk philosophy that underpins the current U.S. passenger screening model, the author postulates that these four effects have a greater negative impact on X-ray operator performance than is present under either the RBS or Israeli models. Diminished performance stems from the fact that under the later two models the operator knows the risk category of the individual whose property is being screened, and he is not constrained by time to complete the visual search process. For these reasons, the associated time pressures and the equal-risk assumption with the current U.S. model

result in the decreased probability of detection value. It is the author's judgment that the estimated probability of detection for X-ray performance for the current U.S. model must be decremented by two levels on the ten-point scale in Table 7 as compared with the baseline level assigned to the other two policy options. The first decrement reflects the impact of time constraints to complete the visual search of the image. A second decrement accounts for the effects of DTC and SOS on explosive-device detection. Applying these decrements decreases the estimated representational probability of detecting an explosive device during X-ray screening from "highly probable" (85 percent) to "more likely than not" (60 percent), as compared with the other two models being evaluated.

Because of the potential for catastrophic failure of a passenger aircraft, the threat object of greatest concern during the passenger screening process is an explosive device hidden either on the terrorist or accessible to the terrorist within carry-on property.<sup>34</sup> Allowing an individual with the intent to commit an act of terrorism to board a commercial flight is of similar concern. A primary objective of passenger security screening is to prevent these such situations from occurring. As a result, this analysis confines the assessment of passenger screening system effectiveness to solely the conditional probability of detecting an explosive device and the conditional probability of identifying a terrorist operative. The conditional probability of identifying a terrorist operative is denoted as  $P_{1X}$ , where  $X$  is used to specify the particular model being evaluated (*US* for Current U.S.; *I* for Israeli; and, *RB* for the Risk-Based model).  $P_{2X}$  represents the conditional probability of detecting the main explosive charge or detonator during primary and/or secondary screening of either the passenger or his property, and  $X$  is assigned the same letters indicating the specific model being evaluated.

As noted previously in this thesis, a primary difference between the current U.S. system and both the Israeli and RBS approaches is how the process responds to an alarm at any stage in the security screening system. Under the current U.S.

---

<sup>34</sup> The potential catastrophic result from an explosive device is demonstrated by the August 2004, attack by two Chechen female suicide bombers, who detonated suicide explosive belts aboard two Russian commercial aircraft, resulting in the deaths of all individuals onboard both flights.

approach, alarms are not viewed as systems alarms, and response is largely limited to secondary measures applied to resolve just the specific alarm. As a result, the conditional probability of identifying a terrorist operative or detecting an explosive device is limited to the individual primary security measure with the highest overall probability of detection. Referring to the assigned values in Tables 8 and 9, the probability of identifying a terrorist is  $P_{1US} = 85\%$ , while the probability of identifying an explosive device concealed in accessible property is  $P_{2USProperty} = 60\%$ ; and  $P_{2USPerson} = 85\%$ , if hidden on the individual.

Both the Israeli and RBS approaches have two common elements that are different in comparison to the current U.S. model. First is the emphasis on identifying passengers deemed as posing a higher risk of committing a violent act on board the aircraft and subjecting these individuals to more intensive security scrutiny during passenger screening. Underlying this philosophy is the idea that, without an individual with the intent to inflict harm, there is no threat to aviation. A second key difference is that both the Israeli and risk-based security processes are predicated on any alarm being a system alarm that triggers the full extent of screening of both the person and his property. As a result, the overall system effectiveness increases as additional screening measures are added, with the conditional probability of identifying either a terrorist operative or explosive device based on the formula where  $P_x$  is the conditional probability of the security program and  $p_n$  is the probability of detection of the individual security measures included in the approach as shown in tables 8 and 9, including all primary and associated secondary screening measures. These results are reflected in the four equations below:

$$P_{1I} = [1.0 - [0.15*0.25*0.4*0.4*0.85]]$$

$$P_{2I} = [1.0 - [0.25*0.15*0.15*0.15]]$$

$$P_{1RB} = [1.0 - [0.25*0.15*0.25*0.4*0.6*0.85]]$$

$$P_{2RB} = [1.0 - [0.25*0.15*0.15*0.15]]$$

For the Israeli model,  $P_{1I}$  reflects that the security program has a 99.5 percent probability of identifying a terrorist. The conditional probability of detecting an explosive device ( $P_{2I}$ ) for the Israeli model is 99.8 percent. Under the proposed risk-based model,  $P_{1RB}$  is 99.6 percent, and  $P_{2RB}$  is 99.9 percent. This difference in alarm

response impacts overall system effectiveness as reflected in Table 10, where the RBS and Israeli models are assessed as having a higher overall probability of detecting both the terrorist operative, and an explosive device, regardless of whether that device is hidden on the passenger or in his carry-on property.

|                    | <b>P<sub>1</sub> Identify Terrorist</b> | <b>P<sub>2</sub> Identify Explosive Device</b> |
|--------------------|-----------------------------------------|------------------------------------------------|
| Current U.S. Model | 0.85                                    | 0.6                                            |
| Israeli Model      | 0.995                                   | 0.998                                          |
| Risk-Based Model   | 0.996                                   | 0.999                                          |

Table 10. Conditional Probability of Detection Comparison

***b. Probability of Deterring Terrorist Attack***

Deterrence within this thesis is the ability to dissuade a terrorist operative from attempting the use of a specific plot to attack commercial aviation (Bowen, 2002, p. 2). Whether a terrorist judges that a particular plot is likely to succeed is influenced by the security measures that must be overcome, which provides deterrence value to the system. While deterrence is traditionally considered in the context of nation states, the concept can and does apply to nonstate actors as well. Arguments against the efficacy of deterrence on terrorist groups typically include an assertion that terrorists are not rational actors, and therefore deterrence is of little value with respect to terrorism (Davis & Jenkins, 2002, p. xviii). However, more recent theories reject the assertion that terrorists are irrational at the individual level, holding that they therefore consider the chances of success or failure when selecting particular targets and tactics to achieve their desired results (Moghaddam, 2006, pp. 4–5; Hoffman, 2006, pp. 239–40, 251–52).

Although there is no direct evidence that terrorists engage in conscious cost-benefit determination when selecting a particular attack plot over another, there is anecdotal evidence to suggest that terrorists do assess the likely success of an attack. This evidence is reflected in the continued adaptation of terrorist tactics and methods in response to changes in aviation security procedures and indicates that terrorists may well be deterred from a specific method when they perceive the chances of success are low.

Since 9/11, we have seen several plots directed against aviation that illustrate how deterrence has resulted in the evolution of explosive device construction and concealment methods as aviation security measures tightened and were perceived by the terrorists as more effective. These plots include the August 2006 effort to conceal liquid explosives in bottles of sports drink, the December 2009 concealment of an explosive device in the underwear of a terrorist flying from Amsterdam to Detroit, and the July 2011 report that terrorists are considering surgically implanting explosives inside suicide bombers (Johnson & Gorman, 2011, pp. 1–3).

The deterrent effect of passenger security screening provides a number of potential benefits to counterterrorism efforts. First, deterrence can result in a shift by terrorists to more sophisticated and difficult techniques of construction and concealment to avoid detection during the screening process. As evidenced by the failed attack on December 25, 2009, sophisticated devices and concealment methods are more prone to fail. Perceived effectiveness of the system can also require the terrorist to spend more time in preoperational surveillance and planning, thereby providing more time for the intelligence community and law enforcement personnel to identify and interdict the plot prior to its attempted execution. Finally, the deterrent effect of perceived system effectiveness can increase the anxiety level of the terrorist operative from fear they will be caught, which improves the capability of the system and “reduces the chance of an attack that would succeed” (Martonosi & Barnett, 2006, p. 4).

While it is not possible to determine the deterrence threshold of any terrorist with respect to a given plot, Martonosi and Barnett provide a mathematic model to calculate deterrence. This model allows for a comparison of the deterrence of different approaches by calculating the probability that the terrorist attempt would be stopped by the security measures in place. This deterrence value is represented by the formula  $Q = [P_1 + (C + (1 - C) r) \epsilon]$  and is used to calculate the probability that a terrorist attempt would be stopped by the passenger security screening process. The definitions and assigned values used in this analysis are reflected in Table 11, which is followed by an explanation of the rationale used to establish these values.

|                      | <b>Definition</b>                                                                                                                                                                                                                                         | <b>US</b> | <b>Israeli</b> | <b>RBS</b> |
|----------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------|----------------|------------|
| <b>Q</b>             | The probability that a terrorist attempt is stopped by the screening process                                                                                                                                                                              |           |                |            |
| <b>C</b>             | The a priori probability that an actual terrorist is classified as a high-risk passenger by the passenger screening process                                                                                                                               | 0.954     | 0.995          | 0.996      |
| <b>r</b>             | The proportion of passengers categorized as low risk who are selected at random for secondary security screening measures                                                                                                                                 | 0.05      | 0.05           | 0.05       |
| <b>P<sub>1</sub></b> | The conditional probability of detecting an explosive device during primary security screening of passengers given that the passenger undergoes only primary security measures                                                                            | 0.6       | 0.994          | 0.992      |
| <b>P<sub>2</sub></b> | The conditional probability of detecting an explosive device during secondary security screening of passengers, given the passenger also completed primary screening                                                                                      | 0.94      | 0.998          | 0.999      |
| <b>ε</b>             | The opportunity of sending a terrorist operative to secondary security screening by correctly identifying him through a risk-assessment process, reflected as the difference between P <sub>2</sub> and P <sub>1</sub> (P <sub>2</sub> – P <sub>1</sub> ) | 0.34      | 0.004          | 0.007      |

Table 11. Definitions and Values for Thwarting a Terrorist Attempt (from Martinosi & Barnett, 2006)

“C”—the probability of categorizing a terrorist operative as high risk during the security screening processes—is defined by the system effectiveness computations above and adopted from the computation for P<sub>1</sub> in Table 10. These computations reflect that the conditional probability of identifying a terrorist during the security screening process is “probable” under the current U.S model and is “nearly certain” for both the Israel and risk-based security approaches. For the Israeli and risk-based security models, this calculation indicates near certainty of subjecting a suspect terrorist operative to the full scope of primary and secondary security measures for both the individual and his accessible property. Under the Israeli system, this result stems from

the multiple points of interaction between airport security personnel and passengers, where travelers are observed for signs of suspicious behavior. Additionally, the personal interview measure that underpins the security program is viewed as highly effective in identifying possible signs of deception or when the contents of luggage do not seem to match with the passenger's responses. Under the proposed RBS model, the near certainty stems primarily from the systems alarm approach, where any anomalous behavior or equipment alarm results in full application of all primary and secondary security measures being applied as if the individual was initially categorized as a high-risk passenger.

The proportion of passengers identified as low risk, "r," and randomly selected for some secondary security screening measures is set at five percent of total passenger volume and is held constant at this level for each model. As explained in Chapter IV, the U.S. passenger screening model relies on random and unpredictable selection for various secondary security screening measures. The estimate is that upwards of five percent of all passengers are randomly selected for some secondary screening at the passenger security screening checkpoint. This estimate reflects the capacity constraints of secondary screening measures (especially the availability of the TSO to perform random measures) because of the high false-alarm rates associated with primary security measures. For both the RBS and Israeli models, the assumption is that the number of randomly selected passengers will be very low, since the underlying philosophy for these models is to focus on finding people with ill intent and not on randomness as a principle means of deterring a terrorist attack. For both models, "r" is estimated at just one percent.

The conditional probability that primary property search methods would detect an explosive device, " $P_1$ ," is derived from the same formula used to compute conditional probability for systems effectiveness. For the U.S. model, we must split this category into two components—detection of the device on the person and detection of the device in property—because each alarm is viewed as separate and distinct, and resolution efforts are focused on just the trigger alarm condition and are determined by the primary measure with the greatest individual detection probability. For property, the value of  $P_1$  is

0.6, reflecting the fact that X-ray screening of property is “more likely than not” able to identify an explosive device. For devices hidden on the person, the value for  $P_1$  is 0.25, or “probably not,” reflecting the probability of device detection using AIT equipment, which is not in use at all security checkpoints and does not screen 100 percent of all passengers at those airports where the equipment is deployed; the standard walkthrough metal detector will not detect explosives or many IED components that are nonmetallic.

The value for  $P_2$ , the conditional probability of finding an explosive device during secondary screening, is set based on the results of the calculation for  $P_2$  under the security effectiveness analysis. Again, because of differences in viewing all alarms as systems alarms, the  $P_2$  values for the current U.S. model are different for an explosive hidden in the passenger or concealed in their accessible property.

Given the above analysis assumptions and rationale, and using Martonosi and Barnett’s deterrence formula  $Q = [P_1 + (C + (1 - C) r) \epsilon]$ , the deterrence value of each security model can be computed as shown below and reflected in Table 11:

$$Q_{US} = [0.6 + (0.954 + (1 - 0.954) 0.05) 0.34] = 0.925.$$

$$Q_{Israeli} = [0.994 + (0.995 + (1 - 0.995) 0.05) 0.004] = 0.998.$$

$$Q_{RBS} = [0.992 + (0.996 + (1 - 0.996) 0.05) 0.007] = 0.999.$$

As noted by the research team, when the value of  $Q$  exceeds the terrorist deterrence threshold, the terrorist group or individual operative is unlikely to proceed with that specific plot and will likely shift to a different attack method. The researchers assert that, as terrorists view the probability of success as lower than the probability of detection, they will be deterred from carrying out that method of attack (Martonosi Barnett, 2006, p. 2). Although it is not possible to determine the specific deterrence threshold level for any given terrorist plot and the operatives involved, it is possible to assess the effectiveness of the various policy options with respect to a terrorist group’s assessment of the difficulty of overcoming passenger security measures. Based on this analysis, each of the three models provides a high level of deterrence value, and the differences between them in this regard are deemed insignificant.

## 2. Risk Mitigation

Risk mitigation assesses the reduction in overall risk to the aviation system based on the effectiveness of the security process. With respect to the risk mitigation evaluation in this thesis, risk is narrowly limited to the use of an improvised explosive device (IED) against a commercial aircraft introduced on board the aircraft through the passenger screening checkpoint. This criterion uses the standard DHS definition of risk, where risk is equal to the product of threat, vulnerability, and consequence ( $R = T * V * C$ ).

### a. Threat

Two components comprise the assessment of threat [T]. The first is intent [I], which assesses the attractiveness to terrorists of an attack on a commercial passenger aircraft as a means of furthering their goals. The capability [C] of the terrorists to conduct such an attack constitutes the second component of the overall threat. For the purposes of analyzing the effectiveness of passenger screening under the three models being compared, the evaluation of threat is limited to just the use of an explosive device brought through the screening checkpoint. Threat is the product of intent and capability ( $T = I * C$ ). (DHS, 2010a, p.36). Table 12 assigns a threat value to each of the four passenger risk categories: high risk ( $T_{HIGH}$ ); unknown risk ( $T_{UNKNOWN}$ ); low risk ( $T_{LOW}$ ); and no risk ( $T_{NO}$ ). These categories are described in Chapter IV under the RBS model.

|               | <b>Intent</b> | <b>Capability</b> | <b>Threat Score</b> |
|---------------|---------------|-------------------|---------------------|
| $T_{HIGH}$    | 0.95          | 0.95              | 0.903               |
| $T_{UNKNOWN}$ | 0.5           | 0.95              | 0.475               |
| $T_{LOW}$     | 0.15          | 0.95              | 0.143               |
| $T_{NO}$      | 0.05          | 0.95              | 0.048               |

Table 12. Risk Groups Threat Values

The values for both the intent and capability components of threat are derived from Table 7. Terrorists have demonstrated the ability to manufacture a variety of improvised explosive devices capable of destroying a commercial aircraft.<sup>35</sup> For this reason, the capability components of threat are held constant across all risk categories, and the assessment is that it is almost certain that terrorist operatives possess this capability. Therefore, a threat value of 0.95 will be used. With capability held constant, the dominant variable that alters the threat score for each individual passenger category is therefore the intent component. For high risk travelers, who by definition are likely associated with terrorist organizations, intent to conduct such an attack is assessed as almost certain (under the right conditions), and a value of 0.95 will be used. Since the intent of the unknown-risk passenger cannot be determined, this analysis will use a 0.5 factor to reflect that uncertainty. Intent of the low risk is assessed as “highly improbable” and will use the corresponding value of 0.15, while it is “almost certainly not” probable that the no-risk passenger intends to commit an act of terrorism using an explosive device, and a value of 0.5 is assigned to passengers in that category.

***b. Vulnerability***

Vulnerability is defined as the likelihood that the security system will fail and allow the attack to succeed (DHS, 2010a, p.38). Absent any security measures, the baseline vulnerability of the aviation system would be 100 percent (or 1.0), reflecting the fact that the system is certain to fail to detect either a terrorist operative or an explosive device. Each additional security measure is intended to reduce that baseline vulnerability to some lower level. As more security measures are added, the result is a continued reduction in the baseline vulnerability of the system overall, and the impact is influenced by the way that the measures are combined. When security measures are used in combination, they have a greater vulnerability reduction impact than when implemented as a standalone feature. This multiplier effect accounts for that reason that the United States uses a layered security approach and Israel employs a concentric ring approach to

---

<sup>35</sup>Two examples are the August 2004 destruction of two Russian commercial passenger aircraft by suicide bombers, and the 2006 liquid explosives plot. For an example of how a sports-drink-bottle-sized liquid explosive could destroy an aircraft in flight, as intended in the August 2006 terrorist plot from terrorists living in the United Kingdom, see <http://news.bbc.co.uk/2/hi/7536167.stm>

aviation security. The need to balance security measures with civil rights and liberties and to minimize the impact on business prevents reducing system vulnerability all the way to zero. Despite all of the criticisms regarding the effectiveness of passenger screening since 9/11, there have been no successful attacks on commercial aviation within the United States, indicating that the system is “probably not” going to fail. The long record of success demonstrated by the Israeli aviation security system also reflects that their model is “probably not” going to fail. Therefore, the vulnerability component of risk is assigned the corresponding value of 0.25 (or 25 percent) from Table 7, and this value will be held constant when calculating risk throughout this thesis.

### *c. Consequence*

Consequence is defined as the impact or effect of the incident (DHS, 2010a, p.10). This thesis will use both direct and indirect economic impact. Direct consequences include loss of life and loss of property. The direct impact estimates are computed using standard program management estimation techniques, using the formula  $C_N = [C_H + C_L + (4 \cdot C_E)]/6$  where C = Nominal Consequence;  $C_H$  = High Estimate;  $C_L$  = Low Estimate; and  $C_E$  = Expected Consequence. The total direct-consequence estimate is \$1,615 (million), based on the estimates reflected in Table 13 (all dollar values shown are in millions).

|                             | <b>Low Estimate</b> | <b>High Estimate</b> | <b>Expected</b> | <b>Nominal</b> |
|-----------------------------|---------------------|----------------------|-----------------|----------------|
| Aircraft <sup>36</sup>      | \$72.85             | \$261.98             | \$164.18        | \$165.26       |
| Deaths <sup>37</sup>        | 189                 | 550                  | 270             | 303            |
| Value of Life <sup>38</sup> | \$2                 | \$10                 | \$5             | \$5.33         |

Table 13. Consequence Estimates

<sup>36</sup> Aircraft replacement cost estimates are based on average replacement costs of \$72.85M for a B737; \$261.98M for an B777; and \$164.18 for a B767 (retrieved March 25, 2011, from <http://www.boeing.com/commercial/prices/index.html>).

<sup>37</sup> Estimates on the number of deaths resulting from destruction of a passenger aircraft while in flight are based on a low estimate equal to the capacity of a B737 aircraft; a high estimate equal to the capacity of a B777 aircraft; and an expected figure based on the number of actual deaths in the Pan Am 103 attack over Lockerbie Scotland (Schneidewind, 2005, p. 40; <http://archives.syr.edu/panam/>).

<sup>38</sup> Value-of-life estimates found in von Winterfeldt & O’Sullivan, 2006, p.67.

Indirect consequences reflect the economic impact of a 10 percent drop in air travel for a year following a successful terrorist attack. This economic impact would be felt across 20 business sectors identified by the U.S. Department of Commerce Bureau of Economic Analysis that have direct dependencies with the air transportation sector; it is calculated at \$42,064 million.<sup>39</sup> The combined consequence impact of a successful IED attack aboard a commercial passenger aircraft is estimated at \$43,679 million (Santos & Haimes, 2004, p. 1447; Von Winterfeldt & O’Sullivan, 2006, p. 67).

**d. Risk**

Under the current U.S. and proposed RBS approaches, the Secure Flight system is used to designate specific passengers as high risk based on matching individuals to the biographic identifier information on individuals who are on the selectee screening subset of the terrorist watch list. While the exact number is classified, the percentage is assumed to be very small, and a value of 1 percent will be used for either the current U.S. and RBS models (or 0.01 of the total passenger population in the high risk category). Due to the increased use of demographic and ethnic profiling inherent in the Israeli approach, a significantly higher percentage of passengers would be categorized as high risk as compared with the proposed RBS model. The author assumes that the percentage of high-risk travelers could be as much as ten times higher than in the United States, and a value of 0.1 is assigned.

Currently, there is a small percentage of individuals subject to fewer primary screening requirements because they are identified as low risk. The TSA recently announced two specific groups of passengers that fall into this low-risk category: children under 12 and air carrier pilots (TSA, 2011d, p. 1; TSA 2011e, p. 1). The author estimates that these categories currently represent a small fraction of passengers, and a value of 1 percent is assigned to this risk group. The author also judges that under the RBS model TSA can categorize as many as 50 percent of the total passenger volume into the low-risk category, and about 3 percent of passengers can be classified as posing little to no risk.

---

<sup>39</sup> The 20 sectors are listed in the Santos and Haimes modeling of demand reduction across the U.S. economy following a terrorist attack on the aviation transport sector (Santos and Haimes, 2004, p. 1449).

The corresponding values of 0.5 and 0.03 are assigned to the low and no-risk categories respectively. All remaining passengers are assigned to the unknown-risk group, which represents 98 percent of passengers under the current U.S. model; 88 percent of passengers under the Israeli model; and 46 percent of passengers under the proposed RBS model. Each model, and the percentage of passengers assumed to be in each of the four risk categories, is shown in Table 14.

| <b>Risk Category</b> | <b>Current U.S.</b> | <b>Israeli</b> | <b>Risk-Based</b> |
|----------------------|---------------------|----------------|-------------------|
| High Risk            | 0.01                | 0.1            | 0.01              |
| Unknown Risk         | 0.98                | 0.88           | 0.46              |
| Low Risk             | 0.01                | 0.01           | 0.5               |
| No Risk              | 0.0                 | 0.01           | 0.03              |

Table 14. Passenger Risk Category Percentages

The two constants in the risk equation are the fixed consequence of \$43,679 million and a vulnerability of 25 percent for the passenger screening system. These constants can be multiplied to reflect a consequence and vulnerability ( $C * V$ ) constant of \$10,919.75. This combined constant can then be multiplied by the threat component to arrive at the risk score for each risk category. Table 15 reflects the individual computation of risk for each category of passengers.

| <b>Category</b>     | <b>C * V</b> | <b>Threat</b> | <b>Risk</b> |
|---------------------|--------------|---------------|-------------|
| <b>High Risk</b>    | 10,919.75    | 0.903         | 9860.53     |
| <b>Unknown Risk</b> | 10,919.75    | 0.475         | 5186.88     |
| <b>Low Risk</b>     | 10,919.75    | 0.143         | 1561.52     |
| <b>No Risk</b>      | 10,919.75    | 0.048         | 524.15      |

Table 15. Category Risk Scores

A weighted average of risk will be used to determine the overall risk score for each of the three policy options, using the percentage of passengers within each risk category for each model. This approach uses the percentage of passengers assigned to each risk category from Table 14 and multiplies that percentage by the risk value for each category from Table 15. The results are shown in Table 16.

| <b>Model</b>   | <b>High Risk</b> | <b>Unknown Risk</b> | <b>Low Risk</b> | <b>No Risk</b> | <b>Weighted Score</b> |
|----------------|------------------|---------------------|-----------------|----------------|-----------------------|
| <b>U.S.</b>    | 9860.53 * 0.01   | 5186.88 * 0.98      | 1561.52 * 0.01  | 524.15 * 0.0   | 5197.36               |
| <b>Israeli</b> | 9860.53 * 0.1    | 5186.88 * 0.88      | 1561.52 * 0.01  | 524.15 * 0.01  | 4683.92               |
| <b>RBS</b>     | 9860.53 * 0.01   | 5186.88 * 0.46      | 1561.52 * 0.5   | 524.15 * 0.03  | 3281.05               |

Table 16. Weighted Risk Score

While this quantitative analysis is solely limited to an assessment of security system effectiveness and risk reduction, the best policy option for passenger security screening stems from categorizing passengers by risk and applying the appropriate security measures based on that risk, as proposed under the RBS model. This approach results in the security effectiveness of the RBS model being approximately equal to that of the Israeli model. Overall weighted system risk is also reduced, with the RBS model providing the best risk mitigation option. The difference in risk between the RBS and Israeli models stems from the higher percentage of passengers categorized as high risk under the Israel model, as compared to either of the other two approaches evaluated.

## **C. QUALITATIVE EVALUATION**

### **1. Constitutional Permissibility**

Any passenger security screening has the potential to implicate rights guaranteed to individuals by the U.S. Constitution. With the three models being evaluated for this thesis, the First, Fourth, and Fifth Amendments to the U.S. Constitution have the greatest potential impact. Among other rights, the First Amendment prohibits Congress from

enacting any law that abridges freedom of speech. Under the Fourth Amendment, individuals are to be free from unreasonable searches by the government. The Fifth Amendment protects against the deprivation of life, liberty, and property of individuals by the government without due process and protects an individuals from being compelled to be a witness against himself in any criminal matter. This section assesses the constitutional permissibility of the three policy options through a review of various federal court rulings with respect to these constitutional rights.

**a. First Amendment**

The First Amendment precludes the federal government from restricting certain enumerated freedoms such as speech, press, religion, assembly, and redress of grievances.<sup>40</sup> Several decisions in the area of First Amendment case law have potential application to the passenger screening environment. In some instances, these rulings have very direct application to the aviation passenger screening context, while others reflect a context different, but analogous to the aviation security process.

Case law has generally held that the right to active speech extends to the boundary where one’s exercise of active speech endangers others. The initial standard regarding the location of this boundary was set by the Supreme Court’s decision in *Schenk v. U.S.*, which established the “clear and present danger” standard (*Schenk v. U.S.*, 249 U.S. 47 (1919)). For nearly 50 years, the “clear and present danger” test of *Schenk* was easily applied to active speech. The underlying principle of imminent danger flowing from unrestrained speech was reinforced by the Court in *Brandenburg v. Ohio*, which held that government cannot place limits on speech or press freedoms—even when individuals advocate the use of violence or other lawlessness—“except where such advocacy is directed to inciting or producing imminent lawless action and is likely to incite or produce such action” (*Brandenburg v. Ohio*, 395 U.S. 444 (1969)). This connection between the expression of ideas—so-called active speech—and overt action resulting from that expression has generally been the lens through which the courts have

---

<sup>40</sup> In 1925, the Supreme Court held in that the due process clauses in the First and Fourteenth Amendments also apply to state and local governments; thus, it is not just the federal government that is precluded from restricting these rights. See *Gitlow v. New York*, 268 U.S. 652 (1925).

viewed the constitutionality of any government restrictions on First Amendment rights. Often overlooked in the general discussion of the right to free speech is the passive exercise of this right by not speaking. Chief Justice Burger noted that “the right to speak and the right to refrain from speaking are complimentary components of the [same] broader concept” (*Wooley v. Maynard*, 430 U.S. 705 (1977)). It is the exercise of free-speech rights by refraining from speech where the potential to intrude on First Amendment privilege and to restrain action is pertinent. Although the context of *Wooley* involved compelling an individual to advocate a specific opinion of a government, the court in *Riley v. National Federation of the Blind of North Carolina* noted that “compelled disclosure of fact, like matters of opinion, may infringe upon the First Amendment” (*Riley v. Nat’l Fed. of the Blind of North Carolina*, 487 U.S. 781 (1988)). In these situations the “imminent lawless action” standard used by the courts for nearly a century may be impossible and certainly more difficult to apply.

The decision to exercise the First Amendment right not to speak may impact the security interview processes of both the RBS and Israeli models considered in this thesis because both incorporate an interview of passengers by security personnel. In the Israeli model, this interview is applied to every passenger and varies in length and intensity, based on a number of factors, including unspecified demographic criteria, the detection of signs of deception or elevated behaviors, responses to the interview questions, and the travel pattern of the individual being interviewed. Under the RBS model, the security interview would be required for every passenger in the high-risk category. Two questions come to mind with respect to interviews of passengers by government security personnel where the First Amendment should be considered: First, does government have the right to include the requirement for certain (or all) passengers to submit to a security interview? Second, what are the implications if a passenger exercises his right to free speech by refusing to respond to security interview questions.

Overcoming potential First Amendment hurdles with respect to the first question is relatively easy. The courts have provided the government with broad discretion in defining the appropriate measures required to ensure the security of commercial aviation. As the court held in *Hartwell*, “By submitting to the screening

process, [the] defendant impliedly consented to the search and was lawfully required to complete the search” (*U.S. v. Hartwell*, 296 F. Supp. 2d 596, 605 (E.D. Pa. 2003)). The *Hartwell* decision held that the entire passenger security screening process, consisting of several distinct primary and secondary search measures, was considered a single search process. Including the requirement that some or all passengers submit to a security interview within the passenger screening process would not make the entire process any less voluntary. Entering that process would continue to imply the passenger’s consent and that, once granted, could not be withdrawn until the process was complete. Additionally, the Supreme Court has “repeatedly refused to declare that ‘only the least intrusive search practicable can be reasonable under the Fourth Amendment.’” (*EPIC v. DHS*, 653 F.3d 1, 22 (D.C. Cir. 2011), quoting *City of Ontario v. Quon*, 130 S. Ct. 2619, 2632 (2010)).

While requiring passengers to submit to and cooperate during a security interview could be viewed as intrusive by some, the level of intrusiveness is calibrated to the level of risk that the passenger poses to the aircraft. Concern by some advocacy groups or individuals that the personal nature of the questions infringes on First Amendment rights is diminished by the voluntary nature of the process. The court’s determination in *Davis* that the purpose of airport security searches is to deter individuals from attempting to carry explosives or other weapons on board a commercial aircraft clearly applies (*U.S. v. Davis*, 482 F.2d 893, 908 (1973)). If an individual does not wish to submit to the security measures required by the government, then he can choose another means of transportation. That being said, the constitutionality of the security interview could hinge on the nature, content, and purpose of the interview questions.<sup>41</sup>

Determining how the exercise of free speech rights through a refusal to respond to questions during the security interview is impacted by First Amendment rights is more challenging. The analysis of this question centers on several important elements: First, do the boundaries of active speech as established in case law apply to the exercise of speech rights by refusal to speak? Second, is it permissible to compel an individual to

---

<sup>41</sup> As example, questions regarding ethnicity, religion, political opinion, association, or support of particular government policies would potentially violate First Amendment rights. The specific content of the security interview questions is beyond the scope of this thesis.

respond to questions during the security interview? Third, is denying access beyond the security checkpoint, and hence to the passenger's reserved aircraft seat, for refusing to answer security interview questions abridging their right to free speech?

In 1991, the Supreme Court held that any law is presumed in violation of First Amendment protections if that law "imposes a financial burden on speakers because of the content of their speech" (*Simon & Schuster v. New York State Crime Victims Bd.*, 502 U.S. 105 (1991)). In order to be permitted past the security checkpoint and allowed to proceed to their departure gate, passengers must complete all defined security requirements. If the passenger is not permitted to proceed past the security checkpoint, he may be denied rebooking by the air carrier or charged a rebooking fee. Requiring a passenger to cooperate during the security interview as part of the screening process may potentially impose a financial burden on that passenger. To support different requirements and treatment of passengers who refuse to cooperate with the security interview and are thus denied entry into the sterile airport area, "the State must show that its regulation is necessary to serve a compelling state interest, and is narrowly drawn to achieve that end" (*Simon & Schuster*, quoting *Arkansas Writers' Project*, 502 U.S. 105, 118 (1991)). This matter raises the question as to whether the government has the authority to impose this type of requirement and whether or not the requirement supports a compelling state interest.

We turn to *Haig v. Agee* for an examination of the issue of whether the government has the authority to impose such a requirement (*Haig v. Agee*, 453 U.S. 280 (1981)). In that case, the U.S. State Department revoked Agee's passport, thereby restricting him from travel overseas after the individual began a campaign of identifying and revealing the names of undercover operatives and agents of the Central Intelligence Agency (CIA). During the hearing, evidence showed that, as a result of Agee's speech, several CIA agents he had identified were killed. In his suit, Agee claimed that Congress has not expressly authorized the Secretary of State to revoke passports and that the infrequent exercise of the claimed power demonstrated inconsistency, which reflected disparate treatment of Agee by the state. Both elements of the court's decision in *Agee*—expressed congressional authority and the frequency of exercising these powers—are

relevant to the passenger screening context. With respect to express congressional authority, the court in *Agee* noted the “broad rule making authority” that Congress granted the Secretary of State and found that “congressional silence is not to be equated with congressional disapproval” (453 U.S. at 291). The authority granted to the TSA by Congress is similarly broad in scope and permits the agency to “issue, rescind, and revise such regulations as are necessary” to protect aircraft passengers and property on an aircraft from criminal violence and hijackings (49 U.S.C. §114; 49 U.S.C. §44903). This broad authority permits the TSA to include a security interview of some or all passengers as part of the screening process and to require cooperation with that interview.

In *Agee*, the court found that, absent specific evidence that Congress intended to restrict the broad powers it granted, “the consistent administrative construction” in exercising those powers established a precedent that the courts should follow (453 U.S. at 291). As to the claim that the government had infrequently exercised those powers, the court found that “although a pattern of enforcement is one indicator of Executive policy, it suffices that the Executive has ‘openly asserted’ the power at issue” (453 U.S. at 301). The TSA has been similarly consistent in its application of the right to deny any passenger permission to pass through the security checkpoint without first completing the prescribed security measures. Various courts have sustained the position that passengers must complete the entire process once it has begun (see, e.g., *Davis, Hartwell, U.S. v. Aukai*, 440 F.3d 1168 (2006)). The TSA has also demonstrated consistency in asserting executive power to define and revise security requirements to address changes in terrorist tactics, and Congress has not restricted this power. Extending the logic of *Agee*, the consistency in asserting executive power within the aviation security domain provides a basis for requiring passengers identified for a security interview to cooperate with that interview.

In *United States v. Davis*, 482 F.2d 893 (9th Cir. 1973), the Ninth Circuit opined that passenger security measures were intended to deter attempts to carry explosives or weapons aboard an aircraft. The court’s ruling in this 1973 case occurred in the face of a fundamentally different threat against aviation. The wave of threats to commercial aviation in the late 1960s and early 1970s was characterized by hijackings

motivated by political ideology and largely fell into hijackings for transportation (e.g., to flee oppressive Communist regimes) and hijackings for extortion (either for financial gain or to pressure Western governments to accede to the demands of the terrorist groups) (Holden, 1986, p. 878). While individuals were killed during the hijackings in this era, the purpose of the hijackings was not the wanton murder of innocent men, women, and children on board the aircraft. In the face of that threat, security measures at airports were likely a significant deterrent to attempts to introduce weapons and explosives on board the aircraft. The threat environment at the time of *Davis* is not the threat we face in the present.

Today's terrorism threat involves religious fanaticism expressed through suicide martyrdom, where the goal is wanton destruction and wholesale death. When the deterrent effect of aviation security measures is insufficient, the process must be capable of detection and prevention. The purpose of the security interview within both the Israeli and RBS models is to detect individuals with the intent to commit an act of terrorism on board an aircraft and to prevent those individuals from gaining access to the aviation system. Adding a security interview component to the passenger screening process, with the requirement that passengers cooperate during that interview, would not violate First Amendment protections, as long as the questions did not directly address matters of ethnicity, religion, political opinion, association, or support of particular government policies.

**b. Fourth Amendment**

There is a long history of court support for warrantless searches of passengers at airport checkpoints. One of the most cited early cases is *United States v. Davis*, 482 F.2d 893, a 1973 case from the United States Ninth Circuit Court of Appeals. In *Davis*, the court held that “[airport] searches conducted as part of a general regulatory scheme in furtherance of an administrative purpose, rather than as part of a criminal investigation to secure evidence of crime, may be permissible under the Fourth Amendment though not supported by a showing of probable cause directed to a particular person to be searched” (482 F.2d at 908). This ruling, that warrantless airport search of

passengers and property for weapons or explosives is constitutionally permissible, did place a reasonableness provision on the conduct of such searches. The Court in *Davis* noted that “to meet the test of reasonableness, an administrative search *must be limited in its intrusiveness* as is consistent with satisfaction of the administrative need that justifies it” (482 F.2d at 919) (emphasis supplied). A further implication of the *Davis* ruling is that airport searches “are not selective,” in that they are applied broadly to all passengers without regard to reasonable suspicion or probable cause; the application of such searches is random. In fact, the court in *Davis* stated that “a compelled search of persons who elect not to board would not contribute to barring weapons and explosives from the plane ... [and] such searches would be criminal investigations subject to the warrant and probable cause requirements of the Fourth Amendment” (482 F.2d at 911). This language left open the opportunity for an individual to withdraw consent to be searched by electing not to proceed past the security screening checkpoint when they feared imminent discovery.

While the decision in *Davis* hinged upon the consensual nature of airport searches, this application of the administrative search doctrine does not depend solely upon consent. In *United State v. Biswell*, 406 U.S. 311 (1972), the U.S Supreme Court ruled that the lawfulness of warrantless searches conducted in support of a regulatory scheme supporting a compelling government interest does not depend on consent. The court held that “it is also apparent that if the law is to be properly enforced and inspection made effective, inspections without warrant must be deemed reasonable official conduct under the Fourth Amendment” (406 U.S. at 316). Although the matter at hand in *Biswell* was a regulatory inspection of a gun dealer, the court’s ruling was specifically extended to airport searches in *United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007) (en banc). *Aukai* challenged the constitutionality of secondary screening when controlled dangerous substances (CDS) were found on the appellant’s person after he had taken actions to indicate that he wanted to withdraw his consent to be searched. Citing *Biswell* in their unanimous ruling, the *Aukai* court held that “the constitutionality of an airport screening search, however, does not depend on consent, *see Biswell*, 406 U.S. at 315, and requiring that a potential passenger be allowed to revoke consent to an ongoing airport security search makes little sense in a post 9/11 world” (497 F.3d at 960). Eliminating all

questions of whether or not passengers could withdraw consent after beginning the screening process, the *Aukai* ruling stated unequivocally that “our [prior] case law, however, has erroneously suggested that the reasonableness of airport screening searches is dependent upon consent, either ongoing consent or irrevocable implied consent” (497 F.3d at 960).

In a precedent-setting decision in 2006, the United States Third Circuit Court of Appeals also found that airport security screening searches did not violate Fourth Amendment protections against warrantless search. This decision in *United States v. Hartwell*, 436 F.3d 174, held that prior court rulings, such as *U.S. v. Albarado* (495 F.2d 799 (2d Cir. 1974)), that treated as separate searches each step in the screening process were incorrect and that the defendant had in fact “experienced a single warrantless search, which was initiated without individualized suspicion” (436 F.3d at 178). The court’s ruling also noted that the Supreme Court in two separate instances<sup>42</sup> had opined that warrantless airport searches are reasonable because “the need for such measures to ensure public safety can be particularly acute” (436 F.3d at 178). More recently, the U.S. Court of Appeals for the District of Columbia, in *Electronic Privacy Information Center v. United States*, reaffirmed the compelling governmental interest behind searches of airline passengers and noted that “a potentially escalating series of search techniques,” even when not the least intrusive methods available, were consistent with the Fourth Amendment (*EPIC v. U.S.*, 653 F.3d 1 (D.C. Cir. 2011)). The consistency of federal court rulings over the past four decades regarding the permissibility of warrantless administrative searches in general—and airport security searches in particular—will not inhibit any of the three policy options.

Clearly the post 9/11 rulings in *Hartwell*, *Aukai*, and *EPIC* support the constitutional permissibility of the current U.S passenger screening approach with respect to the Fourth Amendment. The *Hartwell* ruling in particular supports the adoption of a systems alarm philosophy that is key to the security effectiveness of both the RBS and Israeli models, where the entire process is considered a single search to which the

---

<sup>42</sup> *Chandler v. Miller*, 520 U.S. 305 (1997); *City of Indianapolis v. Edmond*, 531 U.S. 32 (2000).

passenger consents and cannot from which he cannot withdraw until the process is complete. However, the court's language in *Davis*, as well as *Hartwell*, raises the question of whether subjecting some passengers to additional security measures absent an alarm, or allowing some passengers to undergo less security than others, could be viewed as individualized suspicion and stray beyond the special-needs exception carved out by the courts.

The Second Circuit addressed this concern in the border security context in 2007. In this case, the court found that even though Customs and Border Patrol (CBP) officers required individuals who attended an Islamic conference in Canada to undergo extensive secondary screening measures—including being photographed, fingerprinted, and subject to extensive interviewing for up to two hours—“some measure of deference is owed to CBP due to its considered expertise in carrying out its mission of protecting the border” (*Tabbaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2007)). This finding was based on the fact that the security measures used were considered routine in nature, that preventing terrorists from entering the country was a compelling governmental interest, and that the actions were taken in response to intelligence that raised concern that terrorists would use the conference to switch identity documents with other conference participants and attempt to enter the country. Although the authority for conducting searches at the border derives from different case law from that of the administrative special-needs exception to the Fourth Amendment, the compelling nature of the governmental interest in the aviation passenger screening context argues for similar deference being afforded to TSA as is provided to CBP. In fact, in *United States v. Skipwith*, 482 F.2d 1271 (5th Cir. 1973), the Fifth Circuit “did not differentiate between interstate and international travel” when considering the constitutionality of passenger screening in a purely domestic context, which supports extending the deference given to CBP to execute its counterterrorism mission to the TSA to execute its similar counterterrorism mission (Herzog, 2005, p. 382).

Under the RBS model, individuals approved as either no-risk or low-risk passengers—and thus subject to less passenger security at the airport checkpoint than other passengers—should not create any undue concern. The Courts have thus far not

differentiated the various security screening measures applied, and as reflected in *Edmond*, the courts have not defined “the outer limits of intrusiveness in the airport context” (*City of Indianapolis v. Edmond*, 531 U.S. 32 (2000)). In fact, the court in *EPIC* supported use of advanced imaging technology as consistent with the Fourth Amendment since this technology provides a means “of detecting, and therefore deterring, attempts to carry aboard airplanes explosives in liquid or powder form” that the older magnetometer technology is unable to detect (*EPIC v. U.S.*, 653 F.3d 1 (D.C. Cir. 2011)). As the nature of the threat changes and new technologies and procedures are added to the process in response to or in anticipation of that change, the courts have continued to sustain the constitutionality of airport security searches. Extending the decision in *Hartwell* that all measures in the process are considered “a single warrantless search,” even when they are not all applied to every passenger, provides the case law foundation for such differentiation. Passengers who consent to an extensive background investigation in order to be approved as low- or no-risk travelers are in fact undergoing security screening, with the background check substituting for more intrusive security measures at the airport.

The courts have not overturned the current method of identifying high-risk passengers and requiring them to undergo more extensive security measures. In fact, the *Aukai* case involved the defendant’s being sent to more extensive security screening because he did not possess any identification and was deemed a higher-risk passenger. The ruling of the Ninth Circuit en banc held that “where the risk to public safety is substantial and real, blanket suspicionless searches calibrated to the risk may rank as ‘reasonable’—for example searches now routine at airports and at entrances to courts and other official buildings” (*U.S. v Aukai*, 497 F.3d 955, 958 (9th Cir. 2007), quoting *Chandler v. Miller*, 520 U.S. 305 (1997)). Calibrating the type and level of security measures to the appropriate risk posed by the individual passenger appears to be a reasonable and prudent measure that meets the court’s expectations. As noted by the court in *Davis*, the purpose of airport security searches “is not to detect weapons or explosives or to apprehend those who carry them, but to deter persons carrying such material from seeking to board at all” (*U.S. v. Davis*, 482 F.2d 893, 908 (9th Cir. 1973)). The *Aukai* decision noted that, to be an effective deterrent, the screening process must

also be capable of detecting explosives. Applying more extensive measures of security to individuals more likely to be in possession of weapons or explosives through a risk-based process strengthens the degree of deterrence and applies the minimal level of invasiveness necessary to deter each passenger based on his assessed risk category. For these reasons, both the RBS and the Israeli approaches, which vary the level of security based on the assessed risk posed by the individual passenger, should not present any constitutionality concerns with respect to the Fourth Amendment.

**c. Fifth Amendment**

The Fifth Amendment provides individuals with the guarantee of due process, equal protection under the law, and the right to liberty. The adoption of profiling in the aviation security context, as is inherent in the Israeli model, may be inconsistent with these rights guaranteed by the Fifth Amendment. Profiling for the purposes of this thesis is referred to as “9/11 profiling” and consists of “subjecting people who look Middle Eastern, Arab, or Muslim to discretionary law enforcement attention as a way to prevent terrorist activity” (Schildkraut, 2009, p. 5).

Department of Justice (DOJ) guidelines regarding profiling do permit the use of race and ethnicity by federal personnel performing aviation or border security duties when involved in combating “threats to national security” or ensuring the integrity of the nation’s borders. This DOJ guidance authorizes federal personnel to use all means permitted by law to prevent “catastrophic events” but cautions that the claim of a national security compelling interest must not be a “pretext for invidious discrimination” (DOJ, 2003, pp. 12–13). The DOJ appears to gain justification for this exception from court rulings that state that “it is obvious and unarguable that no governmental interest is more compelling than the security of the Nation” (*Haig v. Agee*, 453 U.S. 280, 307 (1981); *Aptheker v. Secretary of State*, 378 U.S. 500, 509 (1964)).

Several court decisions address the use of race, appearance, or ethnicity with respect to Fourth Amendment reasonable-suspicion matters but do not specifically address whether such profiling is inconsistent with the Fifth Amendment. In 1975, the Supreme Court ruled that using one’s race was permissible when determining whether

reasonable suspicion for a more intrusive search was warranted when other “articulable facts” were present (*United States v. Brignoni-Ponce*, 422 U.S. 873, 884 (1975)). In 2010, the First Circuit stated that “[j]ust as it cannot be said that appearance, even ethnic appearance, of a suspect is never relevant, it certainly cannot be said that it is always or even generally relevant” (*United States v. Ramos*, 629 F.3d 60, 68 (1st Cir. 2010)). With respect to the equal protection clause, the courts have determined that, even when race was the predominate reason for stopping a suspect, this use of profiling did not conflict with the Fourth Amendment (*United States v. Weaver*, 966 F.2d 392 (8th Cir. 1992)). In *Whren v. United States*, the court noted that “the constitutional basis for objecting to intentionally discriminatory application of laws is the Equal Protection Clause” but did not rule specifically on that matter (517 U.S. 806, 813 (1996)). With respect to Fifth Amendment rights, the constitutionality of either the Israeli method of profiling or the 9/11 profiling described above may well depend upon whether the courts determine that such measures satisfy the “compelling state interest” of preventing acts of terrorism aboard an airplane. The availability of specific intelligence information that provides some basis for the demographic criteria applied in the profiling approach would likely strengthen the justification for using these measures. This question raises concerns about adopting any profiling measure as part of passenger security screening and leads to the conclusion that the Israeli model is likely incompatible with Fifth Amendment equal protection guarantees.

The other aspect of the Fifth Amendment requiring consideration is the right against self-incrimination. This right, that a person cannot be compelled to provide witness against himself, was settled by the Supreme Court, in arguably the most familiar of all court rulings, in the 1966 case of *Miranda v. Arizona*, 384 U.S. 436 (1966). In *Miranda*, the court placed limits on the admissibility of statements made by individuals suspected of criminal activity while in the custody of law enforcement personnel. Noting the significant psychological stress placed on criminal suspects when questioned in isolation, the court found that “the very fact of custodial interrogation exacts a heavy toll on individual liberty and trades on the weakness of individuals. (384 U.S. at 455). The court also found that the protections afforded individuals against self-incrimination as

guaranteed by the Fifth Amendment, extend beyond the criminal trial itself and provide protection against self-incrimination “in all settings” where the individual is limited in his freedom of movement and action. This finding led to the requirement that all individuals subject to a custodial interrogation be apprised of the right against self-incrimination, and when the individual elects to exercise those rights, they “must be fully honored” (384 U.S. at 467). Following the decision by the *Miranda* court, the constitutionality of questions asked of individuals within the screening context hinges on two key elements: 1) whether the situation is considered a custodial interrogation, and 2) whether the individual is suspected of criminal activity.

Several rulings by federal courts directly address the question of custodial interrogation. The foundation for their application in the aviation passenger screening context rests on cases involving the questioning of individuals by customs officials in the border crossing environment. In a 1983 case, the Second Circuit found that routine immigration and customs questions asked at the border do not take place within a custodial environment, even in light of the fact that the individual is not allowed to withdraw from the process until completed by the customs or immigration officials (*U.S. v. Silva*, 715 F.2d 43 (2d Cir. 1983)). The *Silva* court found that, even though the defendant was sent for secondary inspection, the detention and questioning of the individual was routine since they were not focused on obtaining information that would be used against the individual in a criminal trial. Rather, the nature of the questions fell within the exclusions recognized by the *Miranda* court and were “[g]eneral on-the-scene questioning as to facts surrounding a crime or other general questioning of citizens in a fact-finding process” (*U.S. v. Silva*, 715 F.2d at 47, quoting *Miranda v. Arizona*). In a ruling rejecting the appeal of a case from the district court, the Third Circuit determined emphatically that, absent suspicion that the individual being questioned was involved in criminal activity, it was immaterial for *Miranda* purposes whether the questions took place during primary or secondary inspection settings (*U.S. v. St. Vallier*, 404 Fed. Appx. 651 (3d Cir. 2010)). Citing the ruling in *U.S. v. Kiam*, 432 F.3d 524 (2006), the court noted that “custody is not dispositive in the context of border questioning” as long as the questioning is not solely related to gathering information for criminal prosecution and

that the boundary between custodial and noncustodial interrogation is not violated as long as the questions deal with the admissibility of the individual, even when they also address potential criminal conduct (404 Fed. Appx. at 656). In these instances, the requirements of *Miranda* do not apply.

Several cases have extended this reasoning to the aviation passenger screening environment. The *Hartwell* court determined that “routine questioning of passengers at airport security checkpoints does not amount to custodial interrogation” (436 F.3d at 606). While the court was willing to make this declarative statement, there are two elements in the *Hartwell* decision that have potential impact on passenger screening measures. First, the *Hartwell* court differed from the *St. Vallier* ruling in concluding that because Hartwell’s interrogation occurred in a separate room “by two TSA agents and a police officer blocking the exit,” Hartwell’s “freedom was thus curtailed to a degree associated with formal arrest requiring that he be Mirandized before [the] interrogation occur[ed]” (436 F.3d at 607). This difference could be interpreted by future courts to indicate that TSA should provide *Miranda* warnings to passengers when TSA requires the individual to complete secondary screening measures to resolve alarms in private screening room settings (as opposed to passengers who request completion of alarm resolution procedures in a private setting away from public view). Second, the decision in *Hartwell* noted that the emphasis placed on Hartwell’s suspicious behavior during the screening process had focused “the eye of suspicion” on him, which could imply that the questioning was no longer routine in nature but rather focused on potential criminality, which would require that *Miranda* rights be provided to the individual (436 F.3d at 606).

As determined in *Silva*, *St. Vallier*, and *Kiam*, there is a boundary between routine questioning that does not invoke *Miranda* and interrogation based on suspicion or in support of information for criminal prosecution, which can easily be breached during passenger screening. While it is clear that the courts view all questioning focused on criminal conduct as requiring *Miranda*, it is not always clear when that line has been crossed. Recently the district court of Nevada spelled out five elements to be considered in determining whether or not the questioning is custodial. These factors are “(1) the

language used to summon the individual; (2) the extent to which [the] defendant was confronted with evidence of guilt; (3) the physical surroundings of the interrogation; (4) the duration of the detention; and (5) the degree of pressure applied to detain the individual” (*U.S. v. Hughes*, 2009 WL 4330481 \*9 (D. Nev.), quoting *U.S. v. Bautista*, 684 F.2d 1286 (9th Cir. 1982)).

The consistency of these various court rulings over an extended time period indicates that 9/11–type profiling, applied regularly as part of airport security measures, would likely violate the U.S. Constitution. The exception might be a narrowly tailored application that fell within the guidelines on profiling provided by the Department of Justice, which directly supported compelling state interest needs. These rulings appear to disallow consideration of the Israeli model, with its inherent profiling based on some level of demographic measures. However, they may well support the separation of passengers into different risk categories, as proposed in the RBS model, without undue concern regarding the violation of either DOJ guidance or the Fifth Amendment guarantee of the right to liberty. Individuals who applied for and were denied approval to be categorized as either low- or no-risk passengers would require some redress process to ensure an RBS program was not in violation of the due process clause of the Fifth Amendment, but defining such processes is beyond the scope of this thesis.<sup>43</sup>

The courts have been equally consistent in determining when individuals must be given their *Miranda* rights. Case law has determined that the passenger screening process does not constitute a custodial interrogation environment and that general security questions and routine security measures do not require advising passengers of their right against self-incrimination. However, there are situations where the passenger in question is suspected of being involved in criminal activity, and further questions after that point could be for the purpose of gathering information in support of criminal

---

<sup>43</sup> The DHS already operates traveler redress systems for individuals who believe they have been inappropriately placed on the selectee screening or no-fly listings, and for the CBP Global Entry program, and such redress programs may well be adequate to meet the due process needs of an RBS program.

prosecution. In these instances, the individual must be advised of his rights, as explained in *Miranda*, or the information and evidence discovered would not be admissible in any future criminal prosecution.

## **2. Social Acceptance**

With more than 1.7 million individuals traveling via commercial aviation each day within the United States, there is frequent interaction between the American public and the TSA at airports around the country. Arguably, the American public interacts with TSA personnel more frequently than any other government agency and holds strong opinions regarding the effectiveness and efficiency of the current passenger security screening process. These opinions are often influenced by media criticism regarding TSA policies, procedures, and effectiveness, which result in the broad perception that the vast majority of Americans do not support current airport security measures. This perception may not be entirely accurate, although public acceptance of more invasive security procedures is declining.

The decline in public acceptance of TSA security measures was particularly acute following the introduction of advanced imaging technology (AIT) whole-body scanning equipment and enhanced physical search procedures in November 2010. These more invasive measures were in direct response to the terrorist attempt on Christmas Day 2009 on board Northwest Airlines flight 263 from Amsterdam, Holland, to Detroit, Michigan. The explosive device used in that attempt was specifically constructed and concealed in a manner that was able to defeat both the security technology and security procedures in place at that time. Although an early CBS News public-opinion poll conducted during November 7–10, 2010, showed that 81 percent of respondents supported the use of AIT equipment and more thorough pat downs as necessary security measures (Condon, 2010a, p. 1), the intense media coverage of those in opposition to these enhanced security procedures resulted in a quick decline of that support. Two weeks after this initial poll, and a media frenzy characterized by headlines of “naked body scanners” and “don’t

touch my junk,” the Washington Post and ABC News conducted a similar survey on November 21, 2010. At that time social support for AIT use had dropped a full 17 percentage points, to just 64 percent.

In addition to declining support for AIT use, the survey results noted that over half of all respondents indicated that they felt the enhanced pat down process had gone too far (Condon, 2010b, p. 1). Social acceptance of these measures continued to erode, as noted in a public opinion survey conducted for the U.S. Travel Association in December 2010. The results of this poll of individuals that had flown at least once in the previous 24 months showed that a full 41 percent of respondents felt that these measures violated their basic civil rights. Support for continued use of AIT as a primary security measure for screening passengers was evidenced by only 22 percent of the respondents, and a mere 16 percent expressed positive support for the more thorough pat down searches (U.S. Travel Association [USTA], 2010, pp. 17, 21, 27). Based on these survey results, social acceptance of the current U.S. security approach has diminished following the introduction of more invasive technologies and procedures that the public perceives as going too far when applied broadly to all passengers. Absent some significant trigger to change these opinions, the current aviation security policy involving the introduction of more invasive procedures and technologies in reaction to increased sophistication in explosive-device construction and concealment techniques will continue to undermine social acceptance of the current TSA approach.

The significant impact of the 9/11 attacks and the resulting surge in negative feelings toward Muslims and individuals from the Middle East have caused a general improvement in American public support for some form of demographic profiling as an effective counterterrorism tactic. This “9/11 profiling” consists of “subjecting people who look Middle Eastern, Arab, or Muslim to discretionary law enforcement attention as a way to prevent terrorist activity” (Schildkraut, 2009, p. 5). Although public support for law enforcement use of racial profiling to prevent crime has not changed substantially prior or subsequent to 9/11, support for profiling to prevent terrorism—as opposed to crime prevention—registers different results. In a 2004 random telephone public opinion survey, while 77 percent of respondents rejected traditional profiling in the crime

prevention context, 66 percent approved the use of 9/11 profiling for counterterrorism—“an impressive 43 percentage point” difference according to the researcher (Schildkraut, 2009, p. 67). This result compares favorably with both a 2002 Pew Research Center survey and a 2005 Gallup Poll survey that found 59 percent and 53 percent support respectively for 9/11-type profiling to prevent terrorist attacks in the United States (Johnson et al., 2011, p. 4).

Immediately following the attempted terrorist attack on December 25, 2009, a CBS News poll in January 2010 found that 51 percent of respondents felt that the use of ethnic profiling as part of aviation security measures was justified. This support had declined to just 37 percent in November 2010 (Condon, 2010a). These results indicate that it is possible that the American public would support requiring some additional security scrutiny being required for passengers, based on some level of demographic or religious profiling, as is inherent in the Israeli model. However, the data highlights the potential transient nature of that support, with favorable attitudes towards profiling increasing following a well-publicized terrorist attempt and then social acceptance of ethnic profiling declining as the episode recedes into history. This transience in the social acceptability of the Israeli model is likely to present problems with any long-term implementation of this approach, absent additional terrorist attacks within the United States.

The traveling public appears more accepting of security measures that subject different groups of passengers to varying levels of security measures. The USTA survey results noted that 80 percent of respondents supported a process that included background checks of passengers to evaluate risk, while 64 percent felt it was appropriate to include questioning and other intelligence methods as alternative security measures to more invasive physical search methods (USTA, 2010, pp. 25–26). Support for separate security lines for frequent travelers was indicated by 60 percent of respondents, also the number who felt positive about volunteering personal information for prescreening and the use of a “fast track” government-issued identification card to speed through airport security measures. Overall, 65 percent of respondents supported different security requirements for travelers cleared through a U.S. government background check (USTA, 2010, pp. 29,

30, 33). Even if such a program required up to an annual application fee, support for voluntary background checks to allow travelers to speed through airport security measures remains high. In a survey reported on by the Los Angeles Times, 45 percent of all respondents indicated a willingness to pay \$150 annually to expedite their way through passenger screening. Among business travelers and “frequent leisure travelers,” support for such a fee-based, prescreening, risk assessment program was at 75 percent and 61 percent respectively (Martin, 2011, pp. 1–2). Based on these survey data, the risk-based security model is likely to receive social acceptance by the American public. Since the TSA administrator publicly announced plans to implement some form of risk-based security program for passenger screening, media reports have been generally favorable.

### **3. Political Feasibility**

Because security screening directly impacts so many citizens and private-sector entities alike, the topic is politically charged. Any approach to passenger screening must be approved and funded by Congress and the administration. Although individual members of Congress have offered criticism of the current approach to passenger screening—especially since the introduction of advanced imaging technology and enhanced physical pat down procedures—there has been no legislation passed that restricts the TSA’s authority to define requirements and procedures for aviation security. As noted in *Agee* above, one should not equate congressional silence with congressional disapproval. To the contrary, Congress expressly provided the TSA with broad power to issue, rescind, or modify any regulations deemed necessary to protect passengers from terrorist acts and hijackings aboard commercial aircraft (49 U.S.C. §§114, 44903). While it is certainly possible that Congress will find that the TSA has overreached in defining security requirements and procedures for passenger screening, it has thus far not done so, and the political feasibility of the current approach is deemed very high.

The same cannot be said with respect to political support for adopting the Israeli model. Clearly, the calls to implement this approach following each major aviation security incident have brought the approach to the attention of Congress, but no legislative action has ensued to move toward implementation. Additionally, Congress has

thus far demonstrated a reluctance to increase costs on airline passengers or air carriers to pay a greater share of aviation security costs through increased 9/11 security fees paid by the airlines or through increases in per segment passenger security fees added to the price of an airline ticket in order to fund the level of security provided at Ben Gurion Airport. Currently, passengers pay only \$2.50 per flight segment and a maximum of \$5.00 per one-way trip in security fees, generating about \$2 billion in revenue to offset a portion of the federal cost of providing aviation security (TSA, 2011g). This fee would need to be raised by more than a factor of 10 to generate \$50 billion. Even if Congress agreed to raise individual security fees, it is unlikely to double the current level of appropriations for the TSA to fund the remaining costs, and even less likely to provide a 10-fold increase in appropriations necessary to provide the entire \$60 billion per year required to implement a system equivalent to that used in Israel. Political support for implementing the Israeli model is likely very low.

Whether or not the political support exists for implementing an RBS approach is less clear. This model does not entail the cost increases associated with adopting the Israeli approach and promises to improve security effectiveness, while lessening the inconvenience on many passengers. However, RBS may well create a perception of privilege and disparate treatment as passengers are grouped in categories according to risk, even if the approach does not impinge on constitutional rights. As the TSA begins to talk publicly about its intent to shift to a risk-based security approach, there has been little, if any, public political opposition to this concept. Rather, this reality leads to the conclusion that if the general public is supportive of an RBS approach to passenger security measures, and such an approach does not increase the overall cost of providing aviation security, then political support will be strong for such measures. If the public rejects RBS because of concerns that risk categorization is accomplished through racial profiling or other socially unacceptable means, or if the public rejects the approach because of visible differences in the primary security requirements for passengers in each of the four risk categories, then political support for RBS is likely to evaporate.

## **D. CONCLUSION**

The Israeli security model would improve the security effectiveness of the passenger screening process because more time would be provided to complete primary screening. This option would also effectively mitigate risk from the current threat stemming from Islamic terrorists by profiling passengers for additional security measures. This approach would create significant constitutional problems and would likely result in the courts' rejection of these measures. Social acceptance would be mixed, with some advocating profiling and others objecting on civil rights grounds. Political support is unlikely for two primary reasons: First, the public backlash against profiling would prevent bipartisan consensus for adopting this method. Second, full implementation would increase the overall cost of passenger screening. Overall, the debatable constitutionality of this option, and the lack of social acceptance, makes the approach politically infeasible. Although this option is expected to provide a high level of security while lowering system risk in comparison to the current U.S. approach, support for the use of profiling inherent in the Israeli approach is not expected to garner the long-term acceptance of the American people. This likely outcome is based on the lack of acceptance of current procedures that are less disruptive and intrusive on the traveling public than entailed in the Israeli approach.

In contrast, the proposed RBS approach provides an equivalent level of security effectiveness to the Israeli model and offers the lowest level of systems risk of any of the three policy options. Separating passengers into risk categories based on the results of background investigations, and applying the appropriate primary security measures based on that assessed level of risk, does not conflict with First, Fourth, or Fifth Amendment rights. The RBS approach is also likely to enjoy the highest level of public and political support and is more sustainable over time than either the Israeli or current U.S. models. To realize the security benefits of the RBS approach requires that the TSA shift away from mere alarm resolution and adopt a systems alarm philosophy.

THIS PAGE INTENTIONALLY LEFT BLANK

## **VI. CONCLUSIONS AND RECOMMENDATIONS**

Risk-based security ... means moving further away from what may have seemed like a one-size-fits-all approach and establishing TSA as a high performing counterterrorism agency. It means focusing our resources on those we know the least about, and using intelligence—often classified—in better ways to inform the physical screening process.

Pistole, 2011

### **A. INTRODUCTION**

Since the terrorist attacks on September 11, 2001, the effectiveness of aviation security within the United States has been the focus of significant public and political attention. In the months following the attack, Congress passed the Aviation and Transportation Security Act (ATSA), which assigned responsibility for aviation security to the federal government through the creation of the Transportation Security Administration (TSA). Although a significant number of changes have been implemented to improve the efficacy of security screening during the past 10 years, the underlying philosophy—that all passengers pose an equal risk—has remained unchanged. This philosophy requires that every individual travelling aboard a commercial aircraft submit to the same primary security requirements during the passenger screening process. Early attempts to categorize passengers into different risk groups were unsuccessful, and changes to technology and screening procedures continue to be applied broadly to all individuals at screening checkpoints.

This approach has resulted in several problems that have been highlighted in a variety of investigative reports and media coverage. One significant challenge to continuing the current approach stems from the highly reactive nature of the process. As terrorist tactics and methods evolve, and their ability to construct and conceal explosive devices becomes more sophisticated, the TSA has responded by implementing ever more intrusive procedures and technologies that are applied to all passengers. The end result is a system that contains a high degree of threat uncertainty and one that requires the individual transportation security officer to broadly search for threat objects without foreknowledge of the actual risk posed by any individual passenger. Several reports by

the Government Accountability Office and the Inspector General for the Department of Homeland Security highlight the difficulties inherent in the current process in sustaining high levels of performance in detecting explosive devices. This continuing performance deficit, combined with the application of more intrusive procedures and technologies, generates a great deal of public and media criticism. Throughout the past decade, there have been frequent calls to change the current U.S. model and to adopt either the Israeli approach or to shift to a risk-based model. General perceptions are that the Israeli approach provides significantly greater security performance and that a risk-based model provides a commonsense solution to the aviation security problem.

This thesis provides a comparison of these two alternative models against the current U.S. approach. Evaluation of the three policy options was conducted through an analysis of both quantitative and qualitative factors. Quantitative factors include security effectiveness, which assessed security performance and the deterrence value of passenger screening, and risk mitigation. Qualitative factors include constitutional permissibility with respect to First, Fourth, and Fifth Amendment rights; social acceptance; and political feasibility. Collectively, these five factors allow for a direct comparison and the relative ranking of the models.

## **B. FINDINGS AND CONCLUSIONS**

### **1. Security Effectiveness**

The two major categories evaluated to assess overall security effectiveness of the three passenger screening approaches are detection and deterrence. Detection considered the conditional probabilities associated with detecting either a terrorist operative or an explosive device hidden either on the passenger or in his carry-on property. Conditional probabilities were determined by evaluating the various primary screening measures associated with each specific policy option. In each instance, the risk-based security approach was determined to be the most effective of the three models, although the difference between the RBS and Israeli models was an insignificant one-tenth of one percent.

Two primary reasons account for the difference in system effectiveness of the RBS and Israeli models with respect to the current U.S. model. Perhaps the most critical impact stems from how alarms are treated during the screening process. Unlike the current U.S. process, which largely resolves the individual alarm, the other two approaches treat every alarm as a systems alarm. Under the systems alarm concept, an alarm occurring anywhere in the process automatically triggers the full scope of primary and secondary security measures to be applied to both the individual and his property. For example, if a prohibited item was identified during the X-ray screening of the passenger's property, the response would entail individual explosive trace detection (ETD) screening of all individual items in the passenger's bag, separate X-ray screening of all electronic items and the empty bag itself, ETD screening of the individual passenger's hands, primary screening of the individual using both AIT and pat down procedures, and a security interview of the passenger and any travel companions. The other element that contributes to differences in system effectiveness is the time allotted to complete primary X-ray screening. A variety of research studies demonstrates a direct and logarithmic relationship between the time provided to complete visual searches and performance errors. When time for visual search is constrained, the impact of dual target cost (DTC) and satisfaction of search (SOS) phenomena increases, and detection performance decreases. Search performance of X-ray operators also increases when they know that they are screening property belonging to a passenger categorized as either a high or unknown risk and when they are not under any time constraints to complete the search. Both the Israeli and RBS models provide that search environment to improve operator performance.

The relative ranking of the deterrence value of each model also results in RBS being the best, with the current U.S. system having the lowest level of deterrence. That said, the differences between the first and last ranking are insignificant at only seven-tenths of one percent separating these models. All three models were deemed to provide effective deterrence to terrorist attempts to penetrate the passenger screening checkpoint with an explosive device.

## **2. Risk Mitigation**

Evaluation of the mitigation effects on risk to the aviation sector was narrowly limited to just the use of an explosive device that resulted in the catastrophic loss of the aircraft and all passengers. This approach permitted the isolation of the passenger screening process and the comparison of the three different models. Risk was computed using the DHS risk formula where risk is equal to the product of threat, vulnerability, and consequence ( $R = T * V * C$ ). The components of vulnerability and consequence were held constant in that analysis. For the vulnerability factor, each model was assessed as “probably not” going to fail and the vulnerability value set at 25 percent. Consequence assumed a combination of direct and indirect economic loss factors across the top 20 impacted business sectors identified in the research and was set at \$42,679 million. The threat component considered both capability, which was held constant at 95 percent, and intent, which varied across the four categories of passengers proposed in the RBS model.

Using these values, a weighted risk score was computed based on the percentage of passengers in each of the four risk categories. This evaluation determined that the model with the greatest level of risk mitigation is the RBS approach, followed by the Israeli model, and then the current U.S. model. The difference between the RBS and Israeli models reflects nearly a 30 percent reduction in weighted risk scores and stems from the increased number of passengers identified as high risk under the Israeli approach. This increase in high-risk passengers stems from the use of demographic and ethnic profiling inherent in the Israeli model that does not exist under the RBS approach, which is estimated to cause a tenfold increase in the numbers of individuals categorized as high-risk passengers.

## **3. Constitutional Permissibility**

Due to the potential impact on rights guaranteed to individuals by the U.S. Constitution, any approach to passenger security screening must be considered with respect to how the screening measures potentially impact on those rights. The three areas assessed with respect to the constitutional permissibility of the three policy options are the First, Fourth, and Fifth Amendments.

The rights to freedom of speech, religion, assembly, and association provided by the First Amendment do not present any concerns regarding the current U.S. approach. However, there is a potential impact on First Amendment rights with respect to the security interview measure contained in both the Israeli or RBS models. This potential impact stems from the requirement that some or all passengers submit to and cooperate with a security interview and the implications on the right to travel for individuals who do not successfully complete that security step. Review of various court decisions indicates that under the broad authority that Congress provided to TSA, that agency has the authority to require this step. While the Supreme Court has ruled that the right to free speech includes the right to refrain from speaking, the exercise of free speech by refraining from speech occurs within the context of the government compelling individuals to support specific points of view; the courts would sustain requiring individuals to complete the security interview as part of the totality of the passenger screening process necessary to be permitted to fly aboard a commercial aircraft. Where the security interview could implicate First Amendment rights lies in the purpose of the interview and the nature of the questions asked. If the stated purpose of the security interview is to identify the religious or political beliefs of individuals, then the courts would likely see the interview as being in conflict with the First Amendment. Where the purpose is solely to identify individuals who may have the intent to commit violence aboard the aircraft, and the questions avoid matters of religion, ethnicity, or political beliefs, the conclusion is that the courts would find no First Amendment conflicts.

Numerous court decisions have sustained security screening at airports as an appropriate and necessary administrative search exception to the Fourth Amendment right against unreasonable searches by government. This special-needs exception allows the government to conduct warrantless searches of individuals at airport checkpoints due to the compelling government interest in protecting aircraft passengers from hijacking and other acts of terrorism. Court decisions since 9/11 have clarified and supported the appropriateness of warrantless airport screening searches, including the decision that these searches do rely on consent and that once screening has started, individuals cannot withdraw from the screening process until it has been completed. The courts have also

supported the application of different levels and search methods to different individuals based on risk, as well as the introduction of more intrusive technologies and procedures that have been implemented in response to changes in the terrorist threat. Although various court decisions have alluded to the level of intrusiveness involved in airport searches, they have consciously avoided establishing an outer boundary of intrusiveness in the aviation context. What the courts have stated is that warrantless airport searches are constitutionally permissible, even when the approach does not involve the least intrusive methods available. The consistency in court decisions over the past several decades sustaining the permissibility of airport searches leads to the conclusion that none of the three models, including adopting the systems alarm approach contained in the Israeli and RBS models, would violate Fourth Amendment protections. Because the RBS model calibrates the level of intrusiveness for each risk category by varying the type of physical screening measures applied, the courts may well view this approach as more constitutionally supportable.

It is the Fifth Amendment guarantees to due process, equal protection, and the right to liberty where the models do raise constitutional concerns. In particular, the courts would likely determine that the use of ethnicity and other demographic criteria to profile passengers as high risk, as is done under the Israeli model, is incompatible with the right to equal protection. Some court decisions support the Department of Justice guidelines regarding the use of racial or ethnic profiling in the aviation security application in exigent circumstances to prevent catastrophic events, but the institutional application of racial or ethnic profiling is incompatible with the Fifth Amendment. Another potential constitutional conflict inherent in all three models is the issue of custodial interrogation. The courts have generally held that, similar to searches as part of border security, the airport search environment does not typically constitute a custodial environment and that individuals do not need to be advised of their right against self-incrimination before being asked questions in that environment. However, the courts are very clear that in situations where there is an individualized suspicion of criminality, or upon discovery of criminal activity, the individual must be advised of his Fifth Amendment rights, as defined in *Miranda v. Arizona*, or any evidence will be suppressed during criminal proceedings.

#### **4. Social Acceptance**

The social acceptance criterion assesses the degree to which the American people will accept the security approaches associated with each policy option. With more than 1.7 million individuals travelling by commercial aviation within the United States, the TSA arguably interacts with the general public more frequently than does any other government agency. Negative media stories abound regarding prohibited items getting past the checkpoint undetected, pat downs procedures applied to children and elderly individuals, and more invasive equipment like advanced imaging technology, dubbed “naked body scanners” by some. This negative media coverage and the frequent interaction with the passenger screening process in an environment absent any significant terrorist attack within the United States since 9/11 has caused many individuals to criticize the TSA and openly complain that the agency lacks common sense. To many frequent travelers, the checkpoint security process is an inconvenience and a cause of delay, and for the infrequent traveler security screening is highly stressful. In general, the current U.S. model is not widely accepted or supported by many individuals, with just 22 percent of respondents supporting the use of AIT equipment and only 16 percent supporting more thorough pat downs in December 2010.

The use of discretionary law enforcement counterterrorism techniques directed to individuals who look Muslim or Arab or who come from the Middle East, as in the Israeli model, appears to have transient public support. Support for these measures increased in the immediate aftermath of 9/11 and the attempted attack on December 25, 2009, but it quickly declined to nearly half the postincident peak levels. With less than 40 percent of respondents maintaining steady support for profiling as an appropriate aviation security measure, the long-term support for the Israeli model is questionable.

The travelling public appears decidedly more supportive of the RBS model. In two separate opinion polls conducted in 2010, roughly 65 percent of respondents supported the idea of separate security requirements for individuals who completed a government-conducted background check. Among frequent business and leisure

travelers, support for separating passengers into different categories based on risk was as high as 75percent—even if it required a \$150 per year enrollment fee to defray the costs of the background check.

Based on this research, the RBS model has the highest likelihood of being the most socially acceptable to individuals within the United States. This conclusion is based on an assessment that the public views a risk-based approach as common sense and as capable of minimizing the inconvenience to a large percentage of passengers placed in the low-risk category. The fact that a large percentage of frequent travelers expressed a willingness to pay for such an approach, even though they were not provided any specific details regarding how the screening process would be expedited for low-risk passengers, supports this conclusion. Although public support for the current U.S. approach is low, it is roughly equal to the level of public support for racial profiling for general law enforcement purposes, which by and large is socially unacceptable to the American people. The conclusion drawn is that institutionalizing profiling as part of the aviation security process would be less socially acceptable than the current U.S. approach, and the Israeli model is the least favorable from this perspective.

## **5. Political Feasibility**

The topic of passenger security screening is politically charged, in part because it directly impacts so many citizens and private-sector entities and also because of the many congressional committees and subcommittees that provide oversight to the TSA. Even though the TSA administrator recently announced the desire to shift to a risk-based passenger screening approach, Congress has the ability to exercise considerable influence over any policy option. Therefore, the political feasibility of policy options must be considered.

In some respects, it is arguably easier for Congress to continue with the current U.S. model than it is to adopt one of the other two options being evaluated. When the Aviation and Transportation Security Act was enacted, placing the TSA in charge of aviation security, Congress provided that agency with broad authority to define and revise security procedures and standards in order to protect airline passengers from acts

of terrorism. Despite frequent criticism from individual member of Congress regarding the effectiveness of passenger screening and the implementation of more invasive procedures and technologies, the broad authority granted the TSA has not been restricted, and funding to implement these changes has been provided. While it is certainly possible that Congress will at some point determine that the TSA has overreached, it has thus far not done so, and the conclusion is that the political feasibility of the current U.S. model remains very high.

The same conclusion cannot be reached with respect to implementing the Israeli security model. There have been several calls for implementing the Israeli model during the last decade, yet no legislative action has resulted to move toward implementation of that approach. This situation stems from two primary causes. First, replicating the Israeli model throughout the 450 federalized airports within the United States for which the TSA has direct security responsibility for screening commercial airline passengers and their baggage is cost prohibitive and represents an assessed annual cost of close to \$60 billion. The fact that Congress has thus far resisted requests by the administration to raise the per-ticket security fee from its current level of \$2.50 per segment to \$5.00 per segment leads to the conclusion that there is currently no political will or perceived need to broadly implement the Israeli model. The second reason why adopting the Israeli model is likely not politically feasible stems from the use of profiling that is embedded in the process and the low probability that political consensus to institutionalize some type of demographic-based profiling could be reached. The overall conclusion is that the Israeli model has the lowest level of political feasibility of any of the three policy options.

The political feasibility of implementing the RBS approach is less clear. Since the TSA administrator testified in early 2011 that he was moving toward a risk-based approach, political criticism of that idea has been muted, and comments from political leaders have been generally supportive. The fact that the RBS model holds the promise of improving security effectiveness without increasing costs, and that many travel groups and trade associations are on record in support of an RBS approach, argues for political feasibility. However, if the public rejects the RBS model over concerns that categorizing passengers by risk creates a “privileged class” of individuals or is based on some

unacceptable demographic means of profiling or because the rejection of applicants for the low-risk category impacts employment or other aspects of individuals lives, political support for the approach could quickly evaporate. Considering all of these factors, the conclusion is that the political feasibility of the RBS model is greater than the Israeli approach but less certain than continuing the current U.S. process.

## 6. Summary of Findings

Table 17 provides a side-by-side comparison of the relative rankings of each of the three policy options with respect to the five criteria used in this evaluation. As noted in Chapter III, each criterion is assigned a relative ranking where 1 reflects the best option for achieving the desired evaluative criteria outcome and 3 reflects the least attractive option to achieve this outcome. As an example, under the security effectiveness criteria, the RBS option is considered the most effective and is assigned a value of 1. Conversely, the current U.S. approach is evaluated as the least effective and is assigned a relative value of 3.

| <b>Model</b> | <b>Security Effectiveness</b> | <b>Risk Mitigation</b> | <b>Constitutionally Permissible</b> | <b>Social Acceptance</b> | <b>Political Feasibility</b> |
|--------------|-------------------------------|------------------------|-------------------------------------|--------------------------|------------------------------|
| Current U.S. | 3                             | 3                      | 2                                   | 2                        | 1                            |
| Israeli      | 2                             | 2                      | 3                                   | 3                        | 3                            |
| Risk Based   | 1                             | 1                      | 1                                   | 1                        | 2                            |

Table 17. Side-by-Side Model Comparison

This use of relative rankings permits comparison of each option against the evaluative criteria by adding the respective numbers, where the model with the lowest total score is potentially the best of the three policy choices. For Table 17, the total scores for the three policy choices are: current U.S. model = 11; Israeli model = 13; and risk-based security model = 6. Using these five criteria to evaluate each policy option in the narrowly defined context of the passenger screening portion of the total aviation security system, the risk-based security model is by far the best approach for Congress, the

Department of Homeland Security, the Transportation Security Administration, and the American public to consider. The benefits of the RBS model are that it offers high levels of security effectiveness and deterrence; it effectively mitigates the risk to aviation from explosive devices brought through the checkpoint; it does not conflict with rights guaranteed under the First, Fourth, and Fifth Amendments of the U.S. Constitution as interpreted by various court decisions; it is likely more socially acceptable than either of the other two approaches; and implementation is likely politically feasible.

### **C. IMPLEMENTATION CHALLENGES AND RECOMMENDATIONS**

Implementing the RBS approach is not without its challenges, which are not addressed in this thesis. The following provides an overview and recommendations related to some of these challenges.

#### **1. Physical Changes to Airport Checkpoints**

Physical changes will be necessary at airport checkpoints in order to efficiently separate individuals by risk category so that individuals are subject to the appropriate security measures calibrated to their risk category (Poole & Passantino, 2003, p. 14). These checkpoint reconfiguration changes need to support 1) the ability for individuals categorized as trusted and low-risk to self-select for processing through separate security lanes; 2) installation of biometric identity verification technology at checkpoints and boarding gates; and 3) the ability to separate high-risk and ordinary passengers for security screening using accepted protocols. Some airports have already installed biometric airport badge readers and designated specific lanes for employee and aircrew use, and it may be possible to leverage these efforts and equipment as part of the implementation strategy.

#### **2. Technology Integration and Implementation Costs**

Technology integration and RBS implementation costs involve efficiently integrating various existing government databases into a comprehensive database required to support risk-based checkpoint screening and biometric identity verification. Integration of databases and different technologies is likely a significant hurdle. Existing

identification systems such as airport access control systems, the DHS Automated Biometric Identification System (IDENT) data storage system,<sup>44</sup> the Global Entry and US-VISIT systems operated by Customs and Border Protection, the Transportation Worker Identity Card (TWIC), Homeland Security Presidential Directive 12 (HSPD-12)<sup>45</sup> identification card databases, and the background investigation systems operated by the Department of Defense and the Office of Personnel Management at a minimum would be necessary to fully implement the program. Additionally, the infrastructure and integration of a new government program for registered traveler participants would also be necessary.

The complexity of this effort is believed to equal about half that of implementing the Secure Flight program. Using the TSA costs combined with the cost of changes required at the Terrorist Screening Center to support the Secure Flight implementation provides a basis for estimating the scope of work and costs to integrate a risk-based passenger screening program. According to the Department of Justice Inspector General (DOJ IG), the direct and indirect costs of Secure Flight for 2005 and 2006 exceeded \$58 million (DOJ, 2005, pp. 11–12). In addition to DOJ costs, the TSA received appropriations of nearly \$300 million for the program during the five-year period from 2004 through 2009 (Barrick, Hite, & Wilshusen, 2009, p. 8). Leveraging the lessons learned and the development effort already completed on Secure Flight, an estimate of initial implementation costs of between \$180 million to \$200 million over three or four years provides a reasonable starting point to fully develop and implement the risk-based passenger screening program as proposed above.

---

<sup>44</sup> IDENT is a DHS-wide system for the storage and processing of biometric and biographic information for DHS national security, law enforcement, immigration, intelligence, and other DHS mission-related functions (Yonkers, 2006, p. 2) .

<sup>45</sup> HSPD-12 requires a government-wide, standardized, and secure identification card for all federal employees and government contractors. When fully implemented, the biometric identification card will be used for employees to gain access to federal facilities based on rights granted to the individual cardholder. HSPD-12 is also being considered for access to federal government information technology systems ([http://www.dhs.gov/xabout/laws/gc\\_1217616624097.shtm](http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm)).

### **3. Background Investigations and Sustaining Program Costs**

Policy decisions are needed regarding the level of background investigation required for individuals to be classified as either no- or low-risk travelers. Additionally, there is a need to establish clear and transparent rules regarding the factors that would automatically disqualify an individual from these two lowest risk groups. Similar rules and policies are required with respect to recurrent vetting so that information from the intelligence or law enforcement communities that changes the risk assessment of individuals can be quickly applied. The scope of the initial and recurrent vetting requirements drives initial and annual program sustaining costs (Dillingham, 2002, p. 3). Policies and procedures are also required to establish a redress process, determine what information could be shared with individuals denied approval as a low-risk traveler, and set appropriate limits on how this information would be shared (Dillingham, 2002, pp. 14–16; Poole & Passantino, 2003, pp. 19–23).

As part of these policy decisions, Congress and the administration will also need to decide whether to implement a fee to offset the costs of the RBS program or whether the program would remain fully funded through appropriations. Making the application process free to all individuals would likely increase the number of people who applied for the program, which would improve the efficiency of the overall screening process. Charging an application and background investigation fee could dissuade the infrequent traveler from applying for program participation and potentially inhibit realizing the full level of efficiencies and security benefits possible with the RBS model.

Research indicates that once the program becomes operational, a fee-based approach would defray most if not all operational and maintenance program costs. Initial estimates for Registered Traveler assumed participants would be willing to pay an initial \$100 enrollment fee and a nominal annual user fee for perpetual vetting (Dillingham, 2002, p. 18). Participants in the Global Entry program pay a nonrefundable enrollment fee of \$100 for two years' enrollment (United States Customs and Border Protection, 2009, p. 2). The 250,000 participants in the private-sector Registered Traveler program paid a \$200 annual fee to get head-of-the-line privileges with no decrease in security requirements, generating approximately \$250 million annually (Franks, 2009).

## **D. AREAS FOR FUTURE RESEARCH**

This thesis is narrowly tailored in scope to just the comparison of the current U.S., Israeli and risk-based passenger security screening models, using information available in open sources. Due to the limitations of this focus, the end result is not intended to be a fully implementable solution, and several areas for further research can be identified.

### **1. Security Officer IED Detection Performance**

Prior research into visual search demonstrates that the time allowed for search and the alertness of the operator to the increased likelihood of finding a target object can improve detection performance, but this research was not conducted in the aviation security context. A specifically designed experiment on the detection of sophisticated and well-concealed explosive device components in the passenger screening environment would be beneficial to validate or dispute these assumptions.

### **2. Security Interview**

The RBS model shifts away from a broad search for objects to a focus on individuals and the identification of passengers who intend to potentially commit an act of violence or terrorism aboard the aircraft. In support of this change, the RBS model employs a security interview of all individuals identified as high risk. Research into the structure of the interview process and the nature of questions to be asked that support the identification of intent would provide an empirical basis for the security interview and would guide the training development efforts needed to implement that approach.

### **3. Adapting to Different Airport Configurations**

Commercial airports throughout the United States vary widely in design and physical constraints at passenger screening checkpoints. Application of the RBS model across various airport configurations would require tailored solutions that support implementation both at large, multiple-lane checkpoints and at smaller two-lane configurations. Research into the way in which the RBS model would operate across these different physical environments would benefit implementation and operation decisions.

#### **4. Systems Alarm Impact**

As noted above and in Chapter V, adopting a systems alarm philosophy is key to realizing the security benefits of the RBS model. Implementing this approach to the manner in which security officers respond to alarms creates a potential impact on checkpoint design and equipment requirements. Research on the capacity necessary to address the primary and secondary search needs of the unknown- and high-risk traveler under the systems alarm approach applied to all four risk categories would benefit implementation decisions as well as checkpoint staffing requirements.

THIS PAGE INTENTIONALLY LEFT BLANK

## LIST OF REFERENCES

- Air Line Pilots Association. (2010). Meeting today's aviation security needs: A call to action for a trust-based security system. ALPA White Paper, Washington, D.C. Retrieved September 4, 2010, from [http://www.alpa.org/portals/alpa/pressroom/pressreleases/2010/whitepapers/AviationSecuritySystemWP\\_1-19-10.pdf](http://www.alpa.org/portals/alpa/pressroom/pressreleases/2010/whitepapers/AviationSecuritySystemWP_1-19-10.pdf)
- Alberto, V., & Bogatz, D. (2003). Computer assisted passenger prescreening system ("CAPPS II"): National security v. civil liberties. Retrieved January 12, 2011, from <http://www.maxwell.syr.edu/uploadedFiles/campbell/events/AlbertoBogatz.pdf>
- Atlas, P. (2010). Psychology, not just technology for airport security: Real clear politics. Retrieved April 9, 2011, from [http://www.realclearpolitics.com/articles/2010/01/06/psychology\\_not\\_just\\_technology\\_for\\_airport\\_security\\_99795.html](http://www.realclearpolitics.com/articles/2010/01/06/psychology_not_just_technology_for_airport_security_99795.html)
- Aviation and Transportation Security Act. Public Law 107-71 (2001).
- Aviation security market: TSA plans to procure and deploy 1,800 advanced imaging technology machines (AITs) by 2010. (2010). *Homeland Security News*. Retrieved November 25, 2010, from <http://www.homelandsecuritynews.info/2010/03/aviation-security-market-tsa-plans-to-procure-and-deploy-1800-advanced-imaging-technology-machines-ait-by-2014/>
- Babu, V. L. L., Batta, R., & Lin, L. (2006). Passenger grouping under constant threat probability in an airport security system. *European Journal of Operational Research* 168: 633–44.
- Barnett, A. (2004). CAPPS II: The foundation of aviation security. *Risk Analysis* 24(4): 909–16.
- Barry, E. (2011). Deadly blast comes at sensitive time for Russia. *New York Times*. Retrieved January 30, 2011, from <http://www.nytimes.com/2011/01/25/world/europe/25moscow.html>
- Berbaum, K. S., Brandser, E. A., Franken, E. A., Dorfman, D. D., Calswell, R. T., and Krupinski, E. A. (2001). Gaze dwell times on acute trauma injuries missed because of satisfaction of search. *Academic Radiology* 8: 304–14.

- Berrick, C. A. (2008). Transportation security: Efforts to strengthen aviation and surface transportation security continue to progress, but more work remains. Testimony before the Subcommittee on Transportation Security and Infrastructure Protection, Committee on Homeland Security, House of Representatives (April 15, 2008). Washington, D.C.: Government Accountability Office, GAO-08-651T. Retrieved August 9, 2009, from <http://www.gao.gov/new.items/d08651t.pdf>
- Berrick, C. A., Hite, R. C., & Wilshusen, G. C., (2009). TSA has completed key activities associated with implementing secure flight, but additional actions are needed to mitigate risks. Washington D.C.: Government Accountability Office, GAO-09-292. Retrieved August 15, 2009, from <http://www.gao.gov/new.items/d09292.pdf>
- Blumenkrantz, Z., & Stern, Y.; (2007). *Colored Tags for Arab's Luggage at Ben Gurion Airport Discontinued*; *Haaretz*, (July 8, 2007). Retrieved April 9, 2011 from <http://www.haaretz.com/news/colored-tags-for-arabs-luggage-at-ben-gurion-airport-discontinued-1.227007>
- Bowen, W. Q. (2002). Deterring mass-casualty terrorism. National Defense University, *Joint Force Quarterly* 30(Summer): 25–29. Retrieved October 2, 2002, from <https://www.hsdl.org/?view&did=607>
- Breverman, E., & Ortiz, D. R., (2002). Federal legal constraints on profiling and watch lists. In *Protecting America's Freedom in the Information Age*, 149–60). New York: Markel Foundation. Retrieved October 7, 2010, from [http://www.markle.org/downloadable\\_assets/nstf\\_full.pdf](http://www.markle.org/downloadable_assets/nstf_full.pdf)
- Bruner, J. S., & Postman, L. (1949). On the perception of incongruity: A paradigm. *Journal of Personality* 18(2): 206–23. Retrieved June 10, 2011, from <http://web.ebscohost.com.libproxy.nps.edu/ehost/pdfviewer/pdfviewer?sid=b37290d0-e2b7-4388-9706-8660ad2dcab6%40sessionmgr110&vid=2&hid=126>
- Bush, G. W. (2002). National strategy for homeland security. Washington, D.C.: The White House. Retrieved May 10, 2009, from [http://www.dhs.gov/xlibrary/assets/nat\\_strat\\_hls.pdf](http://www.dhs.gov/xlibrary/assets/nat_strat_hls.pdf)
- Cane, M. S., Dunsmoor, J. E., LaBar, K. S., & Mitroff, S. R. (2011). *Anticipatory anxiety hinders detection of a second target in dual-target search*. Retrieved April 18, 2011, from [http://www.duke.edu/~mitroff/papers/Cain\\_Dunsmoor\\_LaBar\\_Mitroff\\_inpress.pdf](http://www.duke.edu/~mitroff/papers/Cain_Dunsmoor_LaBar_Mitroff_inpress.pdf)

- Chertoff, M. (2009). *The national infrastructure protection plan: Partnering to enhance protection and resiliency*. Washington D.C.: Department of Homeland Security. Retrieved October 14, 2010, from <https://www.hsdl.org/?view&doc=107536&coll=limited>
- CNN. (2011). *Airport security: How the Israelis do airport security; CNN Opinion*. Retrieved January 15, 2011, from [http://articles.cnn.com/2010-01-11/opinion/yeffet.air.security.israel\\_1\\_airport-security-isaac-yeffet-el-al/4?\\_s=PM:OPINION](http://articles.cnn.com/2010-01-11/opinion/yeffet.air.security.israel_1_airport-security-isaac-yeffet-el-al/4?_s=PM:OPINION)
- Condon, S. (2010a). Poll: 4 in 5 support full-body airport scanners. CBS News. Retrieved September 5, 2011, from [http://www.cbsnews.com/8301-503544\\_162-20022876-503544.html](http://www.cbsnews.com/8301-503544_162-20022876-503544.html)
- Condon, S. (2010b). After a week of backlash, is public opinion turning against the TSA measures? CBS News. Retrieved September 5, 2011, from [http://www.cbsnews.com/8301-503544\\_162-20023682-503544.html](http://www.cbsnews.com/8301-503544_162-20023682-503544.html)
- Croft, J. (2004). Without a trace: Recent terrorism attacks in Russia expose a potential gap in US airline security. *Air Transport World*. Retrieved August 9, 2009, from <http://www.atwonline.com/channels/safetySecurity/article.html?articleID=1119>
- Davis, P. K., & Jenkins, B. M. (2002). Deterrence and influence in counterterrorism: A component in the war on al Qaeda. Santa Monica, CA: Rand Corporation. Retrieved March 15, 2011, from [http://www.rand.org/content/dam/rand/pubs/monograph\\_reports/2005/MR1619.pdf](http://www.rand.org/content/dam/rand/pubs/monograph_reports/2005/MR1619.pdf)
- Davis, D. W., & Silver, B. D. (2004). Civil liberties vs. security: Public opinion in the context of the terrorist attacks on America. *American Journal of Political Science* 48(1): 28–46. Retrieved April 21, 2011, from <http://web.ebscohost.com.libproxy.nps.edu/ehost/pdfviewer/pdfviewer?sid=2e957f03-f9de-485d-8f98-db53fb7703bc%40sessionmgr113&vid=2&hid=112>
- DeGrave, M. (2004). Airline passenger profiling and the Fourth Amendment: Will CAPPS II be cleared for takeoff? *Boston University Journal of Science and Technology Review* 10(1): 125–53.
- Dempsey, J. X., & Flint, L. M. (2004). Commercial data and national security. 72 *Geo. Wash. L. Rev.* 1459.
- Dillingham, G.L. (2001). Aviation security: Terrorist acts illustrate severe weaknesses in aviation security. Testimony before the Subcommittees on Transportation, Senate and House Committees on Appropriations. Washington, D.C.: Government Accountability Office, BAO-01-1166T.

- Dillingham, G. L. (2002). Registered Traveler Program policy and implementation Issues. Washington D.C.: Government Accounting Office, GAO-03-253. Retrieved August 9, 2009, from <http://www.gao.gov/new.items/d03253.pdf>
- Dillingham, G. L. (2003). Aviation security: Progress since September 11, 2001, and the challenges ahead. Testimony Before the Committee on Commerce, Science and Transportation, U.S. Senate. Washington D.C.: Government Accounting Office, GAO-03-1150T. Retrieved January 13, 2011, from <http://www.gao.gov/new.items/d031150t.pdf>
- Dillingham, G. L. (2009). Terrorist acts illustrate severe weaknesses in aviation security. Washington D.C.: Government Accountability Office, GAO-01-1166T. Retrieved August 5, 2009, from <http://www.gao.gov/new.items/d011166t.pdf>
- Dillingham, G. L. (2010). Commercial aviation: Better information about airline-imposed fees and the refundability of government-imposed taxes and fees could benefit consumers. Washington D.C.: Government Accountability Office, GAO-10-885T. Retrieved November 27, 2010, from <http://www.gao.gov/products/GAO-10-885T>
- Downey, M., & Menzies, T. (2002). Countering terrorism in transportation. *Issues in Science and Technology* 18(4): 58–64. Retrieved October 4, 2010, from <http://www.issues.org/18.4/downey.htm>
- Elias, B. (2005). Aviation security-related findings of the 9/11 Commission. Washington, D.C.: Congressional Research Service. Retrieved August 2, 2009, from <https://www.hsdl.org/nps18-04-805-09-1.pdf>
- Ervin, C. K. (2007). The status of U.S. counterterrorism and homeland security. Foreign Policy Research Institute. Retrieved August 15, 2009, from <http://www.fpri.org/enotes/200703.ervin.statuscounterterrorismhomelandsecurity.html>
- Ficks, M. (2003). Exposing hostile intent. *Access Control and Security Systems*. Retrieved April 9, 2011, from [http://securitysolutions.com/news/security\\_exposing\\_hostile\\_intent/](http://securitysolutions.com/news/security_exposing_hostile_intent/)
- Fiske, I. D. (2010). Failing to secure the skies: Why America has struggled to protect itself and how it can change. 15 Va. Jour. L. & Tech. 173.
- Fleck, M. S., Samei, E., & Mitroff, S. R. (2010). Generalized “Satisfaction of Search”: Adverse influences on dual-target search accuracy. *J. of Experimental Psychology* 10(1): 60–71.

- Florence, J. (2006). Making the no fly list fly: A due process model for terrorist watchlists; *Yale L. J.* 115(8): 2148–81.
- Franks, T. (2009). TSA's Registered Traveler program grounded. *USA Today* (June 23, 2009). Retrieved August 15, 2009, from [http://www.usatoday.com/travel/flights/2009-06-22-frequent\\_N.htm](http://www.usatoday.com/travel/flights/2009-06-22-frequent_N.htm)
- Fried, B. (2008). A look at Ben Gurion International Airport security. Retrieved April 9, 2011, from <http://www.homelandsecurity.org/journal/Default.aspx?oid=42&ocat=3>
- Gabbodon, S. L., Penn, E. B., Jordan, K. L., & Higgins, G.E. (2009). The influence of race/ethnicity on the perceived prevalence and support for racial profiling at airports. *Criminal Justice Policy Review* 20(3): 344–58. Retrieved April 9, 2011, from <http://cjp.sagepub.com.libproxy.nps.edu/content/20/3/344.full.pdf+html>
- Garrick, B. J. (2004). Comments on "CAPPS II: The foundation of aviation security." *Risk Analysis* 24(4): 925–27.
- Godwin, H. J., Menneer, T., Cave, K. R., Helman, S., Way, R. L., and Donnelly, N. (2010). The impact of relative prevalence on dual-target search for threat items from airport X-ray screening. *Acta Psychologica* 134: 79–84.
- Golaszewski, R., & Levine, M. E. (2001). E-Z Pass for aviation. *Airport Magazine* 13(6): 54–55.
- Gordon, P., Kim, S., Moore, J. E., Park, J., & Richardson, H. W. (2005). The economic impacts of a terrorist attack on the U.S. commercial aviation system. University of Southern California. Retrieved September 27, 2011, from <http://create.usc.edu/assets/pdf/51835.pdf>
- Gore, A. (1997). Final report of the White House Commission on Aviation Safety and Security. Washington D.C.: Government Printing Office. Retrieved February 14, 2011, from <http://permanent.access.gpo.gov/lps19581/whc97rpt.htm>
- Hamilton, L., & Gorton, S. (2004). Statement before the Subcommittee on Commercial and Administrative Law and the Subcommittee on the Constitution of the Committee on the Judiciary, U.S. House of Representatives, August 20, 2004. Retrieved August 8, 2009, from <http://judiciary.house.gov/legacy/hamgor082004.htm>
- Hasisi, B. & Weisburd, D. (2010). Moving beyond ascribed identities: Legitimacy and procedural justice in airport security. Paper presented at the annual meeting of the ASC, San Francisco Marriott, San Francisco, California. Retrieved April 9, 2011, from [http://www.allacademic.com/meta/p431793\\_index.html](http://www.allacademic.com/meta/p431793_index.html)

- Hellman, Z. (2010). Secure the air. *Jerusalem Post*. Retrieved March 14, 2011, from <http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic>
- Herzog, S. (2005). Constitutional problems posed by aviation security post September eleventh. 6 *Fla. Coastal L. Rev.* 361(Spring 2005): 361–92.
- Hoffman, B. (2006). *Inside Terrorism*. New York: Columbia University Press.
- Holden, R. T. (1986). The contagiousness of aircraft hijacking. *American Journal of Sociology* 91(4): 874–904. Retrieved April 10, 2011, from <http://www.jstor.org.libproxy.nps.edu/stable/pdfplus/2779961.pdf?acceptTC=true>
- Jackson, B. A. (2008). Marrying prevention and resiliency: Balancing approaches to an uncertain terrorist threat. Santa Monica, CA: Rand Corporation. Retrieved July 21, 2009, from [https://www.hsdl.org/RAND\\_OP236.pdf](https://www.hsdl.org/RAND_OP236.pdf)
- Jackson, B. A., Chan, E. W., & Latourrette, T. (2011). Assessing the security benefits of a trusted traveler program in the presence of attempted attacker exploitation and compromise. Santa Monica, CA: Rand Corporation. Retrieved April 15, 2011, from [http://www.rand.org/content/dam/rand/pubs/working\\_papers/2011/RAND\\_WR855.pdf](http://www.rand.org/content/dam/rand/pubs/working_papers/2011/RAND_WR855.pdf)
- Jackson, B. A., & Frelinger, D. R. (2009). Emerging threats and security planning: How should we decide what hypothetical threats to worry about? Santa Monica, CA: Rand Corporation. Retrieved July 21, 2009, from [https://www.hsdl.org/RAND\\_OP256.pdf](https://www.hsdl.org/RAND_OP256.pdf)
- Jamison, R.D. (2009). Interim integrated risk management framework. Washington D.C.: Department of Homeland Security.
- Johnson, D., Brazier, D., Forrest, K., Ketelhut, C., Mason, D., & Mitchell, M. (2011). Attitudes toward the use of racial/ethnic profiling to prevent crime and terrorism. *Criminal Justice Policy Review*. Retrieved April 20, 2011, from <http://cjp.sagepub.com.libproxy.nps.edu/content/early/2011/01/25/0887403410381801.full.pdf+html>
- Johnson, K., & Gorman, S. (2011). Bomb implants emerge as airline terror threat. *Wall Street Journal*, July 7, 2011. Retrieved September 29, 2011, from <http://online.wsj.com/article/SB10001424052702303365804576429741400016376.html>

- Karp, A. (2010). Airports encourage governments to reassess security approach. *ATW Online*, October 5, 2010. Retrieved October 6, 2010, from <http://atwonline.com/airports-encourage-governments-reassess-security-approach-1005>
- Kean, T. H., Hamilton, L., Ben-Veniste, B., Kerrey, B., Fielding, F. F., Lehman, J. F., Gorelock, J.S., Roemer, T. J., Gorton, S., & Thompson, J.R. (2004). *The 9/11 Commission: Final report of the National Commission on Terrorist Attacks upon the United States*. Harrisonburg, VA: R.R. Donnelley.
- Kelly, C. (2009). The “Israelification” of airports: High security, little bother. *Toronto Star*, December 30, 2009. Retrieved April 10, 2011, from <http://www.thestar.com/news/world/article/744199---israelification-high-security-little-bother>
- Kite, L. A. (2004). Red flagging civil liberties and due process rights of airline passengers: Will a redesigned CAPPs II system meet the constitutional challenge? 61 *Wash. & Lee L. Rev.* 1385.
- Koopman, B. O. (1956). The theory of search: II. Target detection. *Operations Research* 4(5): 503–31.
- Kraus, D. M. (1973). Searching for hijackers: Constitutionality, costs, and alternatives. *University of Chicago L. Rev.* 40(2): 383–420.
- Kravitz, D. (2010). Airport “pat-downs” cause growing passenger backlash. *Washington Post*, November 13, 2010. Retrieved January 30, 2011, from <http://www.washingtonpost.com/wp-dyn/content/article/2010/11/12/AR2010111206580.html>
- Kutz, G. D., & Cooney, J. W. (2007). Vulnerabilities exposed through covert testing of TSA’s passenger screening process. Washington, D.C.: Government Accountability Office, GAO-08-48T. Retrieved August 6, 2009, from <http://www.gao.gov/new.items/d0848t.pdf>
- Lappin, Y. (2010). Ben-Gurion Airport revolutionizes security with Unipass biometric system. *Jerusalem Post*, January 5, 2010. Retrieved April 9, 2011, from <http://www.jpost.com/israel/Article.aspx?id=165291>
- Levine, M. (2011). Napolitano: Israeli-style security won’t work for U.S. Retrieved April 24, 2011, from <http://www.foxnews.com/politics/2011/01/04/napolitano-israeli-style-security-wont-work/>
- Lewis, T. G. (2006). *Critical infrastructure protection in homeland security: Defending a networked nation*. Hoboken, NJ: John Wiley & Sons.

- Lipton, E. (2010). U.S. sets new rules for packages on cargo planes. *New York Times*, November 8, 2010. Retrieved January 30, 2011, from <http://www.nytimes.com/2010/11/09/us/09cargo.html>
- Lowrey, A. (2010). Foreign policy: The costs of Israel level security. National Public Radio, January 8, 2010. Retrieved January 16, 2011, from <http://www.npr.org/templates/story/story.php?storyId=122352039>
- Martin, H. (2011). Many fliers say they'd pay for pre-screening. *Los Angeles Times*. Retrieved September 5, 2011, from <http://articles.latimes.com/2011/jul/04/business/la-fi-travel-briefcase-20110704>
- Martonosi, S. E., & Barnett, A. (2006). How effective is security screening of airline passengers? *Interfaces*, 1–8. Retrieved October 10, 2010, from <http://www.hlswatch.com/sitedocs/securityscreening.pdf>
- Masse, T., O'Neil, S., & Rollins, J. (2007). The Department of Homeland Security's risk methodology: Evolution, issues and options for Congress. Washington D.C.: Congressional Research Service. Retrieved October 14, 2010, from <http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA462494&Location=U2&doc=GetTRDoc.pdf>
- McCarley, J. S., Kramer, A. F., Wickens, C. D., Vidoni, E. D., & Boot, W. R. (2004). Visual skills in airport-security screening. *Psychological Science* 15(5): 302–6.
- McLay, L. A., Jacobson, S. H., & Kobza, J. E. (2006). A multilevel passenger screening problem for aviation security. *Naval Research Logistics* (53): 183–97.
- McLay, L. A., Jacobson, S. H., & Kobza, J. E. (2008). Making skies safer: Applying analytics to aviation passenger prescreening systems. *Analytics Magazine* (Spring 2008). Retrieved October 10, 2010, from <http://analytics-magazine.com/spring-2008/243-making-skies-safer-applying-analytics-to-aviation-passenger-prescreening-systems.html>
- McLay, L. A., Jacobson, S. H., & Nikolaev, A. G. (2008). A sequential stochastic passenger screening problem for aviation security. *IIE Transactions* 41: 575–91.
- Menneer, T., Barrett, D. J. K., Phillips, L., Donnelly, N., & Cave, K. R. (2007): Costs in searching for two targets: Dividing search across target types could improve airport security screening. *Applied Cognitive Psychology* 21: 915–32. Retrieved April 18, 2011, from <http://torpedo.nrl.navy.mil.libproxy.nps.edu/tu/ps/dpc.html?dsn=8945846>

- Minert, S. R. (2006). Square pegs, round hole: The Fourth Amendment and preflight searches of airline passengers in a post-9/11 world. 2006 B. Y. U. L. Rev. 1631.
- Moghaddam, F. M. (2006). *From the terrorist's point of view: What they experience and why they come to destroy*. Westport, CT: Praeger Security International.
- Mohammed, A., & Goo, S. K. (2006). Government increasing turning to data mining: Peek into the private lives may help hunt for terrorist. *Washington Post*, June 15, 2006. Retrieved January 15, 2011, from [http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063\\_pf.html](http://www.washingtonpost.com/wp-dyn/content/article/2006/06/14/AR2006061402063_pf.html)
- Morgan, D. (2001). Aviation security technologies and procedures: Screening passengers and baggage. Washington, D.C.: Congressional Research Service. Retrieved August 2, 2009, from <https://www.hsdl.org/RL31151.pdf>
- Napolitano, J. (2010). Remarks by Secretary Napolitano at American Constitution Society National Convention. Washington D.C.: Department of Homeland Security, June 21, 2010. Retrieved January 15, 2011, from [http://www.dhs.gov/ynews/speeches/sp\\_12771582111019](http://www.dhs.gov/ynews/speeches/sp_12771582111019)
- Nie, X., Batta, R., Drury, C. G., & Lin, L. (2009). Passenger grouping with risk levels in an airport security system. *European Journal of Operational Research* 194(2): 574–84.
- Passenger screening Israelis lead world in aviation security at check in and on board. (2001). *Flight International Magazine*. Retrieved March 14, 2011, from <http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/?verb=sr&csi=6953&sr=HLEAD%28passenger+screening+israelis+lead+world+in+aviation+security+at+check+in+and+on+board%29%2BAND%2BDATE%2BIS%2B2001-09-25>
- Persico, N., & Todd, P. E. (2005). Passenger profiling, imperfect screening, and airport security. *American Economic Review* 95(2): 127–31.
- Pickett, S. (2008). *Aviation security: A comparison of the aviation security approaches by the United States and Israel*. Unpublished paper.
- Pistole, J. (2011). Remarks of TSA Administrator, made at the Aviation Security (AVSEC) World Conference, October 4, 2011, Amsterdam, Netherlands. Retrieved October 5, 2011, from [http://www.tsa.gov/press/speeches/100411\\_avsec\\_world.shtm](http://www.tsa.gov/press/speeches/100411_avsec_world.shtm)
- Poole, R. W. (2006). Airport security: Time for a new model. Los Angeles, CA: Reason Public Policy Institute. Retrieved August 8, 2009, from <http://reason.org/files/c7ea6faaa6db365665c4cf3ae661ccdf.pdf>

- Poole, R. W., & Passantino, G. (2003). A risk-based airport security policy. Los Angeles, CA: Reason Public Policy Institute. Retrieved August 8, 2009, from <http://reason.org/files/359408528b992e7d0804df1b590dd424.pdf>
- Power, R. C. (2006). Changing expectations of privacy and the Fourth Amendment. 16 *Widener L.J.* 43–70. Retrieved October 11, 2010, from <http://www.lexisnexis.com.libproxy.nps.edu/lnaucui2api/delivery/printdoc.do?jobhandle>
- Prieto, D. B. (2009). Working paper—War about terror: Civil liberties and national security after 9/11. Washington, D.C.: Council on Foreign Relations. Retrieved August 8, 2009, from [http://www.cfr.org/content/publications/attachments/Civil\\_Liberties\\_WorkingPaper.pdf](http://www.cfr.org/content/publications/attachments/Civil_Liberties_WorkingPaper.pdf)
- Ran, R. (2002). Remarks of Rafi Ran, CEO, New Age Technology, Ltd. before the Aviation Subcommittee, Committee on Transportation and Infrastructure, February 27, 2002, Washington, D.C. Retrieved October 4, 2010, from <http://www.house.gov/transportation/aviation/02-27-02/ran.html>
- Ravid, I. (2004). Safety versus defense: Comments on “CAPPS II: The foundation of aviation security.” *Risk Analysis* 24(4): 929–31.
- Redd, J. S. (2006). National strategy to combat terrorist travel. Washington D.C.: National Counterterrorism Center. Retrieved September 27, 2010, from [http://www.nctc.gov/docs/u\\_terrorist\\_travel\\_book\\_may2\\_2006.pdf](http://www.nctc.gov/docs/u_terrorist_travel_book_may2_2006.pdf)
- Reddick, S. R. (2004). Point: The case for profiling. *International Social Science Review* 79(3&4): 154–56.
- Regan, P. M. (2004). Old issues, new context: Privacy, information collection, and homeland security. *Government Information Quarterly* 21(4): 481–97.
- Rosen, J. (2004). The naked crowd: Balancing privacy and security in an age of terror. 46 *Ariz. L. Rev.* 607.
- Santos, J. S., & Haimes, Y. Y. (2004). Modeling the demand reduction input-output (I-O) inoperability due to terrorism of interconnected infrastructures. *Risk Analysis* 24(6): 1437–51.
- Schildkraut, D. J. (2009). The dynamics of public opinion on ethnic profiling after 9/11. *American Behavioral Scientist* 53(1): 61–79. Retrieved April 20, 2011, from <http://ase.tufts.edu/polsci/faculty/schildkraut/ABSethnicProfiling.pdf>

- Schneidewind, N. F. (2005). Homeland security airport security model. Paper presented at Proceedings of the Workshop on Software Assessment [5<sup>th</sup>] Chicago, Illinois, on November 8, 2005. Retrieved August 7, 2009, from <https://www.hSDL.org/APD022170.pdf>
- Schneier, B. (2007). In praise of security theater. *Schneier on Security*, January 25, 2007. Retrieved August 9, 2010, from [http://www.schneier.com/blog/archives/2007/01/in\\_praise\\_of\\_se.html](http://www.schneier.com/blog/archives/2007/01/in_praise_of_se.html)
- Schwien, F. L., & Jamison, R. D. (2008). DHS risk lexicon. Washington D.C.: Department of Homeland Security. Retrieved February 27, 2011, from [http://www.dhs.gov/xlibrary/assets/dhs\\_risk\\_lexicon.pdf](http://www.dhs.gov/xlibrary/assets/dhs_risk_lexicon.pdf)
- Seifert, J. W. (2004). Data mining and the search for security: Challenges for connecting the dots and databases. *Government Information Quarterly* 21(4): 461–80.
- Simons, M., Brewer, N., & Szul, A. (2009). The Hawley era: Stronger security built on risk management, Intel and workplace improvements. Washington, D.C.: Transportation Security Administration. Retrieved August 9, 2010, from <http://www.tsa.gov/weekly/011209.shtm>
- St. John, P. (1991). *Air piracy, airport security, and international terrorism: Winning the war against hijackers*. Westport, CT: Quorum Books.
- Stone, C. A., & Zissu, A. (2007). Registered travel program: The financial value of registering the good guys. *Review of Policy Research* 24(5): 443–62.
- Trager, R. F., & Zagorcheva, D. P. (2005). Deterring terrorism: It can be done. *International Security* 30(3): 87–123. Retrieved October 2, 2011, from <http://www.jstor.org/stable/4137488>
- Transportation Security Administration. (2011a). What we do: Layers of security. Washington, D.C. Retrieved August 15, 2009, from [http://www.tsa.gov/what\\_we\\_do/layers/index.shtm](http://www.tsa.gov/what_we_do/layers/index.shtm)
- Transportation Security Administration. (2011b). Mission, vision and core values: Who we are. Washington, D.C. Retrieved September 5, 2011, from [http://www.tsa.gov/who\\_we\\_are/mission.shtm](http://www.tsa.gov/who_we_are/mission.shtm)
- Transportation Security Administration. (2011c). Privacy: Advanced imaging technology. Washington, D.C. Retrieved September 5, 2011, from <http://www.tsa.gov/approach/tech/ait/privacy.shtm>

- Transportation Security Administration. (2011d). Crewmember identity verification program to begin testing. Washington, D.C. Retrieved October 3, 2011, from <http://www.tsa.gov/press/releases/2011/0401.shtm>
- Transportation Security Administration. (2011e). Screening pilot for passengers 12 and under. Washington, D.C. Retrieved October 3, 2011, from [http://www.tsa.gov/what\\_we\\_do/screening\\_under12.shtm](http://www.tsa.gov/what_we_do/screening_under12.shtm)
- Transportation Security Administration. (2011f). Make your trip better using 3-1-1. Retrieved January 30, 2011, from <http://www.tsa.gov/311/>
- Transportation Security Administration. (2011g). Transportation security fees: September 11 security fee—passenger fee. Retrieved September 5, 2011, from [http://www.tsa.gov/research/fees/passenger\\_fee.shtm](http://www.tsa.gov/research/fees/passenger_fee.shtm)
- Tucker, J. B. (2003). Strategies for countering terrorism: Lessons from the Israeli experience. Retrieved April 9, 2011, from <http://www.homelandsecurity.org/journal/articles/tucker-israel.html>
- United States Customs and Border Protection. (2009). Global entry program overview. Retrieved August 9, 2009, from [http://www.cbp.gov/xp/cgov/travel/trusted\\_traveler/global\\_entry\\_discription.xml](http://www.cbp.gov/xp/cgov/travel/trusted_traveler/global_entry_discription.xml)
- United States Department of Homeland Security. (n.d.) National infrastructure protection plan risk management framework. Retrieved January 21, 2010, from [http://www.dhs.gov/xlibrary/assets/NIPP\\_RiskMgmt.pdf](http://www.dhs.gov/xlibrary/assets/NIPP_RiskMgmt.pdf)
- United States Department of Homeland Security. (2004). Fact sheet: CAPPS II at a glance. Retrieved January 12, 2011, from <http://www.dhs.gov/dhspublic/display?theme=43&content=3162&print=true>
- United States Department of Homeland Security. (2006). Privacy impact assessment for the global enrollment system. Retrieved October 4, 2010, from <https://www.hsdl.org/?view&doc=65176&coll=limited>
- United States Department of Homeland Security. (2010a). *Risk Steering Committee DHS risk lexicon*. Retrieved March 25, 2011, from <http://www.dhs.gov/xlibrary/assets/dhs-risk-lexicon-2010.pdf>
- United States Department of Homeland Security. (2010b). Global entry program overview. Retrieved October 9, 2010, from [http://www.cpb.gov/xp/cgov/travel/trusted\\_traveler/global\\_entry/global\\_entry\\_discription.xml](http://www.cpb.gov/xp/cgov/travel/trusted_traveler/global_entry/global_entry_discription.xml)

- United States Department of Justice, Civil Rights Division. (2003). Guidance regarding the use of race by federal law enforcement agencies. Retrieved September 17, 2010, from [http://www.justice.gov/crt/split/documents/guidance\\_on\\_race.php](http://www.justice.gov/crt/split/documents/guidance_on_race.php)
- United States Department of Justice, Inspector General. (2005). *Review of the Terrorist Screening Center's efforts to support the Secure Flight Program*. Washington D.C.: Department of Justice Inspector General, Audit Report 05-34. Retrieved August 9, 2009, from <http://www.justice.gov/oig/reports/FBI/a0534/final.pdf>
- U.S. Travel Association. (2010). American traveling public says “there has to be a better way” to conduct air travel security screening. Retrieved September 5, 2011, from <http://www.ustravel.org/news/press-releases/american-traveling-public-says-there-has-be-better-way-conduct-air-travel-secu>
- Viscusi, W. K., & Zeckhauser, R. J. (2003). Sacrificing civil liberties to reduce terrorism risks. *Journal of Risk and Uncertainty* 26(2): 99–120. Retrieved October 10, 2010, from ABI/INFORM Global (Document ID: 410778171).
- Von Rochow-Leuschner, D. (2004). CAPPs II and the Fourth Amendment: Does it fly? *Journal of Air Law and Commerce* 69: 139–73.
- Von Winterfeldt, D., & O'Sullivan, T. M. (2006). Should we protect commercial airplanes against surface-to-air missile attacks by terrorists? *Decision Analysis* 3(2): 63–75. Retrieved March 23, 2011, from <http://www-bcf.usc.edu/~winterfe/should%20we%20protect%20commercial%20airplanes%20against%20surface-to-air%20missile%20attacks%20by%20terrorist>
- Walker, C. (2010). Air security: Rest of the world needs to learn from El Al. *First Post*, January 21, 2010. Retrieved February 27, 2011, from <http://www.thefirstpost.co.uk/58471,news-comment,news-politics,air-security-rest-of-world-needs-to-learn-from-el-al>
- Weiss, M. (2010). Is this the way to make airports safe? *Irish Times*, January 9, 2010. Retrieved March 14, 2011, from <http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lmacademic>
- Wolfe, J. M., Horowitz, T. S., & Kenner, N. M. (2005). Rare items often missed in visual searches. *Nature* 435(May 26, 2005): 439–440.
- Yonkers, S. (2006). Privacy impact assessment for the automated biometric identification system (IDENT). Washington D.C.: Department of Homeland Security. Retrieved August 9, 2009, from [http://www.dhs.gov/xlibrary/assets/privacy/privacy\\_pia\\_usvisit\\_ident\\_final.pdf](http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf)

## **Judicial Opinions**

*Aptheker v. Secretary of State*, 378 U.S. 500 (1964). Retrieved June 16, 2011, from <http://supreme.justia.com/us/378/500/case.html>

*Brandenburg v. Ohio*, 395 U.S. 444 (1969). Retrieved May 25, 2011, from <http://laws.findlaw.com/us/395/444.htm>

*Chandler v. Miller*, 520 U.S. 305 (1997). Retrieved June 5, 2011, from [http://scholar.google.com/scholar\\_case?case=8655257031938182800&q=Chandler+v.+Miller,+520+U.S.+305+%281997%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=8655257031938182800&q=Chandler+v.+Miller,+520+U.S.+305+%281997%29&hl=en&as_sdt=2,21&as_vis=1)

*City of Indianapolis v. Edmond*, 531 U.S. 32 (2000). Retrieved May 29, 2011, from [http://scholar.google.com/scholar\\_case?case=605414745192665577&q=City+of+Indianapolis+v.+Edmond,+531+U.S.+32+%282000%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=605414745192665577&q=City+of+Indianapolis+v.+Edmond,+531+U.S.+32+%282000%29&hl=en&as_sdt=2,21&as_vis=1)

*EPIC v. DHS*, 653 F.3d 1 (D.C. Cir. 2011). Retrieved June 6, 2011, from [http://scholar.google.com/scholar\\_case?case=18146741475039039205&q=EPIC+v.+DHS,+653+F.+3d+1,+22+%28D.C.+Cir.+2011%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=18146741475039039205&q=EPIC+v.+DHS,+653+F.+3d+1,+22+%28D.C.+Cir.+2011%29&hl=en&as_sdt=2,21&as_vis=1)

*Farag v. United States*, 587 F. Supp. 2d 436 (E.D.N.Y. 2008). Retrieved June 26, 2011, from [http://scholar.google.com/scholar\\_case?case=11791946086632507518&q=Farag+v.+United+States+587+F.Supp.+2d+436+&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=11791946086632507518&q=Farag+v.+United+States+587+F.Supp.+2d+436+&hl=en&as_sdt=2,21&as_vis=1)

*Gilmore v. Gonzales*, 435 F.3d 1125 (9th Cir. 2006). Retrieved January 15, 2011, from [http://scholar.google.com/schola\\_case?case=9398795300479678488&q=CAPPS+II&hl=en&as\\_sdt=2,14](http://scholar.google.com/schola_case?case=9398795300479678488&q=CAPPS+II&hl=en&as_sdt=2,14)

*Haig v. Agee*, 453 U.S. 280 (1981). Retrieved June 9, 2011, from <http://laws.findlwa.com/us/453/280.htm>

*Miranda v. Arizona*, 384 U.S. 436 (1966). Retrieved August 8, 2011, from <http://caselaw.lp.findlaw.com/cgi-bin/getcase.pl?court=us&vol=384&invol=436>

*Riley v. Nat'l Fed. of the Blind of North Carolina*, 487 U.S. 781 (1988). Retrieved May 29, 2011, from <http://supreme.justia.com/us/487/781/>

*Schenk v. United States*, 249 U.S. 47 (1919). Retrieved June 11, 2011, from [http://scholar.google.com/scholar\\_case?case=8474153321909160293&q=schenck+v.+united+states+249+u.s.+47+1919&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=8474153321909160293&q=schenck+v.+united+states+249+u.s.+47+1919&hl=en&as_sdt=2,21&as_vis=1)

*Simon & Schuster v. New York State Crime Victims Bd.*, 502 U.S. 105 (1991). Retrieved June 26, 2011, from <http://findlaw.com/us/502/105.htm>

*Tabbaa v. Chertoff*, 509 F.3d 89 (2d Cir. 2007). Retrieved June 10, 2011, from [http://scholar.google.com/scholar\\_case?case=4064074276537644228&q=Tabbaa+v.+Chertoff,+509+F.3d+89+%282d+Cir.+2007%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=4064074276537644228&q=Tabbaa+v.+Chertoff,+509+F.3d+89+%282d+Cir.+2007%29&hl=en&as_sdt=2,21&as_vis=1)

*United States v. Albarado* 495 F.2d 799 (2d Cir. 1974). Retrieved June 5, 2011, from [http://scholar.google.com/scholar\\_case?case=13048931699413913464&q=United+States+v.+Albarado+%28495+F.2d+799+%282d+Cir.+1974%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=13048931699413913464&q=United+States+v.+Albarado+%28495+F.2d+799+%282d+Cir.+1974%29&hl=en&as_sdt=2,21&as_vis=1)

*United States v. Aukai*, 440 F.3d 1168 (9th Cir. 2006). Retrieved June 5, 2011, from <http://www.ca9.uscourts.gov/datastore/opinions/2007/08/10/0410226.htm>

*United States v. Aukai*, 497 F.3d 955 (9th Cir. 2007). Retrieved on June 5, 2011, from <http://caselaw.findlaw.com/us-9th-circuit/1265662.html>

*United States v. Bautista*, 684 F.2d 1286 (9th Cir. 1982). Retrived July 5, 2011, from <http://law.justia.com/cases/federal/appellate-courts/F2/684/1286/40668/>

*United State v. Biswell*, 406 U.S. 311 (1972). Retrieved June 26, 2011, from <http://supreme.justia.com/us/406/311/>

*United States v. Brignoni-Ponce*, 422 U.S. 873 (1975). Retrieved July 5, 2011 from <http://supreme.justia.com/us/422/873/>

*United States v. Davis*, 482 F.2d 893 (9th Cir. 1973). Retrieved June 6, 2011, from <http://ftp.resource.org/courts.gov/c/F2/482/482.F2d.893.71-2993.html>

*United States v. Hartwell*, 296 F. Supp. 2d 596 (E.D. Pa. 2003). Retrieved June 26, 2011, from [http://www.leagle.com/xmlResult.aspx?xmlDoc=2003892296FSupp2d596\\_1830.xml&docbase=CSLWAR2-1986-2006](http://www.leagle.com/xmlResult.aspx?xmlDoc=2003892296FSupp2d596_1830.xml&docbase=CSLWAR2-1986-2006)

*United States v. Hartwell*, 436 F.3d 174 (3d Cir. 2006). Retrieved on June 1, 2011, from <http://law.justia.com/cases/federal/appellate-courts/F3/436/174/593682/>

*United States v. Ramos*, 629 F.3d 60 (1st Cir. 2010). Retrieved June 26, 2011, from <http://www.leagle.com/xmlResult.aspx?xmlDoc=In+FCO+20101217073.xml&docbase=CSLWAR3-2007-CURR>

*United States v. Silva*, 715 F.2d 43 (2d Cir. 1983). Retrieved June 26, 2011, from [http://scholar.google.com/scholar\\_case?case=16044434227898686999&q=United+States+v.+Silva,+715+F.+2d+43+%282d+Cir.+1983%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=16044434227898686999&q=United+States+v.+Silva,+715+F.+2d+43+%282d+Cir.+1983%29&hl=en&as_sdt=2,21&as_vis=1)

*United States v. Skipwith*, 482 F.2d 1271 (5th Cir.1973), Retrieved June 10, 2011, from <http://openjurist.org/482/f2d/1272/united-states-v-skipwith-iii>

*United States v. St. Vallier*, 404 Fed. Appx. 651 (3d Cir. 2010). Retrieved July 5, 2011, from <http://www.lexisnexis.com.libproxy.nps.edu/hottopics/lnacademic/>

*United States v. Weaver*, 966 F.2d 392 (8th Cir. 1992). Retrieved July 5, 2011, from [http://www.soc.umn.edu/~samaha/cases/us\\_v\\_weaver.htm](http://www.soc.umn.edu/~samaha/cases/us_v_weaver.htm)

*Whren v. United States*, 517 U.S. 806 (1996). Retrieved July 5, 2011, from [http://scholar.google.com/scholar\\_case?case=3416424011044753637&q=Whren+v.+United+States,+517+U.S.+806+%281996%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=3416424011044753637&q=Whren+v.+United+States,+517+U.S.+806+%281996%29&hl=en&as_sdt=2,21&as_vis=1)

*Wooley v. Maynard*, 430 U.S. 705 (1977). Retrieved June 26, 2011, from [http://scholar.google.com/scholar\\_case?case=15210508422263730617&q=Wooley+v.+Maynard,+430+U.S.+705+%281977%29&hl=en&as\\_sdt=2,21&as\\_vis=1](http://scholar.google.com/scholar_case?case=15210508422263730617&q=Wooley+v.+Maynard,+430+U.S.+705+%281977%29&hl=en&as_sdt=2,21&as_vis=1)

## INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center  
Ft. Belvoir, Virginia
2. Dudley Knox Library  
Naval Postgraduate School  
Monterey, California
3. John Pistole  
Transportation Security Administration  
Arlington, Virginia
4. Chris McLaughlin  
Transportation Security Administration  
Arlington, Virginia
5. Francine Kerner  
Transportation Security Administration  
Arlington, Virginia
6. Elise Crawford  
Transportation Security Administration  
Rosemont, Illinois
7. Kathleen Petrowsky  
Transportation Security Administration  
Rosemont, Illinois
8. Stephanie Blum  
Transportation Security Administration  
Detroit, Michigan