View metadata, citation and similar papers at core.ac.uk

brought to you by CORE

provided by Calhoun, Institutional Archive of the Naval Postgraduate School

Calhoun: The NPS Institutional Archive

Theses and Dissertations | Thesis Collection

2008-09

Public -- private sector passenger rail Intelligence and terrorism information sharing

Crosbie, William L.

Monterey, California. Naval Postgraduate School

http://hdl.handle.net/10945/3695

http://www.nps.edu/library

Calhoun is a project of the Dudley Knox Library at NPS, furthering the precepts and goals of open government and government transparency. All information contained herein has been approved for release by the NPS Public Affairs Officer.

Dudley Knox Library / Naval Postgraduate School
411 Dyer Road / 1 University Circle
Monterey, California USA 93943

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

PUBLIC – PRIVATE SECTOR PASSENGER RAIL INTELLIGENCE AND TERRORISM INFORMATION SHARING

by

William L. Crosbie

September 2008

Thesis Advisor: Robert Simeral
Second Reader: John McCreary

~~**Distribution authorized to U.S. Government Agencies only. Releasable to state and local government agencies. (Administrative or Operational Use); (September 2008). Other requests for this document shall be referred to President, Code 261, Naval Postgraduate School. Monterey, CA 93940-5000, via the Defense Technical Information Center, 8725 John J. Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218.**~~

~~**This thesis is For Official Use Only; upon removal of Appendices A and C, this thesis is Unclassified.**~~
Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

December 17, 2009

SUBJECT: Sanitized version of *Public – Private Passenger Rail Intelligence and Terrorism Information Sharing* – September 2008.

1. Reference: Crosbie, William L. *Public – Private Passenger Rail Intelligence and Terrorism Information Sharing*. Monterey, CA: Naval Postgraduate School, September 2008. UNCLASSIFIED, [Distribution authorized to U.S. Government Agencies only. Releasable to state and local government agencies. (Administrative or Operational Use); (September 2008). This thesis is For Official Use Only; upon removal of Appendices A and C, this thesis is Unclassified].

2. Upon consultation with NPS faculty, the School has determined that this sanitized version of the thesis (portions of page viii and pages 91 – 164 redacted) may be released to the public, and that its distribution is unlimited, effective December 14, 2009.

University Librarian
Naval Postgraduate School

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington D.C. 20503.			
1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** September 2008	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE: Public – Private Sector Passenger Rail Intelligence and Terrorism Information Sharing			**5. FUNDING NUMBERS**
6. AUTHOR(S) William L. Crosbie			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT ~~Distribution authorized to U.S. Government Agencies only. Releasable to state and local government agencies. (Administrative or Operational Use); (September 2008). Other requests for this document shall be referred to President, Code 261, Naval Postgraduate School. Monterey, CA 93940-5000, via the Defense Technical Information Center, 8725 John J. Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218.~~ **Approved for public release; distribution is unlimited**			**12b. DISTRIBUTION CODE** ~~B~~ A

13. ABSTRACT *(maximum 200 words)*

What is an effective methodology for intelligence and terrorism information sharing within a private passenger rail organization and with their external public partners? This thesis uses three distinct research methodologies that collectively lead to an effective strategy for intelligence and terrorism information sharing within a private passenger railroad, and with its external public partners (Chapter III):

1. Key Amtrak personnel will be interviewed to establish and confirm how intelligence information currently flows within Amtrak and with its external intelligence community and law enforcement partners (Chapter II).
2. A survey of key Amtrak operations personnel to establish Amtrak's intelligence priorities and requirements (Chapter IV).
3. Two case studies on potential models for intelligence and terrorism information sharing (Chapters V and VI).

There were two outcomes from this research: (1) by leveraging the power of informal networks in the context of the abstract megacommunity framework, an effective strategy for intelligence and terrorism information sharing was developed; and (2) based on the needs of front line railroad operating personnel, an intelligence product that helps to protect the public and the nation's critical railroad infrastructure was developed.

14. SUBJECT TERMS Passenger Rail; Private Sector; Intelligence; Intelligence Sharing; Sources; Patterns; Nodes; Nature; Pathways; Decision Makers; Psychology; Networks; Network Analysis; Social Network Analysis; Organizational Network Analysis; Strategy; Megacommunities; Informal Networks; Requirements; Priorities; Multi-Discipline; Dissemination; NYPD SHIELD; British Transport Police; Culture; Multiculturalism; Governance; Collaborative Partnerships; Foreign Intelligence; Liaison	**15. NUMBER OF PAGES** 189
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	~~UL~~ UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

~~**Distribution authorized to U.S. Government Agencies only. Releasable to state and local government agencies. (Administrative or Operational Use); (September 2008). Other requests for this document shall be referred to President, Code 261, Naval Postgraduate School. Monterey, CA 93940-5000, via the Defense Technical Information Center, 8725 John J. Kingman Road, Suite 0944, Ft. Belvoir, VA 22060-6218.**~~

Approved for public release; distribution is unlimited

PUBLIC – PRIVATE SECTOR PASSENGER RAIL INTELLIGENCE AND TERRORISM INFORMATION SHARING

William L. Crosbie
Chief Operating Officer, Amtrak
Honors B.S., Queens University, 1988

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
September 2008**

Author: William L. Crosbie

Approved by: CAPT Robert Simeral
Thesis Advisor

John McCreary, ESQ
Second Reader

Harold A. Trinkunas, Ph.D.
Chairman, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

What is an effective methodology for intelligence and terrorism information sharing within a private passenger rail organization and with their external public partners? This thesis uses three distinct research methodologies that collectively lead to an effective strategy for intelligence and terrorism information sharing within a private passenger railroad, and with its external public partners (Chapter III):

1. Key Amtrak personnel will be interviewed to establish and confirm how intelligence information currently flows within Amtrak and with its external intelligence community and law enforcement partners (Chapter II).
2. A survey of key Amtrak operations personnel to establish Amtrak's intelligence priorities and requirements (Chapter IV).
3. Two case studies on potential models for intelligence and terrorism information sharing (Chapters V and VI).

There were two outcomes from this research: (1) by leveraging the power of informal networks in the context of the abstract megacommunity framework, an effective strategy for intelligence and terrorism information sharing was developed; and (2) based on the needs of front line railroad operating personnel, an intelligence product that helps to protect the public and the nation's critical railroad infrastructure was developed.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. THE WALL....1
B. PASSENGER RAIL AND INTELLIGENCE SHARING....3
C. RESEARCH QUESTION....5
D. SIGNIFICANCE OF RESEARCH....6
E. LITERATURE REVIEW....6
1. Federal Documents....7
a. Summary of Federal Documents....15
2. Private Sector Practices....16
3. Academic Studies....17
4. Summary of Literature Review....17
F. METHOD....18

II. INTELLIGENCE AND TERRORISM INFORMATION SHARING WITH AND WITHIN AMTRAK TODAY....21
A. THE EXISTING MEANS AND METHODS....21
1. Sources of Intelligence for Amtrak....21
2. Pattern and Nodes of Interaction....22
3. Nature of the Information....22
4. Pathways for Intelligence....23
5. Decision Making Nodes....24
B. SUMMARY....25

III. INTELLIGENCE AND TERRORISM INFORMATION SHARING STRATEGY....27
A. PSYCHOLOGY OF INFORMATION SHARING....28
B. NETWORK ANALYSIS....31
1. Social Network Analysis....31
2. Organizational Network Analysis....32
C. INTELLIGENCE SHARING STRATEGY CANVAS....33
D. A STRATEGY FOR PUBLIC – PRIVATE SECTOR PASSENGER RAIL....36
E. MEGACOMMUNITIES AND INTELLIGENCE SHARING NETWORKS....38
F. SUMMARY....42

IV. DEFINING AMTRAK'S INTELLIGENCE REQUIREMENTS....45
A. THE GLOBAL THREAT TO PASSENGER RAIL....45
B. AMTRAK'S INTELLIGENCE REQUIREMENTS....45
1. Priorities and the Type of Information....46
2. Multi-Discipline Dissemination....48
C. SUMMARY....51

V. NYPD SHIELD CASE STUDY....53

A. OVERVIEW OF NYPD SHIELD 53
1. Sector Specific Briefings and Conferences 54
2. Training 55
3. Website 56
4. Intelligence and Analysis Briefings 57
5. Resource Library 57
6. SHIELD Alerts 57
B. NYPD PERSPECTIVE 58
1. Protecting the City 58
2. Protecting the City through Intelligence Information 58
C. NYPD SHIELD VS. AMTRAK REQUIREMENTS 60
D. THE NYPD SHIELD MEGACOMMUNITY 65
E. SUMMARY 67

VI. BRITISH TRANSPORT POLICE MODEL 69
A. BTP COUNTERTERRORISM UNIT BRIEFING REPORT VS. AMTRAK REQUIREMENTS 69
B. THE BRITISH TRANSPORT POLICE COUNTERTERRORISM UNIT BRIEFING: A POTENTIAL SOLUTION? 73
1. The Threat of Terrorism in the United Kingdom 74
2. Culture and Multiculturalism 75
3. Governance 79
4. Agency Authority & Laws 80
C. COMPARATIVE ANALYSIS CONCLUSIONS & JUSTIFICATION 83
D. SUMMARY 83

VII. IMPLEMENTING THE STRATEGY 85
A. AMTRAK'S INTELLIGENCE & TERRORISM INFORMATION UNIT 85
1. Meeting Amtrak's Intelligence Requirements 86
2. Liaison with National Level Intelligence Community 87
3. Collaborative Partnerships with Fusion Centers and Local Law Enforcement 88
4. Collaborate with Foreign Intelligence and Law Enforcement Agencies 88
5. Security Clearance Management 89
B. DELIVERABLES 89
C. SUMMARY 90
D. FINAL THOUGHTS 90

APPENDIX A. [redacted]

APPENDIX B. [redacted]

APPENDIX C. [redacted]

APPENDIX D. [redacted]

LIST OF REFERENCES **167**
INITIAL DISTRIBUTION LIST **173**

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1. Amtrak's current means and methods of acquiring intelligence. 25
Figure 2. Network Topologies.....31
Figure 3. Intelligence and terrorism information sharing strategy canvas. 34
Figure 4. A new intelligence sharing network for public – private passenger rail.....37
Figure 5. Passenger rail intelligence sharing megacommunity. 38
Figure 6. The strength of weak ties in Amtrak's intelligence sharing model. 41
Figure 7. An intelligence-led policing and crime reduction process. 48
Figure 8. NYPD Internet home page – April 14, 2008. 54
Figure 9. The NYPD SHIELD megacommunity. 64
Figure 10. Christian and Muslim population distribution in Great Britain. 76
Figure 11. BTP reporting structure.....79

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. Four actions that will improve intelligence and terrorism information sharing. 35
Table 2. Amtrak Intelligence Priorities and Requirements. 46
Table 3. NYPD SHIELD Reports vs. Amtrak Intelligence Priorities and Requirements. 62
Table 4. BTP CTU Briefing Report vs. Amtrak Intelligence Priorities and Requirements. 70

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

There is no other profession that is held to the standards that intelligence and terrorism information practitioners are required to meet. They are expected to foresee and piece together entire plots from mere threads of information. Unanticipated threats and successful terrorist attacks are intelligence failures in the eyes of Congress and the public. For their persistent service in the face of the impossible, I acknowledge and thank them for the lives they have saved. I hope this thesis helps them achieve their goal – denying the terrorists' goal.

The completion of this thesis and Master's program would not have been possible without the support and guidance of so many people. I would like to acknowledge the Naval Postgraduate School and the Center for Homeland Defense and Security faculty and staff for creating a great learning environment, and bring together such an experienced and intellectually diverse group of students; my classmates for contributing so much to the educational content and value of this program; and Amtrak for seeing the importance of this program and supporting my attendance. I would especially like to acknowledge my advisor, CAPT Robert Simeral, for his wise and timely guidance; and my reader, John McCreary ESQ, for his succinct comments and forthright observations. The end product would have suffered the lesser without your respective contributions. To all I owe a debt of gratitude.

The study of terrorism and international affairs has been a life long dream and passion for me. Be it chasing dreams or the call of duty in the middle of the night, so many lives, in so many immeasurable ways, are impacted. For those of us that choose to serve the public, our family members are the silent unrecognized heroines and heroes. Unconditionally, they allow us to carry our small portion of the weight of freedom. My family is no exception. Thank you … so much.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. THE WALL

With over 80% of America's critical infrastructure owned and operated by the private sector,[1] the strategic value of a public – private partnership is paramount in the fight against terrorism. The recent release of information sharing strategies by the Department of Homeland Security (DHS)[2] and the Office of the Director of National Intelligence (ODNI)[3] is an attempt by the federal government to build this partnership. Both these strategies, however, fall well short of meeting the requirements of the private sector. Within the United States (U.S.), intelligence and terrorism information sharing between the public and private sector is problematic, and remains a significant challenge for both parties. Intelligence and terrorism information is a critical enabler in the risk mitigation decision making process. The strategic deployment of assets and investment of limited capital funds is dependent on actionable intelligence.

The root of this problem was first identified by the Senate Select Committee on Intelligence in response to the controversy surrounding the illegal activities of the Banca Nazionale del Lavoro (BNL) and the Bank of Credit and Commercial International (BCCI) during the early 1990s. The Committee concluded that:

> The fundamental policy governing the relationship between law enforcement and intelligence needs to be addressed by the Attorney General and the DCI, in conjunction with the congressional oversight committees. Confusion is apparent on both sides as to what the proper role (and authority) of intelligence agencies is in circumstances like those

[1] President George W. Bush, *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (Washington, D.C.: The White House 2003), 8.

[2] Department of Homeland Security, *Information Sharing Strategy* (Washington, D.C.: Department of Homeland Security, 2008), http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf (accessed June 8, 2008).

[3] Office of the Director of National Intelligence, *U.S. Intelligence Community Intelligence Sharing Strategy* (Washington, D.C.: Office of the Director of National Intelligence, 2008), http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf (accessed June 8, 2008).

> presented in the BNL case. Indeed, as the conclusions set forth below indicate, there are numerous and significant "disconnects" between the two functional areas.[4]

After the 1993 World Trade Center bombing, Congress began to seek legislative changes that could facilitate information sharing between the intelligence community and law enforcement. The Bremer Commission[5] was established to review counterterrorism laws, regulations, directives, policies, and practices. In a June 2000 report to Congress, the Commission concluded:

> Law enforcement agencies are traditionally reluctant to share information outside of their circles so as not to jeopardize any potential prosecution. The FBI does promptly share information warning about specific terrorist threats with the CIA and other agencies. But the FBI is far less likely to disseminate terrorist information that may not relate to an immediate threat even though this could be of immense long-term or cumulative value to the intelligence community. . . . Moreover, certain laws limit the sharing of law enforcement information, such as grand jury or criminal wiretap information, with the intelligence community. These laws are subject to different interpretations, so that in some cases it is unclear whether the restrictions apply.[6]

Despite recognizing the wall between the intelligence community and law enforcement, the White House and Congress rejected legislative proposals to remove the barrier through broader surveillance and information sharing powers. Attorney General William Barr testified before the 9/11 Commission stating that:

> For three decades leading up to 9/11, Congress was at the fore of a steady campaign to curtail the Bureau's domestic intelligence activities and impose on all its activities the standards and process of the criminal justice system. These concerns made it extremely difficult for the Bureau to pursue domestic security matters outside the strictures of the criminal

---

[4] Senate Select Committee on Intelligence, *The Intelligence Community's Involvement in the Banca Nazionale del Lavoro (BNL) Affair* (Washington, D.C.: U.S. Congress, 103rd Congress, 1st session, February 1993), 35 - 36.

[5] The Bremer Commission's official title was the National Commission on Terrorism. It was headed by former Ambassador L. Paul Bremer.

[6] National Commission on Terrorism, Countering the Changing Threat of International Terrorism (Washington, D.C.: Government Printing Office, June 2000), 15-16.

> justice process. Prohibitions on sharing grand jury information with intelligence agencies and with using intelligence information in criminal investigations created a 'wall of separation.'[7]

In the aftermath of the September 11, 2001 terrorist attacks, all branches of the U.S. government agreed that information must be shared between the intelligence community and law enforcement. As a result of prior recognition of the problem and proposed legislative solutions, within one week of the attacks, a comprehensive bill was before Congress that would ultimately become the USA PATRIOT Act ("*The Patriot Act*"). *The Patriot Act* provides for significant relief from the restrictions on intelligence gathering within the U.S., and the sharing of information acquired during criminal investigations. Some of the more relevant sections of this complex law are as follows:

- Section 203: Authority to Share Criminal Investigative Information
- Section 504: Coordination with Law Enforcement
- Section 905: Disclosure to Director of Central Intelligence of Foreign Intelligence-Related Information with Respect to Criminal Investigations.[8]

Despite the authority and directive to share intelligence information, the intelligence community and law enforcement continue to struggle with its application. This has transcended all levels of government (federal, state, local, and tribal), and the private sector. Intelligence and terrorism information sharing between the public and private sector is no exception.

B. PASSENGER RAIL AND INTELLIGENCE SHARING

The National Railroad Passenger Corporation ("Amtrak") is a private corporation incorporated in the District of Columbia. The Directors on the Amtrak Board are appointed by the President and confirmed by the Senate with the exception of the Secretary of Transportation who holds a permanent Directors position. Although legally a private corporation, Amtrak is effectively a federal agency controlled by the federal

[7] William P. Barr, "Statement of William P. Barr to the National Commission on Terrorist Attacks Upon the United States," *National Commission on Terrorist Attacks Upon the United States*, http://govinfo.library.unt.edu/911/hearings/hearing6/witness_barr.htm (accessed February 29, 2008).

[8] For a detailed analysis of the entire law, please refer to Congressional Research Service (CRS) Report RL31377, *The USA PATRIOT Act: A Legal Analysis* dated April 15, 2002 by Charles Doyle.

government. It services 525 stations, in 46 states, with 305 trains operating daily in a 22,000 mile rail network. Millions of Americans rely on Amtrak to transport them safely to and from work each day. The operating personnel and infrastructure that makes this possible is a critical national asset.[9] Protection of the traveling public and this critical national asset is vital to the survival of the U.S. economy and the corporation.

The value proposition for passenger rail, in comparison to other modes, is easy access to affordable, frequent, high capacity transportation. However, this ease of access is what terrorists have exploited to perform attacks on passenger trains in Madrid, London, and Mumbai. The DHS Office of Intelligence and Analysis - Homeland Infrastructure Threat & Risk Analysis Center warns that the "U.S. commercial passenger and freight rail systems are vulnerable to terrorist attack because of their public accessibility and the difficulty in securing a vast array of railroad assets. Passenger trains and stations are especially attractive terrorist targets because of the large number of people in a concentrated area."[10]

In an attempt to mitigate this threat, passenger rail agencies have altered the focus of their police and security from traditional crime to counterterrorism tactics. They have conducted security needs assessments[11] on their infrastructure and invested in security systems to lower the risk of an attack. They have provided security training to their employees and introduced programs such as "See Something, Say Something."[12] These initiatives have resulted in a significant amount of information being collected that is not

[9] Government Accountability Office, *Passenger Rail Security – Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts* (Washington, D.C.: GAO, 2005), 1.

[10] Department of Homeland Security Office of Intelligence and Analysis, *Strategic Sector Assessment – The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System* (Washington, D.C.: Department of Homeland Security, 2006), 3.

[11] A security needs assessment includes an assessment of assets (criticality, threat, vulnerability, impact, and risk), response and recovery capabilities, and countermeasures.

[12] Metropolitan Transit Authority, "If You See Something, Say Something," http://www.mta.info/mta/security/index.html (accessed December 25, 2007).

based on any guidelines, objectives, or priorities. The information is simply reported to the TSA Transportation Security Coordination Center (TSCC) in compliance with TSA Security Directive RAILPAX-04-02.[13]

According to its own legislative guidelines, DHS is responsible for the collection, processing, analysis, and dissemination of intelligence reports that assist with the deterrence, prevention, preemption of, or response to terrorist attacks against the U.S.[14] Due to the lack of intelligence sharing, the status of information collected about terrorist attacks against passenger rail is not known. What is known is the processing and analysis of information collected to help deter, prevent, preempt, or respond to a terrorist attack against passenger rail is non-existent. Routine intelligence reports specific to the passenger rail sector are required to deploy the limited resources of each passenger rail agency effectively including the deployment of state and local resources.

As a result, critical infrastructure protection is inadequate because the critical enabler is missing. Authorities in the rail system, for example, only have the word of DHS that they are at risk, and are ignorant as to the basis for the continued threat assertions. They cannot gauge the gravity of the threat, and thus, are in the dark as to how and how much to respond and where to put the emphasis. This is a critical vulnerability that shows no indications of improvement anytime soon.

C. RESEARCH QUESTION

What is an effective methodology for intelligence and terrorism information sharing within a private passenger rail organization and with their external public partners?

The current intelligence reports and assessments from the DHS and the TSA provide broad threat information largely based on terrorist attacks that have occurred in other parts of the world. Knowledge of a general threat is helpful in raising the overall

---

[13] Transportation Security Administration, *Threat to Passenger Rail Systems – National Railroad Passenger Corporation (AMTRAK) and Alaska Railroad Corporation – SD RAILPAX-04-02* (Washington, D.C.: Department of Homeland Security, 2004).

[14] 107th United States Congress, *Homeland Security Act of 2002* (Washington, D.C.: United States Congress, November 25, 2002), Sec. 201 (d).

level of awareness and vigilance, but over time, it becomes the accepted norm. The threat of a terrorist attack on passenger rail becomes a backdrop similar to the threat of common crime in our society.

D. SIGNIFICANCE OF RESEARCH

This research will be the first to identify the key factors and components of an effective intelligence and terrorism information sharing methodology between the public and private sector. It could form the basis for a doctoral study of the most effective methodology for the collection, processing, analysis, and dissemination of intelligence information. On its own, as a minimum, it will provide the basis for an intelligence sharing program between Amtrak and other private sector passenger rail entities responsible for public safety and critical infrastructure protection, and their public sector partners. For Homeland Security practitioners and policy makers, it will provide a valuable reference as they contemplate, develop, and implement related Homeland Security policies, strategies, and regulations. It will determine what intelligence information works and what does not work, and why, on the frontlines of transportation public safety and critical infrastructure protection.

E. LITERATURE REVIEW

The literature review that follows will show that no meaningful legislation, policies, strategies, industry practices, or academic research has been put forth on public – private sector intelligence and terrorism information sharing. This is conclusively true when it comes to intelligence sharing with the passenger rail transportation sector. What it will show is that the existing literature only patronizes public – private sector intelligence sharing. This thesis will contribute new research to an area where none exists today.

Literature on intelligence and terrorism information sharing between the public and the private sectors can be separated into three distinct areas: (1) federal documents; (2) documentation of private sector practices; and (3) academic studies.

A literature review of intelligence and terrorism information sharing between the public and the private sectors reveals that the federal government has created a substantial body of work. Upon analyzing the information, however, it is apparent that the problems are well defined, but the proposed solutions lack substance, and are based on very little collaboration with the private sector and civil society.[15] Within the private sector, documented practices of intelligence and terrorism information sharing are not openly available to the public because of the need to protect corporate and national secrets. Academia's focus has largely been on intelligence and terrorism information sharing between the various levels of government. There also appears to be no academic studies specific to information sharing between the public and private sectors.

1. Federal Documents

The need for intelligence and terrorism information sharing with the private sector was first recognized in Presidential Decision Directive 63 (PDD-63) – Critical Infrastructure Protection issued by President Clinton on May 22, 1998. As one of the first legal documents to acknowledge the problem, it attempted to prescribe a solution by creating the National Infrastructure Protection Center (NIPC) and encouraging the creation of the Information Sharing and Analysis Center (ISAC):

> Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector.[16]

PDD-63 recommended the ISACs be designed by the private sector, but emulate the Centers for Disease Control and Prevention since it has "proved highly effective, particularly it[s] extensive interchanges with the private and non-federal sectors."[17] This

[15] Mark Gerencser et al., *Megacommunities* (New York, NY: Palgrave MacMillan, 2008), 56.

[16] President Clinton, *Presidential Decision Directive 63 – Critical Infrastructure Protection* (Washington, D.C.: The White House, 1998), 13.

[17] Ibid.

essentially left the design and function to the sectors that formed them. It is important to understand the ISAC concept and its history because it sets the government framework for information sharing with the private sector that still exists today.

The Homeland Security Act of 2002 established DHS and created the Information Analysis and Infrastructure Protection (IAIP) directorate. All critical infrastructure protection (CIP) functions, personnel, assets, and liabilities within existing organizations, including the NICP, were transferred to IAIP. The act also made the IAIP responsible for collecting, analyzing, and disseminating information to federal, state, and local governments, and the private sector. These responsibilities were subsequently assigned to the Under Secretary for Intelligence and Analysis pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007.[18] Neither act prescribed a means of accomplishing these responsibilities.

The National Strategy for the Physical Protection of Critical Infrastructure and Key Assets issued by DHS in February 2003 established five key objectives related to information sharing:

- Define protection-related information sharing requirements and establish effective, efficient information sharing processes;
- Implement the statutory authorities and powers of the *Homeland Security Act of 2002* to protect security and proprietary information regarded as sensitive by the private sector;
- Promote the development and operation of critical sector Information Sharing Analysis Centers;
- Improve processes for domestic threat data collection, analysis, and dissemination to state and local government and private industry;
- Support the development of interoperable secure communications systems for state and local governments and designated private sector entities; and
- Complete implementation of the Homeland Security Advisory System.[19]

[18] 110th United States Congress, *Implementing Recommendations of the 9/11 Commission Act of 2007* (Washington, D.C.: United States Congress, August 3, 2007), Sec. 531 (a) (2).

[19] President George W. Bush, *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets* (Washington, D.C.: The White House 2003), xi.

This DHS document acknowledges for the first time that there may be barriers to information sharing between the public and private sectors. It suggests that these impediments and disincentives be identified and appropriate measures be adopted to overcome these barriers. It does not suggest what the obstacles are or the appropriate measures to overcome them. The strategy also re-introduces the concept of ISACs by including the promotion of the development and operation of these entities.

The problem of information sharing with the private sector is further recognized in Homeland Security Presidential Directive 7 (HSPD-7) – Directive on Critical Infrastructure Identification, Prioritization, and Protection issued by President George W. Bush on December 17, 2003. HSPD-7 encouraged DHS to collaborate with private sector entities to improve information sharing and analysis. However, it did not mention the ISACs or suggest solutions to overcoming the information sharing barriers with the private sector. The objectives are set out in clause 25 of HSPD-7:

> (25) In accordance with applicable laws or regulations, the Department and the Sector-Specific Agencies will collaborate with appropriate private sector entities and continue to encourage the development of information sharing and analysis mechanisms. Additionally, the Department and Sector-Specific Agencies shall collaborate with the private sector and continue to support sector-coordinating mechanisms:
>
> (a) to identify, prioritize, and coordinate the protection of critical infrastructure and key resources; and
>
> (b) to facilitate sharing of information about physical and cyber threats, vulnerabilities, incidents, potential protective measures, and best practices.[20]

These broad objectives did not define success through any measurable goals or a time frame for completion.

The literature, post HSPD-7, focuses on attempting to change the behavior of either the federal government or private sector depending on the author of the document. The Homeland Security Advisory Council (HSAC) and the National Infrastructure

[20] President George W. Bush, *Homeland Security Presidential Directive 7 - Directive on Critical Infrastructure Identification, Prioritization, and Protection* (Washington, D.C.: The White House, 2003).

Advisory Council (NIAC) issued at least six reports on the subject in the year-and-a-half period between January 2004 and July 2006.[21] For the most part, these reports further define the problem and suggest that collaboration, at all levels of government and with the private sector, is the solution. However, they provide no details on how to accomplish this broad objective.

Two of these studies and the subsequent reports focus on the issue of information sharing with the private sector. The first is the August 10, 2005 report on Homeland Security Information Sharing between Government and the Private Sector. It documents many of the barriers referred to by the President in the National Strategy for the Physical Protection of Critical Infrastructure and Key Assets. However, it offers few solutions to overcome the barriers. It could also be perceived as a response to the audits and reports issued by the Government Accountability Office (GAO) in 2004. The second report, Public-Private Sector Intelligence Coordination dated July 11, 2006, confirms the earlier findings and offers eight specific recommendations developed by industry subject matter experts from federal, state, and local government entities, and the private sector. This report also includes four case studies that analyze the time, quality, quantity, and impact of information flow to and from the private sector. This may be the only analysis that attempts to quantify the problem.

The GAO issued two reports in 2004 on how well DHS is sharing information with the private sector. The GAO reports provide an independent or neutral review of the issue. However, one must remember their mandate is to report and make recommendations to Congress on government agency inefficiencies, non-compliance, and effectiveness, not evaluate private sector performance. The first report, entitled Critical

[21] The reports issued by the HSAC and its predecessor organization the National Infrastructure Advisory Council (NIAC) include:

- *Evaluation and Enhancement of Information Sharing and Analysis*, NIAC, July 13, 2004.
- *Intelligence and Information Sharing Initiative Final Report and Recommendations*, December 200.
- *Homeland Security Intelligence and Information Fusion*, April 28, 2005.
- *Homeland Security Information Sharing between Government and the Private Sector Final Report*, August 10, 2005.
- *Lessons Learned Information Sharing Initiative: Homeland Security Intelligence Requirements Process*, December 2005.
- *Public-Private Sector Intelligence Coordination, NIAC*, July 11, 2006.

Infrastructure Protection - Establishing Effective Information Sharing with Infrastructure Sectors dated April 21, 2004, focused on the status of the private sector ISACs. It reported that:

- the current ISACs were established and developed based on the unique characteristics and needs of their individual sectors;
- DHS and the sector-specific agencies have undertaken a number of efforts to address the public/private partnership called for by federal policy on critical infrastructure protection and to continue to develop their relationships with the ISACs and with each other; and
- a number of challenges to the ISACs' successful establishment, operation, and partnership with DHS and other federal agencies remain, some of which were described by the ISAC Council through a series of white papers.[22]

The report did not recommend any specific actions that could be taken to improve the effectiveness of information sharing between the federal government and the private sector.

The GAO's second report, Critical Infrastructure Protection – Improving Information Sharing with Infrastructure Sectors dated July 9, 2004,[23] focused on improving the efficiency, and effectiveness of information sharing between DHS and the ISACs. The report found that DHS could improve the effectiveness by developing an information sharing plan. This plan would define the roles and responsibilities of the stakeholders. It also found that DHS's ability to collect, analyze, and disseminate information could be improved by developing a Homeland Security Intelligence (HSINT) doctrine. Like most GAO reports, it provides no details on the components of the plan, policies, or procedures. It simply points out they are missing.

[22] Government Accountability Office (GAO), *Critical Infrastructure Protection – Improving Information Sharing with Infrastructure Sectors* (Washington, D.C.: GAO, 2004), 2.

[23] Ibid.

On October 27, 2005, President Bush signed Executive Order 13388 – Further Strengthening the Sharing of Terrorism Information to Protect Americans, which ordered that the highest priority be given to the interchange of information between agencies, all levels of government, and the private sector. Section 1 of Executive Order 13388 makes the objective abundantly clear:

> Section 1. Policy. To the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies:
>
> (a) give the highest priority to … (iii) the interchange of terrorism information between agencies and appropriate authorities of State, local, and tribal governments, and between agencies and appropriate private sector entities; ....[24]

On December 16, 2005, President Bush followed-up Executive Order 13388 by issuing a memorandum to Heads of Executive Departments and Agencies entitled Guidelines and Requirements in Support of the Information Sharing Environment, which re-emphasized that information sharing is a high priority. It directed that, within 90 days of the memorandum, the Director of National Intelligence (DNI) develop and issue common standards for sharing terrorism information with state, local, and tribal governments, law enforcement agencies, and the private sector. The memorandum also directed that within 180 days of the memorandum Secretary of Homeland Security and the Attorney General develop a common framework for the sharing of information with state, local, and tribal governments, law enforcement agencies, and the private sector.

Pursuant to the Intelligence Reform and Terrorism Prevention Act of 2004, the President established the Information Sharing Environment (ISE) and tasked the Program Manager of the ISE to oversee and complete the tasks outlined in his December 16, 2005 memorandum. In May 2006, the PM-ISE issued its recommendations in response to Guideline 2 in the President's December 16, 2005 memorandum. The response recommended that:

---

[24] President George W. Bush, *Executive Order 13388 – Further Strengthening the Sharing of Terrorism Information To Protect Americans* (Washington, D.C.: The White House, 2005).

> DHS must increase its ability to share information in a manner that protects the privacy, civil liberties, and other legal rights of individuals and corporations, as provided for under U.S. law, so that private sector entities can manage risks to their business enterprises, by: . . .
>
> Disseminating actionable alerts and warnings concerning specific private sectors that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations. . . .[25]

Pursuant to the requirements of the 2004 Intelligence Reform and Terrorism Prevention Act, the PM-ISE issued the ISE Implementation Plan in November 2006. The plan, and thus, the federal government, acknowledged that sharing information with the private sector remains a problem citing four key factors:

> First, significant distinctions among the seventeen critical infrastructure and key resources sectors as defined in HSPD-7 (e.g., regulatory regimes, number of players, willingness to collaborate) make it difficult to create a single approach to information sharing operations, structure, and processes. Second, the private sector reports that the demand from Federal, State, and local governments for critical infrastructure and other information since 9/11 has multiplied many times over, imposing more demands on industry to collect information and report it. Third, requests for such information are rarely coordinated or consistent, resulting in duplicative requests. Finally, from the private sector's perspective, the interrelationships between Federal and SLT governments are ambiguous.[26]

The ISE Implementation Plan offered no proposed solution to the problem of sharing terrorism information with the private sector. However, it acknowledged the efforts of the NIAC citing that their July 2006 report entitled Public-Private Sector Intelligence Coordination raised the same issues and reached the same conclusions. It

---

[25] Program Manager – Information Sharing Environment (ISE), "Guideline 2 – Common Sharing Framework," *Information Sharing Environment*, http://www.ise.gov/docs/guidance/guideline%202%20-%20common%20sharing%20framework.pdf (accessed June 22, 2008).

[26] Program Manager – Information Sharing Environment (ISE), *ISE Implementation Plan* (Washington, D.C.: Government Printing Office, 2006), 19 - 20.

also outlined the establishment of a standing subcommittee that will provide a forum to address related private sector issues. The Private Sector Subcommittee was specifically tasked to:

> Action 1.27 The Private Sector Subcommittee will produce a plan that implements elements of the framework as it affects the private sector. This plan must be consistent with statutes and Presidential direction and ensure that information and privacy and legal rights are adequately protected. (Planned Completion: Second Quarter, CY 2007)
>
> Action 2.22 The PM-ISE, in consultation with the ISC, will review the private sector sharing plan developed in Phase 1 and identify priorities for implementation. In addition, some of the recommendations are likely to entail issues requiring executive-level decisions or legislative changes. (Planned Completion: Fourth Quarter, CY 2007)[27]

In January 2007, the PM-ISE and the ISC agreed, as part of their recommendations to Presidential Guidelines 2, to ". . .leverage the CI/KR sector partnership structure, as defined in the NIPP and managed through DHS, as the primary private sector coordination mechanism for the ISE."[28] The PM-ISE's response to action 1.27 and 2.22 above is a baseline document entitled *The CI/KR Information Sharing Environment* and dated April 2007 from the Department of Homeland Security – Office of Infrastructure Protection.[29] According to the PM-ISE's annual report, this ". . . baseline document will serve as a roadmap for improved private sector integration into the ISE."[30] At the time of this literature review, the author has not been able to locate a copy of *The CI/KR Information Sharing Environment*.

On July 26, 2007, the House of Representatives Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment held a hearing on Private Sector Information Sharing: What Is It, Who Does It, and What's Working at DHS?. The

---

[27] Program Manager – Information Sharing Environment (ISE), *ISE Implementation Plan* (Washington, D.C.: Government Printing Office, 2006), 77.

[28] Program Manager – Information Sharing Environment (ISE), *Annual Report to the Congress on the Information Sharing Environment* (Washington, D.C.: Government Printing Office, 2007), 16.

[29] Ibid., 17.

[30] Ibid.

hearing was chaired by the Honorable Chairwoman Harman and the witnesses included key subject matter experts from DHS and the private sector. The DHS witnesses testified that they have made significant progress but a lot more remains to be done. The private sector witnesses testified that it is still not working and may be the worst it has ever been.

Since this hearing, ODNI and DHS have issued Information Sharing Strategy documents.[31,32] Neither of these strategy documents offers any meaningful solution to the problem of public – private sector intelligence sharing. The most promising progress has been made under the Interagency Threat Assessment and Coordination Group (ITACG) pursuant to the Implementing Recommendations of the 9/11 Commission Act of 2007.[33] The March 2008 report, *Establishing the Interagency Threat Assessment and Coordination Group*, submitted to Congress by PM-ISE summarizes their accomplishments.[34] Although there has been some progress on an overarching framework, a public – private sector intelligence sharing strategy remains illusive. The ITAG has yet to issue any intelligence sharing guidance or threat assessments specific to passenger rail.

a. Summary of Federal Documents

Ten years after PDD-63 was issued, much has been written by the federal government on the problem of sharing intelligence and terrorism information between the public and the private sectors. There have been presidential directives, executive orders, presidential memoranda, guidelines and requirements, national strategies and policies, GAO reports, working committees appointed by the President, and hearings in Congress,

---

[31] Office of the Director of National Intelligence, *U.S. Intelligence Community Intelligence Sharing Strategy* (Washington, D.C.: Office of the Director of National Intelligence, 2008), http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf (accessed June 8, 2008).

[32] Department of Homeland Security, *Information Sharing Strategy* (Washington, D.C.: Department of Homeland Security, 2008), http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf (accessed June 8, 2008).

[33] 110th United States Congress, *Implementing Recommendations of the 9/11 Commission Act of 2007* (Washington, D.C.: United States Congress, August 3, 2007), Sec. 521 (a).

[34] Program Manager – Information Sharing Environment (ISE), "Establishing the Interagency Threat Assessment and Coordination Group," *Information Sharing Environment*, http://www.ise.gov/docs/reports/ITACG-CDA.pdf (accessed June 22, 2008).

but the problem still exists. The problem has been well defined by the foregoing literature, but no solutions or alternatives have emerged from this effort.

2. Private Sector Practices

Private sector practices on intelligence and terrorism information sharing with the public sector are not openly available. They protect this information for proprietary reasons and to lower the risk of their means and methods falling into the wrong hands. This could also lead to legal action against the corporation if private customer information becomes available to the general public. Interestingly, the casinos in Las Vegas may be one of the most advanced in sharing intelligence information with government agencies such as Federal Bureau of Investigation (FBI).[35] This is done in an effort to thwart crimes like money laundering and drug trafficking. The quasi public – private sector nuclear electric power generation industry is another sector that may have procedures in place for sharing intelligence information with the government. However, both these examples are not supported by literature openly available to the public for the reasons stated earlier.

In an effort to raise awareness and contribute the untapped private sector knowledge and resources, the private sector has started organizations such as the Homeland Security & Defense Business Council (the "*Council*"). The vision and mission of the *Council* is to ". . . promote the importance of the Private Sector in achieving the vision and mission for homeland security at a national level."[36] They attempt to achieve this by ". . . bring together the best leaders in the private and public sector through industry forums and activities that help to advance thought leadership, future policy, and best practices to advance the homeland security of the nation and the American people."[37] Off the record, representatives from private corporations that belong to the

---

[35] Larry Barrett and Sean Gallagher, "Case 113 - What Sin City Can Teach Tom Ridge," *Baseline* (April 2004).

[36] Homeland Security & Defense Business Council, "Council Vision, Mission, and Value Statement," *Homeland Security & Defense Business Council*, http://www.homelandcouncil.org/aboutus.php (accessed July 12, 2008).

[37] Ibid.

Council state that intelligence sharing is unidirectional, with the private sector providing proprietary information to public sector intelligence agencies and getting no actionable intelligence in return.

3. Academic Studies

Very little has been studied and written on intelligence and terrorism information sharing with the private sector by academia. A review of the academic studies reveals that the subject of information sharing with the private sector is widely mentioned in studies on intelligence information sharing with state and local governments. However, the specific subject of sharing information with the private sector is not analyzed in any detail. It is simply considered the same as sharing intelligence information with state and local governments with no regard to the issues private sector entities present. This quote from a Master's thesis is just one example of this point:

> Successful counterterrorism efforts require that Federal, State, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.[38]

There remains a clear need for the academic study of intelligence and terrorism information sharing between the public and private sectors.

4. Summary of Literature Review

The foregoing literature review shows the definitive need for new research in the area of intelligence sharing. The analysis and conclusions by Judge Richard Posner in his books *Preventing Surprise Attacks,*[39] *Uncertain Shield – The U.S. Intelligence System in*

---

[38] Patrick Miller, "How Can We Improve Information Sharing Among Local Law Enforcement Agencies?" (Master's Thesis, Naval Postgraduate School, 2005), 4.

[39] Richard A. Posner, *Preventing Surprise Attacks* (Lanham, MD: Rowman & Littlefield Publishing Group, 2006).

the Throes of Reform,[40] and *Countering Terrorism*[41] are excellent examples of the type of research that needs to be done, but specifically in the area of public – private sector intelligence sharing. Ideally, it would focus on intelligence and terrorism information sharing in the passenger rail transportation sector. This thesis is the first to answer the call for such research.

F. METHOD

The research methodology consists of three distinct components that will collectively lead to an effective strategy for intelligence and terrorism information sharing within a private passenger rail organization, and with their external public partners (Chapter III):

1. Key Amtrak personnel will be interviewed to establish and confirm how intelligence information currently flows within Amtrak and with its external intelligence community and law enforcement partners (Chapter II).
2. A survey of key Amtrak operations personnel to establish Amtrak's intelligence priorities and requirements (Chapter IV).
3. Two case studies on potential models for intelligence and terrorism information sharing (Chapters V and VI).

The current flow of intelligence information within Amtrak and with its external partners will be established and confirmed by interviewing Amtrak's Chief of Police, the head of Amtrak's Police Intelligence Unit, and Amtrak's VP of Transportation. The data collected from these interviews will be compared to generally accepted intelligence community and law enforcement practices. These practices will be validated through an interview with an experienced neutral member of law enforcement and the intelligence community.

[40] Richard A. Posner, *Uncertain Shield – The U.S. Intelligence System in the Throes of Reform* (Lanham, MD: Rowman & Littlefield Publishing Group, 2006).

[41] Richard A. Posner, *Countering Terrorism* (Lanham, MD: Rowman & Littlefield Publishing Group, 2007).

The narrative and testimonial data collected from this research will be analyzed for common themes using a qualitative evaluation process. The purpose of this analysis is to identify:

1. The most useful and dependable sources of intelligence for Amtrak;
2. The patterns and nodes of interaction;
3. The nature of the information required to protect the public and critical infrastructure;
4. The critical pathways for intelligence in an effective system; and
5. The critical nodes and decision makers that require timely intelligence to protect the public and critical infrastructure.

With the assistance of Amtrak's Office of Security Strategy and Special Operations (intelligence and security policy units), Amtrak's intelligence and terrorism information requirements will be defined and developed, by seeking input from key Amtrak personnel in the following railroad operating departments:

1. Transportation (train operating crews, on-board service personnel, and station personnel);
2. Engineering (infrastructure operations, maintenance, and engineering);
3. Mechanical (locomotive and passenger car maintenance and engineering);
4. Police (law enforcement); and
5. Environmental, Health, and Safety (Environmental Protection Agency, Food and Drug Administration, and Occupational Safety and Health Administration requirements monitoring and compliance).

Two case studies will be purposely analyzed to determine if they meet Amtrak's intelligence and terrorism information sharing requirements. The first case study is on the New York Police Department (NYPD) SHIELD model. This case study will be qualitatively analyzed from two distinct perspectives: (1) NYPD SHIELD and (2) the private sector - Amtrak. The second case study is on the British Transport Police (BTP) Counterterrorism Unit model. The British Transport Police (BTP) practices in the United Kingdom (UK) will be comparatively analyzed with the practices in the U.S.

This research will be the first to identify the key factors and components of a public – private sector intelligence and terrorism information sharing strategy using evidence driven analysis.

THIS PAGE INTENTIONALLY LEFT BLANK

II. INTELLIGENCE AND TERRORISM INFORMATION SHARING WITH AND WITHIN AMTRAK TODAY

This chapter will focus on establishing the status of intelligence and terrorism information sharing with and within Amtrak today.[42] It is a point in time along a dynamic continuum of policies and practices.

A. THE EXISTING MEANS AND METHODS

During February and March 2008, the author interviewed Amtrak Chief of Police John O'Connor,[43] Amtrak Police Inspector (Intelligence Unit) Neil Trugman,[44] and Mr. Bart Johnson,[45] Director for Homeland Security and Law Enforcement Support, Office of the Director of National Intelligence. The purpose of these interviews was to establish and confirm how intelligence information currently flows within Amtrak and with its external intelligence community and law enforcement partners. The testimonial data was a qualitative analysis to identify:

1. The sources of intelligence for Amtrak;
2. The patterns and nodes of interaction;
3. The nature of the information;
4. The pathways for intelligence; and
5. The nodes and decision makers.

1. Sources of Intelligence for Amtrak

In all cases, DHS, the FBI, and the FBI Joint Terrorism Taskforce Force (JTTF) were cited as the most dependable external source of intelligence. State and local sources

[42] For the purpose of this thesis, the status is as of March 2008.

[43] Chief John O'Connor has over 35 years of dedicated law enforcement service in railroad policing. Prior to joining Amtrak, he was the Chief of Police for Long Island Railroad.

[44] Neil Trugman was formerly a Detective (Grade One) with the Washington, D.C., Metropolitan Police Gang Intelligence Unit. He retired after 27 years of dedicated service.

[45] Major Bart Johnson retired from the New York State Police after 25 years of dedicated service to join the Office of the Director of National Intelligence. When he retired from the New York State Police in January 2008, he was the founding head of their Counterterrorism Intelligence Preparedness Response Program (an early version of the state fusion center).

such as state and local fusion centers (SLFC) were noticeably absent as a source of intelligence. The credibility of the information was dependent on the credibility of the source. This seems obvious, but it is critical to understanding the behavior of the risk mitigation decision makers. For example, if the source of the information is determined to be credible, the intelligence officer[46] will take appropriate action to reduce the risk associated with the threat. The intelligence officer, however, would invariably delay these actions, by days in some cases, to confirm the credibility of the source. Consistently, the source was deemed to be credible if it came from one of two areas (the "*Credible Sources*"): (1) foreign intelligence from locations such as the training camps in the tribal provinces of Pakistan; and (2) domestic intelligence from local police investigations. In all cases, the intelligence information was provided by a source external to Amtrak.

2. Pattern and Nodes of Interaction

When intelligence on a domestic threat is received by the intelligence community and law enforcement, an informal network engages in what can be best described as social exchanges of trust in an effort to determine if the intelligence information can be traced back to one of the two aforementioned sources. According to Major Bart Johnson, "You get it [intelligence] officially, and then you start working through the unofficial channels of your network."[47] These informal social networks consist of individuals who have earned the trust of at least one other individual in the network. As Major Johnson states, "official channels and unofficial channels work wonderful. Sometimes the unofficial work better."[48]

3. Nature of the Information

Intelligence must include enough specificity to enable actions that reduce the risk associated with the threat. The specificity would include more than one of the following:

---

[46] Intelligence officer includes intelligence and law enforcement personnel engaged in the function of gathering information.

[47] Bart Johnson (Director for Homeland Security and Law Enforcement, Office of the Director of National Intelligence), interview with the author, Washington, D.C., February 8, 2008.

[48] Ibid.

1. the nature of the threat;
2. the delivery method;
3. location;
4. date and/or time; and
5. the asset to be attack.

This is analogous to having physical evidence in a crime investigation. According to Amtrak Police Inspector Neil Trugman,

> In law enforcement, there is nothing stronger than physical evidence, finger prints and DNA and in terrorism you don't have the opportunity for finger prints and DNA, unfortunately, until it's done. When you have a map and photographs, and writings of what is going to be done …, and you see that came from an interview, that is good physical evidence.[49]

According to Amtrak Chief of Police John O'Connor, it is "Traditional law enforcement. Once you have information that specific you pull out all the stops. The danger to the public is too great."[50] The nature of the information is also a key secondary variable in determining the credibility of the source. It is a secondary variable because often the information includes the necessary specifics, but is not credible because it cannot be traced to one of the two *Credible Sources*.

4. Pathways for Intelligence

This research showed that threat information typically flows from the DHS or FBI to an intelligence officer where the source is validated and confirmed in their personal informal network to be one of the two *Credible Sources*. Once the credibility of the threat information is confirmed, the intelligence officer will then take action to mitigate the risk independent of those individuals responsible and accountable for the protection of the public and critical infrastructure. On the surface this seems simple, but the effort on the part of the intelligence officer to validate and confirm the source credibility is time

[49] Neil Trugman (Amtrak Police Inspector), interview with the author, Washington, D.C., February 25, 2008.

[50] John O'Connor (Amtrak Chief of Police), interview with the author, Washington, D.C., February 21, 2008.

consuming and ineffective. Amtrak Police Inspector Neil Trugman captures this inefficiency and how it could potentially be eliminated in the following statement:

> The experience of law enforcement to marry up with analytical people is really the lesson learned. The analysts look at a situation and analyze it to great detail. Law enforcement has the experience to implement plans and to prevent things from happening. I think that ended up being the lessons learned here. We needed to include the federal agencies that were getting this information and the analytical people that were getting this information and putting into the computer systems that we were able to read, we had to include the investigative people, the intelligence and law enforcement people, because they have insight of the potential of this actually happening or not happening.[51]

5. Decision Making Nodes

There are three critical decision making nodes: (1) the intelligence provider; (2) the domestic intelligence officer; and (3) the position(s) accountable for protecting the public and critical infrastructure. The intelligence provider is the *Credible Source* agency or individual, and the intelligence officer is usually the head of counterterrorism bureau, but is often a lower level officer assigned to coordinating intelligence. The narrative and testimonial interview data clearing shows that law enforcement views it the responsibility of their senior leadership to take action and protect the public and the critical infrastructure. Amtrak Police Inspector Neil Trugman espouses:

> The day police officers get out of the academy they are taught how to prevent things from happening. The federal agencies historically are investigating things after they occur and they really didn't have a preventive measure, except maybe in spying. For the most part they are new to this, in preventing things from happening. They were always an investigative leg to handle situations after they happen. Where cops, state and local law enforcement, have always in the beginning always learned how to prevent.[52]

In the private sector, this is the Chief Operating Officer and their critical operating personnel.

---

[51] Neil Trugman (Amtrak Police Inspector), interview with the author, Washington, D.C., February 25, 2008.

[52] Ibid.

Figure 1 summarizes and illustrates Amtrak's current means and methods of acquiring and verifying intelligence. The research showed that there is no formal connection between the intelligence community (ODNI – NCTC[53]), law enforcement (FBI), and private sector passenger rail railroads such as Amtrak. The threat information only becomes trusted after it has been validated in the informal network of the intelligence officer.

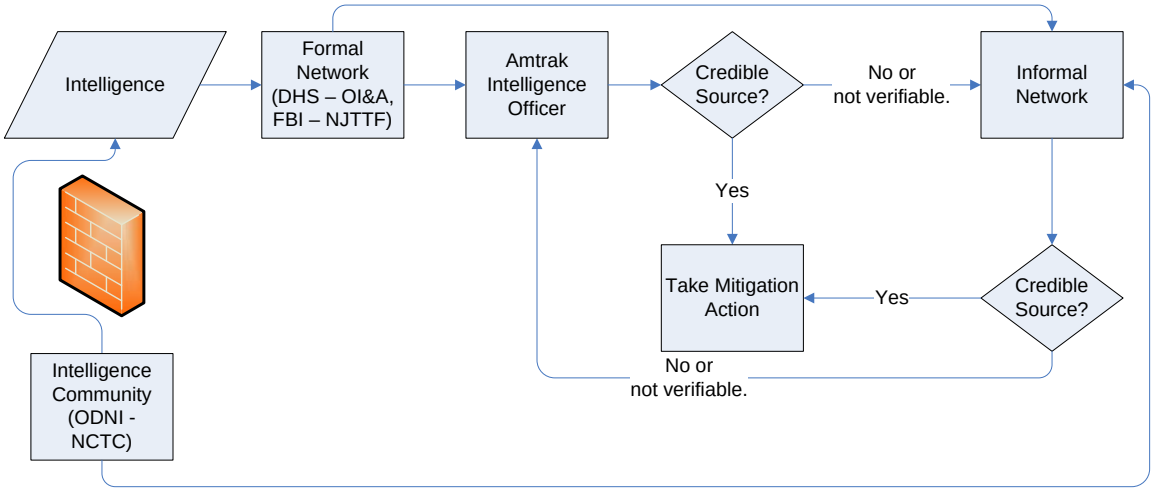


Figure 1. Amtrak's current means and methods of acquiring intelligence.

B. SUMMARY

This chapter established the network Amtrak currently relies on for intelligence and terrorism information. Like most passenger rail organizations, Amtrak:

- Relies on DHS, the FBI, and the FBI JTTF field offices for official intelligence. SLFCs are noticeably absent as a source for intelligence and threat information. Also noticeably absent is a routine means of processing threat information from local authorities;
- Verifies and confirms intelligence using an informal network of personal contacts with the intelligence community and law enforcement;
- Verifies and confirms the credibility of the intelligence source before taking action;

[53] NCTC is the abbreviation for the National Counterterrorism Center.

- Requires some specifics on the nature of the threat, delivery method, location, date – time, or asset to be attacked before taking action;
- Relies on law enforcement to take the lead in mitigating the risk associated with the threat;
- The existing means and methods is not intelligence analysis, it is report processing and management. The law enforcement officer becomes both the analyst and the crisis manager; and
- The existing model lacks synthetic diagnostics and prognostic analytical techniques.

The foregoing research has largely focused on the history and current status of intelligence sharing between public and private (Amtrak) sector agencies. The remaining chapters will focus on three interrelated threads:

1. A proposed strategy for public – private sector passenger rail intelligence and terrorism information sharing;
2. Defining the intelligence priorities and requirements for passenger rail (Amtrak); and
3. Defining the dissemination criteria for intelligence and terrorism information in the passenger rail transportation sector.

It will show why the proposed strategy is effective through two case studies (Chapters V and VI) and will conclude with the resources recommended to implement and execute the strategy.

The next chapter will propose a public – private sector passenger rail intelligence and terrorism information sharing strategy. It will present a theoretical analysis of why information is chosen to be shared, or not shared. Based on this understanding, the final sections of this chapter will present an intelligence and terrorism information sharing strategy for passenger rail.

III. INTELLIGENCE AND TERRORISM INFORMATION SHARING STRATEGY

> *The biggest impediment to all-source analysis – to a greater likelihood of connecting the dots – is the human or systemic resistance to sharing information.*[54]

The 9/11 Commission claimed that it is human nature to resist sharing information. In making this unsubstantiated claim, they did not attempt to understand the social psychology of information sharing before making sweeping recommendations regarding this perceived problem. When designing a system or network for the sole purpose of sharing information, it is important to understand the social laws of human behavior. According to psychologist, Dr. Phil Zimbardo, ". . . situations interact to generate behavior; people are always acting within various behavioral contexts. People are both products of their different environments and producers of the environments they encounter."[55] The resistance to sharing information may be more of a response to the situation, structure, systems or rules that have been created around information sharing, than a human behavior.

A literature review on the social psychology of information sharing reveals that a significant amount of research has been done using network analysis to connect the dots and root out terrorists before they strike. Some of the significant, and well debated, academic literature on network analysis as it relates to terrorism includes:

1. *Networks and Netwars: The Future of Terror, Crime, and Militancy* by John Arquilla and David Ronfeldt;[56]
2. "Networks, Netwar, and Information-age Terrorism" by John Arquilla, David Ronfeldt, and Michele Zanini;[57]

---

[54] 9/11 Commission, *The 9/11 Commission Report* (New York, NY: W.W. Norton & Company, 2004), 416.

[55] Dr. Phil Zimbardo, *The Lucifer Effect* (New York, NY: Random House, 2008), 319.

[56] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, D.C.: RAND Corporation, 2001).

[57] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-age Terrorism," in *Countering the New Terrorism*, ed. Ian O. Lesser et al., (Santa Monica, CA: RAND, 1999).

3. "Uncloaking Terrorist Networks" by Valdis Krebs';[58]
4. *Understanding Terror Networks* by Marc Sageman;[59] and
5. Social Network Analysis: A Handbook by John P. Scott.[60]

Instead of focusing on rooting out evil, what if network theory was used to improve day-to-day information sharing and communication so good things could be done with accurate intelligence? Before answering this question, however, it is important to understand what makes people share information in some situations and withhold it in others. What is the psychology of information sharing?

A. PSYCHOLOGY OF INFORMATION SHARING

During the 9/11 hearings, Attorney General William Barr, referred to the inability of the intelligence community and law enforcement to share information as the ". . . wall of separation."[61] The wall being the situation, the official system, the structure, as well as the long standing rules of engagement between the intelligence community and law enforcement agencies, or a virtual firewall. While conducting research interviews on intelligence sharing, the author uncovered an informal network of weak ties between the intelligence community and law enforcement. This highly effective and efficient informal network routinely thwarts the firewall with social exchanges of trust to establish the source credibility of the intelligence. If it is possible to understand why information is openly and freely shared in informal networks, but not in formal networks, it may be possible to duplicate the situation for the purpose of efficient intelligence sharing.

---

[58] Valdis Krebs', "Uncloaking Terrorist Networks," *First Monday*, http://www.firstmonday.org/Issues/issue7_4/krebs/ (accessed May 29, 2008).

[59] Marc Sageman, *Understanding Terror Networks* (Philadelphia: University of Pennsylvania Press, 2004).

[60] John P. Scott, *Social Network Analysis: A Handbook* (Thousand Oaks, CA: SAGE Publications, 2000).

[61] William P. Barr, "Statement of William P. Barr to the National Commission on Terrorist Attacks Upon the United States," *National Commission on Terrorist Attacks Upon the United States*, http://govinfo.library.unt.edu/911/hearings/hearing6/witness_barr.htm (accessed February 29, 2008).

As with any relationship, communication and information sharing is highly dependent on trust. The more trust in a relationship, the more open and free flowing the communication and value of the information. In his book, *The Speed of Trust*, Stephen M.R. Covey successfully argues the merits of trust in relationships:

> Trust impacts us 24/7, 365 days a year. It undergirds and affects the quality of every relationship, every communication, every work project, every business venture, every effort in which we are engaged. It changes the quality of every present moment and alters the trajectory and outcomes of every future moment of our lives – both personally and professionally.[62]

Thomas Freidman, in his best selling book, *The World is Flat*, supports Covey's argument with this statement:

> Without trust, there is no open society, because there are not enough police to patrol every opening in an open society. Without trust, there can also be no flat world, because it is trust that allows us to take down walls, remove barriers and eliminate friction at borders.[63]

While conducting research at the Institute for Knowledge-Based Organization for their book, *The Hidden Power of Social Networks*, Rob Cross and Andrew Parker determined that two types of trust play a significant role in information flow: *benevolence – based* and *competence – based* trust.[64] *Benevolence – based* trust focuses on vulnerability or trusting someone to not make light of, or expose, your lack of knowledge on a subject. *Competence – based* trust focuses on ability or trusting someone's opinion such that one's thinking is reshaped. When these two components are present in a relationship, information is shared efficiently and effectively. In an informal network, the connection or relationship between two individuals exists because of the presence of

---

[62] Stephen M.R. Covey, *The Speed of Trust* (New York, NY: Free Press, 2006), 1 – 2.

[63] Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-first Century* (New York, NY: Farrar, Straus, and Giroux, 2005), 394.

[64] Rob Cross and Andrew Parker, *The Hidden Power of Social Networks* (Boston, MA: Harvard Business School Publishing, 2004), 99.

these two types of trust. During a research interview on intelligence sharing, Amtrak Chief of Police, John O'Connor, captured the essence of *benevolence – based* and *competence – based* trust in this statement:

> I would reach out to a couple of high ranking transportation law enforcement people where I value their opinion. Within the corporation, I would reach out to our stakeholders and those whose opinion I value. When I say that it is without regard to rank, it may be someone in the police organization at a lower rank because I like the way they think . . .[65]

The strength of this connection or tie, and therefore, the level of information sharing, is directly dependent on the level of *benevolence – based* and *competence – based* trust in the relationship. During their research at the Institute for Knowledge-Based Organization, Rob Cross and Andrew Parker observed that:

> When someone provided access to a limited or sensitive resource, information seekers often took it as a sign that the person viewed them as trustworthy. This, in turn, often promoted reciprocal trust in the person sought for information.[66]

Official networks have forced connections that are not built on this foundation and often lack both kinds of trust. The connection between two individuals exists solely because of their respective positions and areas of responsibility. This is why socializing with new business acquaintances over lunch, or sharing a round of golf, improves communication and strengthens the relationship. The level of both types of trust in the relationship usually improves after these types of social engagements.

Now that it is understood that *benevolence – based* and *competence – based* trust is the catalyst for information sharing in informal networks, it may be possible to duplicate the situational benefits formally through network analysis without rebuilding the impeding walls.

---

[65] John O'Connor (Amtrak Chief of Police), interview with the author, Washington, D.C., February 21, 2008.

[66] Rob Cross and Andrew Parker, *The Hidden Power of Social Networks* (Boston, MA: Harvard Business School Publishing, 2004), 102.

B. NETWORK ANALYSIS

In his controversial and widely debated article, "Networks, Netwar, and Information-age Terrorism," John Arquilla claimed that: "It takes a network to fight a network."[67] There are currently two academically accepted approaches to network analysis: social and organizational. Social network analysis attempts to model networks visually and mathematically. Organizational network analysis focuses on how a network functions or how it operates.

1. Social Network Analysis

Social network analysis uses visual topologies and mathematics to model and measure the efficiency, effectiveness, and resiliency of a network. There are three basic network topologies as shown in Figure 2.

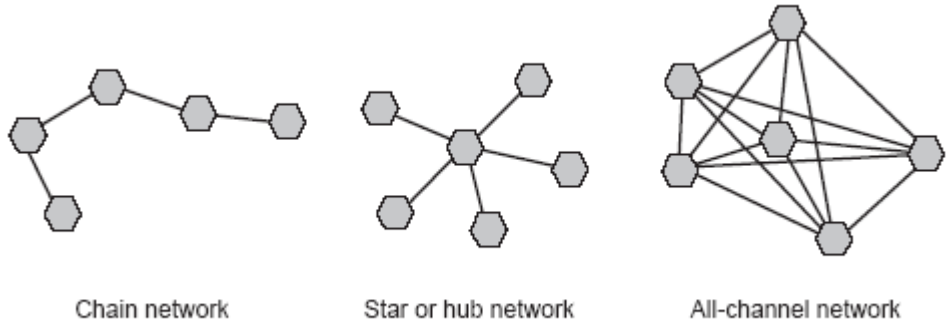


Figure 2. Network Topologies.[68]

The points in the network are commonly referred to as nodes, and the connection between nodes are referred to as links or ties. The *chain* network forces end-to-end communication through the intermediate nodes. In a *star,* or hub, network communication between edge nodes flows through a central node, or hub. An *all-channel*

[67] John Arquilla, David Ronfeldt, and Michele Zanini, "Networks, Netwar, and Information-age Terrorism," in *Countering the New Terrorism*, ed. Ian O. Lesser et al., (Santa Monica, CA: RAND, 1999), 55.

[68] Ibid., 50.

network is a collaborative network where any node can communicate directly with another node. Although there are many other network topologies, their basic structure is a derivative of one, or more, of these three. It should be noted, however, that the foregoing topologies are not representative of known terror networks. Their purpose in this analysis is to provide a conceptual framework.

Official networks, such as the intelligence community and law enforcement agencies, have hierarchical or centralized topologies where a central node or leader controls the network. Informal networks have all-channel or decentralized topologies that are leaderless. Until the advent of network theory, the belief has tended to be that a centralized structure is more effective and efficient than a decentralized one because it is easy to understand the relationships, and it is clear who is in charge. Recent studies have shown that, in some cases, centralized networks are no match for leaderless decentralized networks. The power of decentralization is evident in such human networks as Napster, Skype, Craigslist, Apache, Wikipedia, and Burning Man.[69] Each of these networks is leaderless, but extremely effective and efficient at accomplishing their intended goal. One of their most important characteristics is a tendency to become more open and decentralized when they are challenged.[70] For example, when the record industry shutdown Napster and Kazaa, it resulted in eMule, which is a leaderless and an even more decentralized music distribution network.[71]

2. Organizational Network Analysis

Organizational network analysis concentrates on the design and performance of a network. According to John Arquilla and David Ronfeldt, ". . . the design and performance of such networks depend on what happens across five levels of analysis (which are also levels of practice):"[72]

---

[69] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider* (New York, NY: Penguin Group, 2006), 59 - 81.

[70] Ibid., 21.

[71] Ibid., 25.

[72] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, D.C.: RAND Corporation, 2001), 323.

(a) organizational;

(b) narrative;

(c) doctrine;

(d) technological; and

(e) social.

The organizational level refers to the resiliency of the network design. The narrative level is the story behind the network, and the doctrine is the collaborative strategies and methods. The technology level refers to the systems that facilitate the information sharing. The social level is the personal ties that assure loyalty and trust. According to John Arquilla and David Ronfeldt, the strength of a network is dependent on achieving success across all five levels:

> The strongest networks will be those in which the organizational design is sustained by a winning story and a well-defined doctrine, and in which all this is layered atop advanced communications systems and rests on strong personal and social ties at the base. Each level, and the overall design, may benefit from redundancy and diversity. Each level's characteristics are likely to affect those of the other levels.[73]

Good, if not great, things can be accomplished with the knowledge that information sharing is best accomplished in resilient, decentralized networks of weak ties that have a known purpose, collaborative strategies, technological systems, and most importantly, social strength built on trust. The next section will focus on how this knowledge can be applied to intelligence sharing.

C. INTELLIGENCE SHARING STRATEGY CANVAS

A strategy canvas is an analytic and action framework that serves two purposes. It captures the current state, and presents the value innovation of the desired future state.[74] Figure 3 illustrates the strategy canvas for passenger rail intelligence sharing. The dashed

[73] John Arquilla and David Ronfeldt, *Networks and Netwars: The Future of Terror, Crime, and Militancy* (Washington, D.C.: RAND Corporation, 2001), 324.

[74] Chan Kim and Renée Mauborgne, *Blue Ocean Strategy* (Boston, MA: Harvard Business School Press, 2005), 25.

line illustrates that Amtrak's intelligence priorities and requirements are not being met, and that the intelligence products received from current sources have low to medium value.

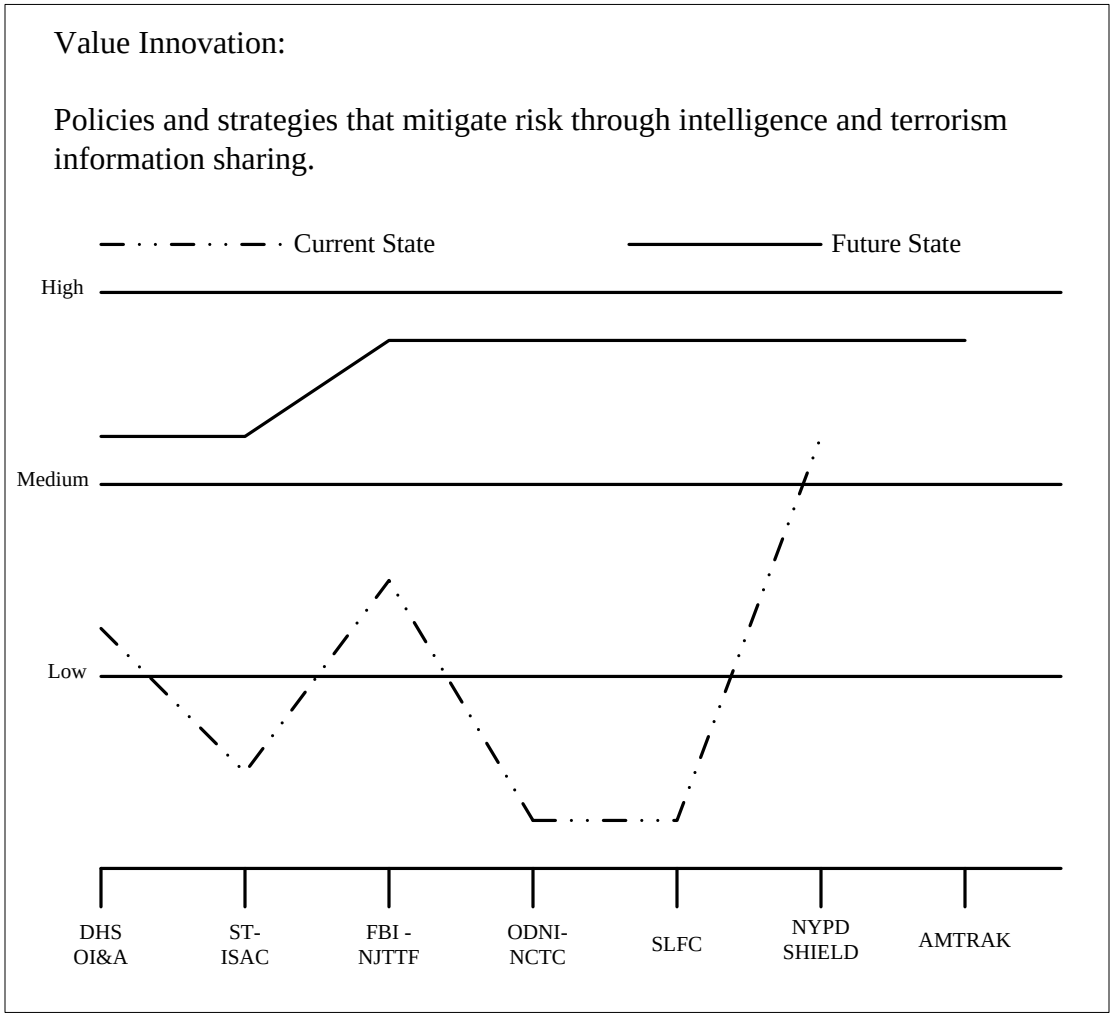


Figure 3. Intelligence and terrorism information sharing strategy canvas.

According to Chan Kim and Renée Mauborgne, the desired future state can be determined by answering the following four questions:

- Which of the factors that the industry takes for granted should be *eliminated*?
- Which factors should be *reduced* well below the industry's standard?
- Which factors should be *raised* well above the industry's standard?
- Which factors should be *created* that the industry has never offered?[75]

Table 1 summarizes the actions that should be taken to achieve Amtrak's intelligence priorities, and increase the value of the intelligence products. The solid line in Figure 3 conceptually shows the future value after taking these actions.

Eliminate	Raise
• Walls between members by building trust	• Trust among members • Collaboration among members • Strength of existing relationships
Reduce	**Create**
• Distrust between members of the network • Formalization of relationships between members	• Connection with state/ local fusion centers • Informal relationships with distance members

Table 1. Four actions that will improve intelligence and terrorism information sharing.

In *Blue Ocean Strategy*, Chan Kim and Renée Mauborgne assert that a good business strategy has three characteristics: (1) focus; (2) divergence; and (3) a compelling tagline.[76] Focus eliminates diffusing efforts across all the possible options. Divergence breaks away from what others are doing to look at alternatives. A compelling tagline

[75] Chan Kim and Renée Mauborgne, *Blue Ocean Strategy* (Boston, MA: Harvard Business School Press, 2005), 29.

[76] Ibid., 37.

brings immediate clarity to the strategy. These characteristics are also inherent in an effective intelligence sharing strategy. The proposal presented in this thesis focuses on intelligence led situational awareness for the passenger rail operating environment. It is specifically designed not to duplicate the intelligence provided by the intelligence community and law enforcement. The compelling tag line is *intelligence led situational awareness.*

D. A STRATEGY FOR PUBLIC – PRIVATE SECTOR PASSENGER RAIL

While policy makers and homeland security practitioners struggle with the application and implementation of the laws enacted in the aftermath of 9/11, Amtrak operates 305 trains daily without actionable intelligence and terrorism information reports under the persistent threat of terrorism. The findings from the foregoing evidence driven research collectively lead to the urgent need for a new strategy. Figure 4 illustrates a proposed network for intelligence and terrorism information sharing within a private passenger railroad and with its external partners, federal, state, and local government, and the private sector. The links, or ties, in Figure 4 conceptually show the interconnections, or relationships, required for intelligence and terrorism information sharing within Amtrak and with the key external partners.

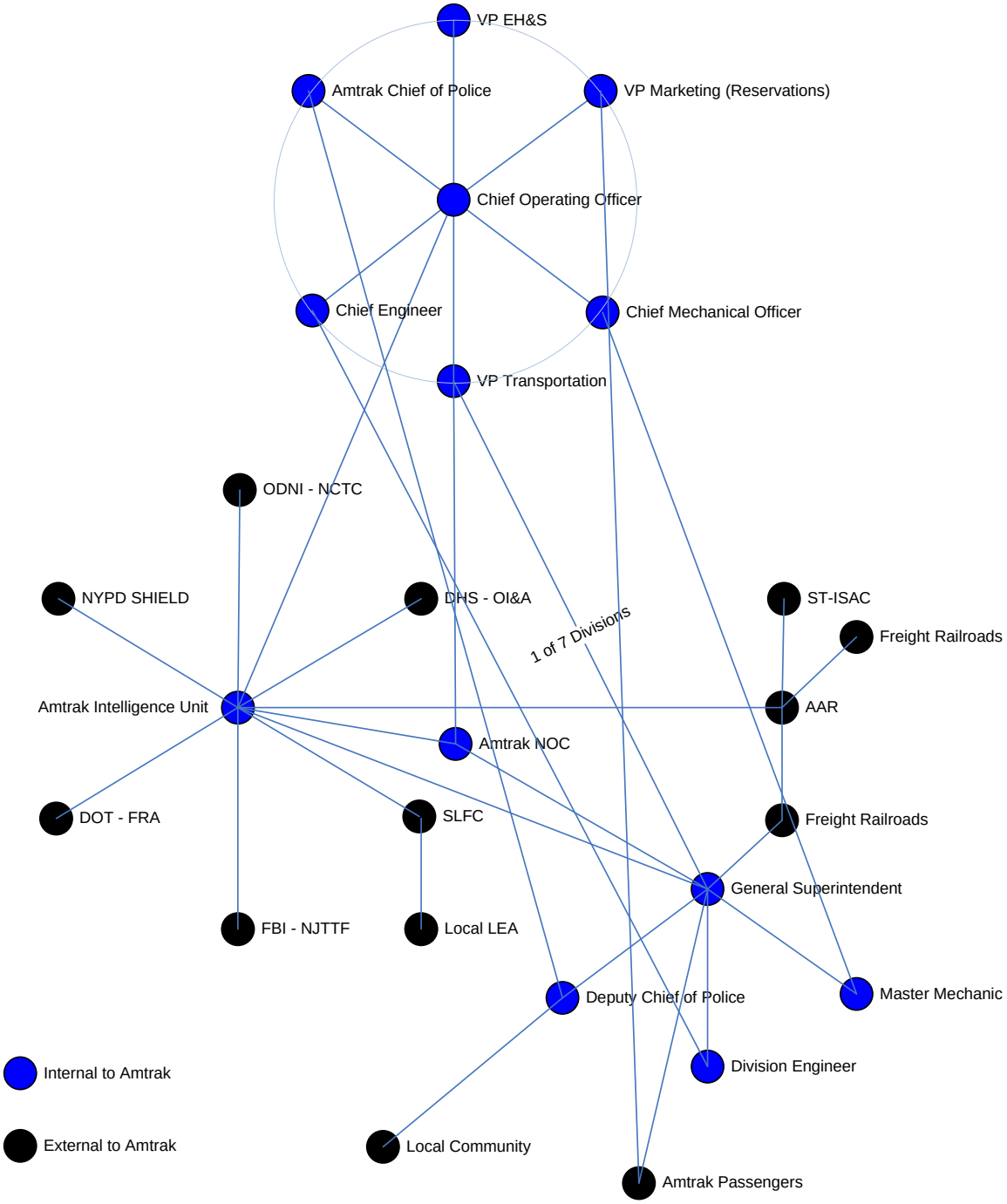


Figure 4. A new intelligence sharing network for public – private passenger rail.

E. MEGACOMMUNITIES AND INTELLIGENCE SHARING NETWORKS

The members external to Amtrak in the intelligence network presented in Figure 4 can be organized into three groups: (1) Government; (2) Civil Society; and (3) Business. Figure 5 conceptually illustrates the external members categorized by these three groups. The position of each entity relative to each other is not important. What is important is the assigned group. The interconnection of the groups shown in Figure 5 forms what is known as a megacommunity.

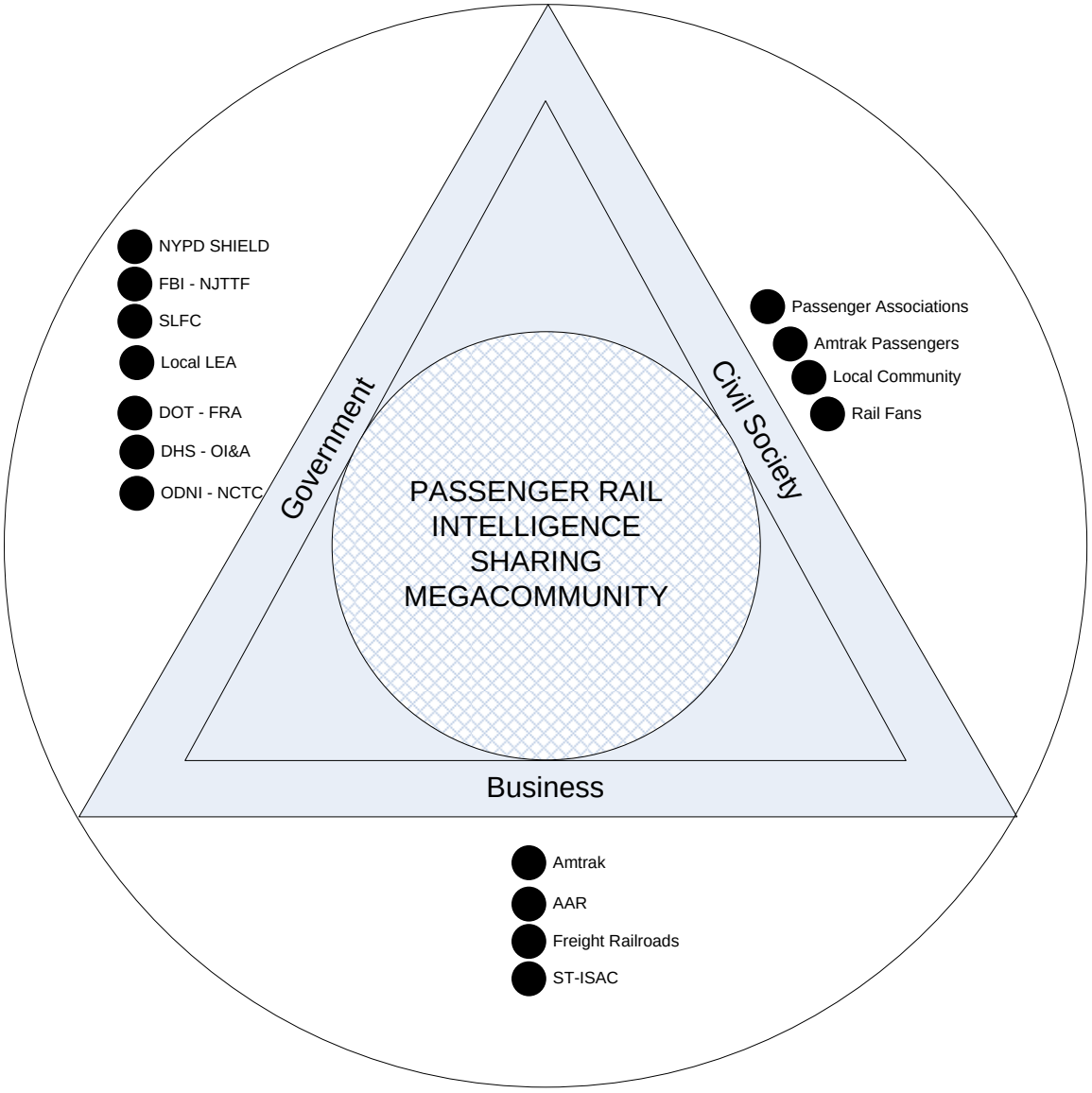


Figure 5. Passenger rail intelligence sharing megacommunity.

According to Mark Gerencser et al.,:

> Megacommunities are not large communities of people; they are communities of organizations whose leaders and members have deliberately come together across national, organizational, and sectoral boundaries to reach goals they cannot achieve alone.[77]

This megacommunity network is focused on the common goal of acquiring and sharing intelligence and threat information specific to passenger rail. Information is shared among the members based on *benevolence* and *competency* based trust. The strength and performance of the network comes from the presence of organizational, narrative, doctrinal, technological, and social levels. The organizational design is sustained by the nobility of protecting America's passenger rail system layered atop of the continuing advance of modern communication systems, which is built upon personal and social ties.

In the groundbreaking research article, "The Strength of Weak Ties," Mark Granovetter argued that ". . . individuals with few weak ties will be deprived of information from distant parts of the social system and will be confined to the provincial news and views of their close friends."[78] Stated in the positive form, social systems with weak ties receive information earlier than those with only strong ties. The evidence presented by Granovetter suggests that social networks with weak ties are able to organize more quickly to take action. He also asserted that weak ties are ". . . important because their likelihood of being bridges is greater than (and that of strong ties less than) would be expected from their numbers alone."[79] A bridge, in this case, is defined as a connection between groups, cliques, or nodes in a social network such as a megacommunity. Based on Granovetter's weak tie theory, Mark Gerencser et al., argue that:

---

[77] Mark Gerencser et al., *Megacommunities* (New York, NY: Palgrave MacMillan, 2008), 28.

[78] Mark Granovetter, "The Strength of Weak Ties: A Network Theory Revisited," *Sociological Theory* (1983): 202.

[79] Ibid., 229.

> In order to form or activate a megacommunity, leaders must utilize weak ties to reach out beyond their sector, beyond their geographical location, and access the latent connections of the networked world. Without weak-tie connections, the megacommunity will not grow appropriately, information will not spread, relationships will not build, and a diversity of opinions will not be incorporated.[80]

A megacommunity with its groups linked by informal weak ties is more efficient and effective than a network based on formal strong ties. Gerencser et al., assert that:

> Weak ties bring information into the network that is not provided by the members with "strong" ties. Indeed, people with many "weak ties" (or casual and temporary acquaintances) are often better informed and better equipped to share information than people with a few "strong ties" to close friends and family members.[81]

Figure 6 illustrates the strength of weak ties in the proposed intelligence and terrorism information network from Figure 4. It conceptually shows how weak ties expand the network at the edges and interconnect previously disconnected key nodes.

[80] Mark Gerencser et al, *Megacommunities* (New York, NY: Palgrave MacMillan, 2008), 136.

[81] Ibid., 72.

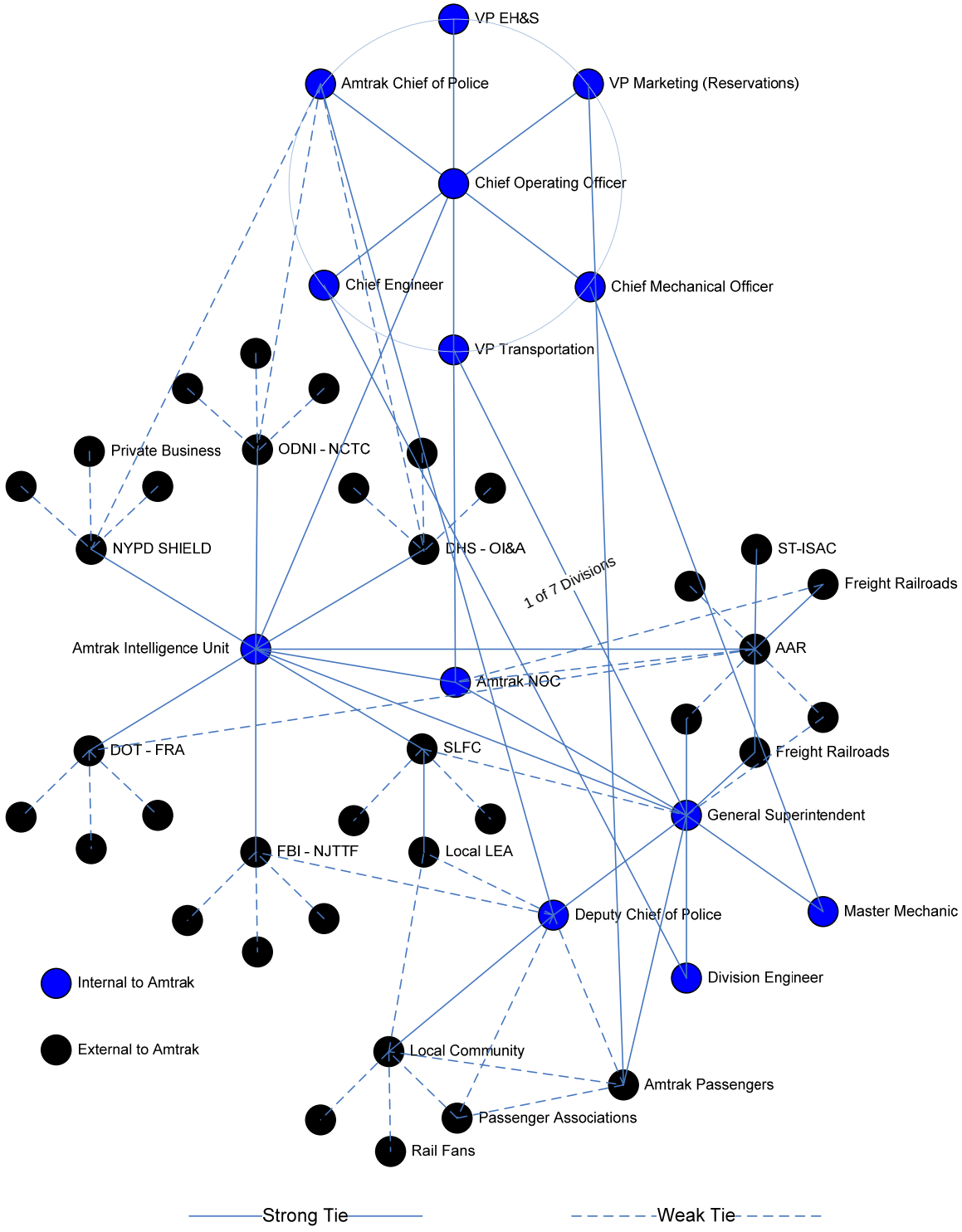


Figure 6. The strength of weak ties in Amtrak's intelligence sharing model.

During a briefing on Amtrak's security strategy with the author, Brian Jenkins captured the essence of the weak tie theory as it applies to intelligence networks with this statement:

> Do not formalize the [intelligence] network. If you formalize it, it is doomed. Keep it an informal working group.[82]

The less codified the network, the more freely information will flow. The emphasis should be on collaborative relationships built on trust; not codifying the relationship with lengthy memorandums of understanding or other legal instruments.

F. SUMMARY

This chapter presented a public – private sector intelligence and terrorism information sharing network for passenger rail. It concluded that:

- *Benevolence – based* and *competence – based* trust between individuals is the catalyst for sharing information in an informal network;
- Information sharing is best accomplished in resilient, decentralized networks of weak ties that have a known purpose, collaborative strategies, technological systems, and most importantly, social strength built on trust;
- The proposed intelligence and terrorism information sharing network for passenger rail is stronger and more effective if it includes weak ties built around the conceptual framework of a megacommunity;
- The proposed intelligence and terrorism sharing network will include members from government (public sector), business (private sector), and civil society;
- The less codified the network, the more freely information will flow; and
- The emphasis should be on collaborative relationships built on trust; not codifying the relationship with lengthy memorandums of understanding or other legal instruments.

The next chapter will present the remaining two threads:

1. It will define the intelligence priorities and requirements for passenger rail (Amtrak); and
2. It will define the dissemination criteria for passenger rail (Amtrak) intelligence and terrorism information.

---

[82] Brian Jenkins (Senior Advisor, RAND), informal briefing session with the author, Washington, D.C., June 17, 2008.

IV. DEFINING AMTRAK'S INTELLIGENCE REQUIREMENTS

The last chapter presented a strategy for intelligence and terrorism information sharing in the passenger rail transportation sector. For this strategy to be effective, it is critical that the intelligence requirements or goals, and the dissemination criteria be clearly defined. This chapter will focus on these two objectives.

A. THE GLOBAL THREAT TO PASSENGER RAIL

On February 29, 2008, the TSA issued a mass transit (passenger rail) threat assessment that concluded previous rail attacks in Madrid (March 2004), London (July 2005), and Mumbai (July 2006) could inspire terrorists to conduct similar attacks in the U.S. The assessment states that mass transit and passenger rail systems are vulnerable to terrorist attacks because they are accessible to large numbers of the public and are difficult to secure. Multiple improvised explosive devices (IEDs) and improvised incendiary devices (IIDs) are the most common means of attacking mass transit targets. Although this threat assessment is seemingly obvious, it reflects the reality of global terrorism. A copy is contained in Appendix A.[83]

B. AMTRAK'S INTELLIGENCE REQUIREMENTS

There are three key issues when defining intelligence requirements: (1) the priorities, which come from the policy makers and field users; (2) the types of information required; and (3) to whom and how often it should be disseminated. The first two are dependent on one another and highly interrelated, and therefore, will be presented together in the next section. The third key issue will be presented in the subsequent section. Collectively, this information did not exist prior to completing this research.

[83] TSA Office of Intelligence, *Mass Transit System Threat Assessment* (Washington, D.C.: Transportation Security Administration, February 2008), 2.

1. Priorities and the Type of Information

The intelligence should focus on risks to the traveling public and critical infrastructure. With the assistance of Amtrak's Office of Security Strategy and Special Operations, the author developed Amtrak's intelligence priorities and requirements based on significant input from corporate and division operating personnel. Key positions were identified in the organization as critical nodes based on their span of control and responsibility. The key positions, or critical nodes, that assisted with the development of Amtrak's intelligence priorities and requirements are: Vice President Transportation, Chief Engineer, Chief Mechanical Officer, Chief of Police, General Superintendents, Division Engineers, Master Mechanics, Deputy Chiefs of Police; and Intelligence Officers (the "Critical Nodes"). A total of 33 individuals were consulted who collectively have over 800 years of railroad operating experience.

Table 2 is a compilation of the interview and survey results. Cumulatively, it specifies Amtrak's intelligence priorities and requirements in the form of questions and the type of information required in each answer. Collectively, the answered questions provide threat information and a detailed image of the operating environment:

Intelligence Priorities & Requirements	
Questions to be Answered	***Types of Information***
1. What natural events will impact Amtrak operations?	• Weather (predicted or actual – flood, hurricane, wildfire, tornado, earthquake, snow, mud slides, excessive heat or cold, etc.)
2. What infrastructure events will impact Amtrak operations?	• Fire/Explosion (accidental or equipment failure) • Accidents adjacent to/in vicinity of right-of-way (e.g., gasoline tanker accident on adjacent highway) • HAZMAT incidents adjacent to/in vicinity of right-of-way (e.g., gas leaks) • Loss of power • Construction/mandated closures (structural, not security related closures) • Military movements/activities (e.g., missile launches from Vandenberg AFB) • Bridge strikes • Movable bridge strikes • Movable bridge failures

Intelligence Priorities & Requirements	
Questions to be Answered	***Types of Information***
	• Derailments • Slow order applications to infrastructure events (e.g., concrete tie replacement, Sperry car, geometry car) • Communication system failures • Signal system failures • Catenary wire down • Broken rail • Theft of property (e.g., copper wire)[84]
3. What anticipated political activities will impact Amtrak operations?	• Movement of VIPs (e.g., POTUS movements, Pope's visit to D.C. and NY) • Planned demonstrations (e.g., animal/environmental rights activists protesting near train stations or using rail for transport to/from demonstration site) • Current political issues (e.g., Tibet protests against Olympic torch) • Union strikes (Amtrak and freight) • International incidents/policy decisions that might cause terrorist backlash (e.g., Paris riots; Mohammed media cartoons; Israeli/Arab peace talks/conflicts)

4. What are the threats to transportation nodes in general, and rail nodes in particular?	• International threats
	• Domestic threats
	  o Threats to employees
	  o Threats to passengers
	  o Threats to facilities

5. What events have occurred which would warrant increased vigilance by Amtrak?	• International terrorist attacks against transportation facilities • Domestic terrorist attacks
6. What criminal activities will impact Amtrak operations?	• Trespassing • Vandalism damaging critical infrastructure • Sabotage • Assault of Amtrak employees • Theft (e.g., recent theft of copper electrical traction returns) • Arson • Bomb threats

[84] Railroads have recently experienced an increase in the theft of copper wire cables. The cables are used in operationally vital systems such train control (signal) and communication as well as electrical traction power systems. The perpetrators sell the cables at scrap metal dealers for the value of the copper, which has risen significantly in recent months.

Intelligence Priorities & Requirements	
Questions to be Answered	***Types of Information***
7. What domestic or international terrorist organizations are planning on attacking domestic rail facilities, and where will they attack?	• Left-wing terrorism • Right-wing terrorism • Single issue (e.g., Earth Liberation Front (ELF) or Animal Liberation Front (ALF)) terrorism • Ethnic terrorism • Religious terrorism (e.g., Islamic radicalization)
8. What terrorism indicators have occurred?	• Surveillance (physical/photographic/IT) • Reconnaissance (physical/digital) • Increase in chatter/threats • Trespassing • Theft of security materials (e.g., IDs, uniforms, documents) • Purchase of IED/explosive components • Rehearsals/dry runs • Discovery of suspect devices
9. What terrorism pre-incident indicators have occurred?	• Surveillance o physical and photographic surveillance o Electronic surveillance (e.g., hacking, phishing, systemic information gathering) • Trespassing • Theft of security materials (e.g., IDs, uniforms, documents) • Discovery of suspect devices o Hoax device(s) o Functional IED(s) • Damage to Amtrak assets o Physical infrastructure • Assault of Amtrak employees
10. What public health issues have occurred?	• Geographic flu report • Communicable diseases • Center for Disease Control (CDC) bulletins • Food and Drug Administration (FDA) bulletins

Table 2. Amtrak Intelligence Priorities and Requirements.

2. Multi-Discipline Dissemination

This section will only focus on disseminating intelligence and terrorism information in the railroad operating environment.

The multi-discipline personnel responsible for safely operating the railroad and protecting the infrastructure are the key enablers to effective intelligence information sharing. Frontline operations personnel are the best equipped to provide information that

enhances existing information to a point where it becomes actionable intelligence. They know what is normal and what is not normal, and can easily distinguish significant events from seemingly insignificant events. Frontline railroad personnel are specifically trained and skilled to detect small variations in the physical characteristics of their operating environment.[85] Even with this ability to detect things out of the ordinary, they need to know the suspicious activity of interest, and where to concentrate their efforts. For intelligence to become actionable in the railroad environment:

1. The railroad police, train crew, and station staff must be part of Amtrak's intelligence cycle; and
2. The Division General Superintendents[86] (operations), Division Engineers (infrastructure), Master Mechanics (rolling stock), and the Police Inspectors must be part of the intelligence cycle with their local intelligence community and law enforcement agencies.

The functional operating characteristics of the railroad environment are the same as Dr. Jerry Ratcliffe's model for intelligence-led policing shown in Figure 7. Multi-discipline front line operating personnel, or intelligence gatherers, *interpret* what they are witnessing in the operating environment. Key decision makers, such as Chief Operating Officers, national operation center personnel, and Division management, are *influenced* by intelligence, and use intelligence to *impact* the operating environment. Ratcliffe refers to this as the 3i model: interpret, influence, and impact.

[85] For example, locomotive engineers must be qualified on the physical characteristics (infrastructure and general geography) before they are permitted to operate a train over a specific territory.

[86] General Superintendents are responsible for all railroad operations in a geographic territory. Amtrak has seven divisions led by seven General Superintendents.

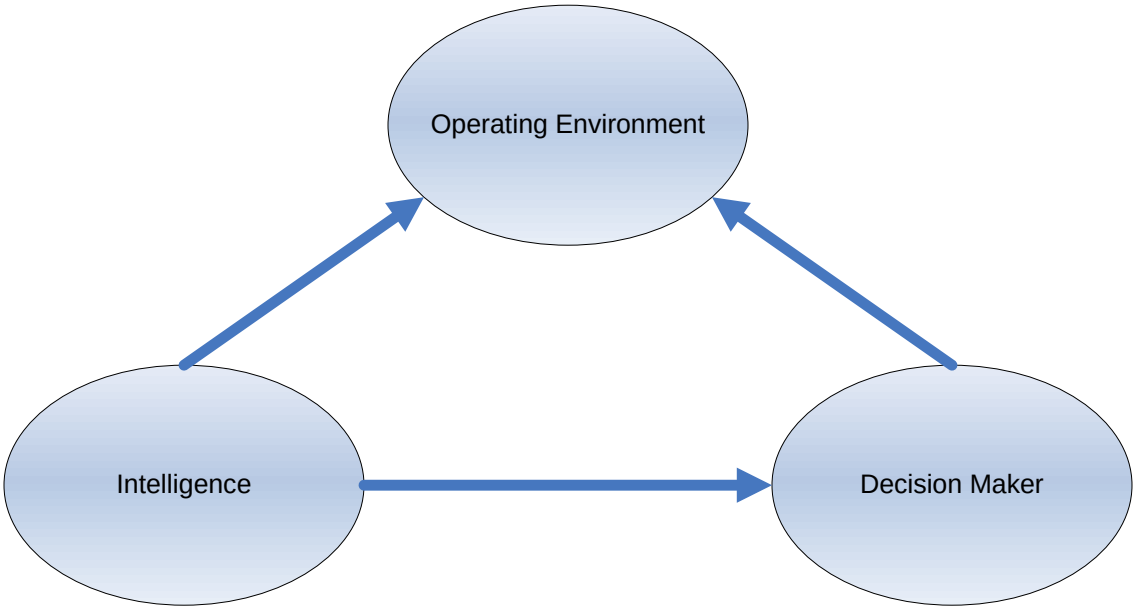


Figure 7. An intelligence-led policing and crime reduction process.[87]

The substantive impact of this model will be to eliminate inconsequential incidents and events, and allow constrained resources to be focused on the events that have potential consequences. The front line work force will be more engaged through a common objective and purpose. This model will alter the traditional paradigm of only allowing the intelligence community or law enforcement to be involved in the intelligence cycle. They will no longer view reporting suspicious activity as yet another task added to their already long list of duties. The workforce will see the results of their input, and become more engaged. By not including all disciplines in the intelligence cycle, valuable information will be overlooked, and a significant resource of information will remain untapped.

In order to provide actionable intelligence and terrorism information at all levels in the corporation, the intelligence briefings and reports must be disseminated as follows:

[87] Jerry H. Ratcliffe, "Intelligence-led Policing Australian Institute of Criminology," *Trends & Issues in Crime and Criminal Justice*, 248 (April 2003): 3.

1. As part of the General Bulletin Order (GBO) and Daily Bulletin Order (DBO)[88] when warranted;
2. National Operation Center (NOC) management (Chief of Systems Operations, Directors of Systems Operations, etc.) shall be provided a daily briefing on the intelligence information relevant for the entire system;
3. Division management (General Superintendent, Division Engineer, Master Mechanic, etc.) shall be provided a daily briefing on the intelligence information relevant to their geographic territory, but in the context of the global threat of terrorism to the system;
4. Train Dispatch Center management (Superintendent Operations, Assistant Superintendent Train Movements, etc.) shall be provided a daily briefing on the intelligence information relevant to their geographic territory, but in the context of the global threat of terrorism to the system;
5. The Chief Operating Officer shall be provided a daily briefing that summarizes intelligence information for the system;
6. The Security Governance Council[89] shall be provided a briefing at its monthly meeting that summarizes intelligence information trends; and
7. The Board of Directors shall be provided an intelligence information briefing at its monthly meeting that summarizes intelligence information trends.

As each level of the organization consumes the intelligence information, they should be required to provide feedback on the usefulness and how well it meets the defined requirements.

C. SUMMARY

This chapter defined Amtrak's intelligence and terrorism information priorities and requirements (Table 2) including dissemination criteria. It specifically established:

[88] Bulletin orders contain special instructions that modify the normal operating rules for a specific geographic area. They also contain general information related to the operation such as speed restrictions, weather, special train movements, a safety rule of the day, and security information. In accordance with federal law and the corporation's operating rules, all operating personnel are required to read and understand the orders before engaging and assuming their responsibilities for that tour of duty (shift).

[89] Amtrak's Security Governance Council is chaired by the President & CEO, and includes the following officers of the corporation: the Chief Operating Officer, Chief Financial Officer, Vice President – Office of Security Strategy & Special Operations, and the General Counsel & Corporate Secretary.

- The nature of the information required to protect the public and critical infrastructure;
- The critical pathways for intelligence in an effective system; and
- The critical nodes and decision makers that require timely intelligence to protect the public and critical infrastructure.

The next chapter will present a case study on the NYPD SHIELD operation and intelligence products as a potential means of fulfilling these requirements, and evidence of the strength of informal megacommunity networks.

V. NYPD SHIELD CASE STUDY

A. OVERVIEW OF NYPD SHIELD

NYPD SHIELD is regarded by the intelligence, law enforcement, and private sector communities as a leading, but sometimes controversial, model for intelligence and terrorism information sharing between the public and private sectors. Between January and May 2008, the author performed a case study on the NYPD SHIELD operation. The author toured the NYPD SHIELD headquarters and interviewed key personnel on the operation. The documentation acquired and the collected testimonial data collected was qualitatively analyzed and compared with Amtrak's intelligence requirements as presented in Chapter IV.

On February 8, 2008, the author met with Inspector Peter Winski (Executive Director, Counterterrorism Division, NYPD) and other Counterterrorism Division staff to be briefed on the NYPD SHIELD operation. Detective Charles Ambio presented an overview of the NYPD SHIELD operation, and provided the author with detailed written information on the initiative.[90] The following summarizes the information acquired at the February 2008 meeting, and subsequent discussions with Inspector Winski and Detective Ambio.

The NYPD SHIELD program is a public-private partnership based on information sharing that specifically seeks assistance from the private sector with the sole purpose of safeguarding the city. The current staffing includes one lieutenant, two sergeants, and four detectives, which is surprisingly small considering NYPD SHIELD's measureable accomplishments. The membership is comprised of both public and private organizations such as financial institutions, cultural institutions, hotels, hospitals, law enforcement

[90] On February 8, 2008, NYPD Detective Charles Ambio provided the author with a binder that contained a detailed overview presentation on NYPD SHIELD; links to relevant Internet information; *Threat Analysis* presentations for three recent terrorist attacks; the NYPD SHIELD Course Catalog for *Corporate & Private Sector Training*; a sample *Vetting Report* for Vornado Realty Trust; sample NYPD SHIELD alerts; positive domestic and foreign news articles on NYPD and the SHIELD operation; and letters of commendation from private sector corporations.

(federal, state, and local), and government agencies (federal, state, and local). They currently have 4,325 members representing 1,897 organizations in 46 U.S. states and 12 countries. The membership and organizations are divided into the following 22 sectors:

- Business Improvement Districts (BIDS)
- Cultural
- Energy/Utilities
- Finance & Banking
- Health & Hospitals
- Law Enforcement
- Media
- Professional Services
- Religious
- Security
- Transportation
- Chemical/Petroleum
- Education
- Entertainment
- Governmental Agencies
- Hospitality & Tourism
- Maritime
- Postal/Parcel
- Real Estate & Property Management
- Retail/Merchant
- Telecommunications/IT
- Other

NYPD SHIELD offers sector specific briefings, conferences, training, an information sharing website, and alerts. In return for these services, they ask the members to be the NYPD's eyes and ears as well as share their personal knowledge on their neighborhood and critical infrastructure.

1. Sector Specific Briefings and Conferences

The sector specific briefings and conferences inform members of the current threat posture in New York City, and advise them of specific initiatives and the role of each sector. The briefings focus on the security challenges for each sector. As of February 2008, a total of 590 members attended eight briefings focused on the hotel, health and hospital, and transportation sectors. The conferences facilitate information sharing and provide a platform for networking between the members within a sector. They are scheduled about every 8 to 10 weeks at NYPD headquarters. Each conference last approximately 90 minutes, and is focused on current and emerging threats. The proceedings are distributed at the conference and posted on the secure NYPD SHIELD website. Past topics have included attack and plot analysis, terrorist methods of operation,

and emerging threats such as the role of women in jihad and the homegrown threat. As of February 2008, NYPD SHIELD has held 10 conferences with 2,720 members in attendance.

2. Training

NYPD SHIELD currently offers training on critical infrastructure protection, terrorism awareness, vehicle borne improvised explosive devices (VBIEDs), and detecting hostile surveillance. The five-day critical infrastructure protection course is aimed at corporate and private security directors and managers. The course content includes the principles of risk assessment, basic methods of security, and the major components of a municipality's infrastructure. The terrorism awareness course is a two to four hour session for security professionals that covers an introduction to terrorism, improvised explosive devices (IEDs), indicators of suicide attacks, and vehicle borne improvised explosive devices. The four-hour VBIED course is aimed at the security professional. The course content includes an introduction to VBIEDs, threat assessments, and search techniques. The detecting surveillance course is a four-hour session for corporate and private security directors and managers. NYPD SHIELD has fulfilled 260 of the 530 training requests received since the program began in August 2005. Over 40% of these requests are for the critical infrastructure protection course. They have held 197 terrorism awareness sessions, 31 VBIED sessions, 20 critical infrastructure protection sessions, and 12 detecting hostile surveillance sessions. Since the program's inception, a total of 7,377 individuals have been trained with representatives from the following organizations:

- McGraw Hill
- Circle Line Cruise
- SIAC
- Metro-Tech BID
- Con Edison
- NY Cruise Line
- Time Warner Center
- Queens Mall
- Yankee and Shea Stadiums
- Goldman Sachs
- NY Waterway
- NYC Department of Parks and Recreation
- Real Estate Board of NY
- Morgan Stanley
- Times Square Alliance
- Battery Park City Authority
- Hunts Point Public Safety
- Staten Island Ferry
- Vornado Reality

3. Website

The NYPD SHIELD website serves three functions: (1) it allows individuals to apply for membership; (2) it facilitates information sharing; and (3) it allows members to request training. The home page includes a security news ticker that searches 12,000 sources from over 125 countries for relevant items of interest. It also includes links to best practices, intelligence and analysis briefings, past conference presentations, weekly newsletters, terrorism digests, and a resource library. Figure 8 shows the home page.

Figure 8. NYPD Internet home page – April 14, 2008.[91]

[91] NYPD, "NYPD SHIELD," *NYPD Counterterrorism Bureau*, http://www.nypdshield.org/public/ (accessed April 14, 2008).

4. Intelligence and Analysis Briefings

NYPD SHIELD intelligence and analysis briefings cover worldwide terrorist attacks and include information on the incident, an in-depth analysis by NYPD Counterterrorism Division analysts, and the potential implications for New York City. The Mumbai Railway Bombings briefing is included in Appendix B as an example. The bombings occurred on July 11, 2006, and the first briefing was released the same day with an update issued on July 17, 2006. A conference was held on July 19, 2006 that included a teleconference with an NYPD Lieutenant on the scene.

5. Resource Library

The NYPD SHIELD website includes access to a resource library that provides terrorism related documents and links to various types of security (air travel, facility, information, etc.), and general research and reference material. The resource library includes downloadable tactical material such as a bomb threat checklist, a list of suspicious package indicators, brochures on Nexus[92] and the Corporate Emergency Access System (CEAS)[93], and a criminal description sheet.

6. SHIELD Alerts

NYPD SHIELD alerts are sent via e-mails to requesting members. The subject matter includes major incidents, suspicious packages, building evacuations, major demonstrations, parades, bank robberies, transit disruptions, weekend events, and rush hour traffic. Oddly, the e-mails are only sent weekdays between the hours of 7:30 AM and 8:00 PM. Alert information is sourced from NYPD Operations, Traffic Management, the Public Information Office, and the Office of Emergency Management as well as news feeds.

---

[92] NEXUS is a Customs and Border Patrol (CBP) trusted traveler program that "Provides expedited travel via land, air or sea to approved members between the U.S. and Canada border." http://www.cbp.gov/xp/cgov/travel/trusted_traveler/ (accessed April 20, 2008).

[93] "CEAS is a pre-event credentialing program, which authenticates critical business employees for access to restricted areas following a disaster or serious emergency using a secure identification card recognized by the police." http://ceas.com/ (accessed April 20, 2008).

B. NYPD PERSPECTIVE

1. Protecting the City

During the February 8, 2008 briefing session, Detective Ambio explained that the primary goal of NYPD SHIELD is to engage the private sector through information sharing with the sole purpose of leveraging the private sector resources to help protect the city. He went on to explain that although it was important to meet and brief the private sector executives, their real objective is to establish a relationship with frontline security and operations personnel. According to Detective Ambio, "the private security guard knows the routine of their environment. The operating personnel can quickly identify the critical assets, and know the vulnerabilities in their business."[94] With a small amount of training, private sector personnel can be an invaluable source of information, and a significant counterterrorism resource.

2. Protecting the City through Intelligence Information

On February 27, 2008, the Northeast Corridor Coalition[95] had their quarterly meeting in New York. In attendance were NYPD Commissioner Ray Kelly, the author, and representatives from the major law enforcement agencies along Amtrak's Northeast Corridor. The NYPD provided a detailed and comprehensive unclassified (for official use only) briefing as part of the meeting. The author observed that it fulfilled a general need for intelligence and terrorism information by the participants. It provided relevant and timely fact based information in the context of the terrorist threat to New York, the major east coast cities, and the country. They clearly stated what they knew, and what they did not know. The NYPD share the information with many other similar groups or coalitions that include state and local representatives as well as the private sector.

---

[94] Detective Ambio (Detective, New York City Police Department), interview with the author, New York, NY, February 8, 2008.

[95] The essence of this coalition is collaboration between Amtrak and state and local law enforcement agencies for the sole purpose of providing a larger presence in stations and on-board our trains. It has been functioning for almost two years and a significant increase in law enforcement presence at stations and on-board our trains along the Northeast Corridor has been seen at no additional expense to Amtrak.

In a private session with Commissioner Kelly, the author asked why he stationed NYPD personnel overseas to gather intelligence as this is not a traditional role for a municipal police department. The Commissioner explained that if they can get unfiltered information quicker, they may be able to turn it into valuable intelligence that saves lives in New York City. In Kelly's opinion, it is necessary to be at the source to get unfiltered information.[96] He made this abundantly clear to the nation with this statement:

> We need the information. We're a city, the only U.S. City, of course, that's been attacked, twice successfully, by terrorists. We can't rely solely on other agencies to protect us here. So there's nothing like self-help, and that's what we're doing.[97]

Clearly, Commissioner Kelly has very little confidence the intelligence community will share timely intelligence. According to Inspector Winski, the converse is not true. Intelligence acquired by NYPD is shared with the FBI and State Department overseas. When it reaches New York, it is shared with the FBI JTTF.[98]

NYPD Inspector Winski, similarly, expressed the importance of source credibility in an interview with the author on February 8, 2008. The example he provided was an August 10, 2007 threat to Washington, D.C. and New York City involving a radiological device (dirty bomb). The source was initially deemed to be credible with the threat intelligence being provided by the New York FBI JTTF. At the direction of Commissioner Kelly, radiological detectors and personnel were deployed at the access roads leading to Manhattan in an attempt to create a secure perimeter. The objective was to have all vehicles pass through a radiological detection screening process before entering the core of the city. Over the course of the ensuing weekend, the credibility of the source waned and was ultimately deemed to be not credible by the FBI JTTF. The countermeasures were withdrawn by early the next week. According to Inspector Winski, "unfiltered information and source credibility is critical in the counterterrorism decision

---

[96] Ray Kelly (Commissioner, New York City Police Department), discussion with the author, New York, NY, February 27, 2008.

[97] Ed Bradley, "Inside the NYPD's Anti-Terror Fight," *60 Minutes*, http://www.cbsnews.com/stories/2006/03/17/60minutes/main1416824.shtml (accessed June 17, 2008).

[98] Peter Winski (Inspector – Executive Director, New York City Police Department), e-mail message to the author, June 17, 2008.

making process."[99] If the source of the intelligence in Inspector Winski's example is initially deemed to be not credible, the cost of deploy equipment and personnel as well as the disruption to the city could have been avoided without a detrimental impact to risk.

C. NYPD SHIELD VS. AMTRAK REQUIREMENTS

Valued by the private sector and non-law enforcement public sector agencies, loathed by the intelligence community and other law enforcement agencies, NYPD SHIELD briefing reports provide a timely tangible report that can be disseminated as part of an effort to lead and motivate a large workforce to remain focused on security. NYPD SHIELD keeps the vigilance drumbeat going and reminds everyone of the ever present threat of terrorism. The NYPD SHIELD incident briefings are controversially valued for the following reasons:

1. No one else is doing what they do;
2. They produce a product within hours of an international or domestic terrorist incident;
3. They are widely disseminated with the lowest level of restrictions;
4. They are brief and to the point;
5. They include relevant background;
6. They include excellent photographs;
7. They include an incident time-line;
8. They are based on the ground truth (fact based);
9. They clearly state what they know and what they do not know; and
10. NYPD SHIELD has credibility whether you like it or not.

The private sector, and a significant portion of the public sector, is ambivalent to who issues the briefing reports within the intelligence community as long as they are accurate, timely, and meet their requirements. NYPD SHIELD is currently the only organization issuing these types of briefings to the private sector.

[99] Peter Winski (Inspector – Executive Director, New York City Police Department), interview with the author, New York, NY, February 8, 2008.

In terms of meeting Amtrak's intelligence priorities and requirements, the NYPD SHIELD briefing reports fall well short. Table 3 compares the NYPD SHIELD briefing reports with Amtrak's intelligence priorities and requirements. This gap analysis shows that only one of the ten questions is routinely answered by their briefing reports. The popularity of the NYPD SHIELD product can only be explained by the demand for intelligence and terrorism information in the private and non-law enforcement public sector. Another way to state this argument is to conclude any intelligence information is good intelligence. This is clearly not the case with NYPD SHIELD briefing reports fulfilling Amtrak's intelligence requirements. If the other entities that support and promote NYPD SHIELD briefing reports carefully consider their specific intelligence priorities and requirements, they will also likely conclude the reports do not meet their specific intelligence needs. Their tendency to support and promote the NYPD SHIELD product comes from fulfilling the demand for intelligence information under a constant threat of terrorism, not from fulfilling their intelligence requirements.

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
1. What natural events will impact Amtrak operations?	• Weather (predicted or actual – flood, hurricane, wildfire, tornado, earthquake, snow, mud slides, excessive heat or cold, etc.)	☒
2. What infrastructure events will impact Amtrak operations?	• Fire/Explosion (accidental or equipment failure) • Accidents adjacent to/in vicinity of right-of-way (e.g., gasoline tanker accident on adjacent highway) • HAZMAT incidents adjacent to/in vicinity of right-of-way (e.g., gas leaks) • Loss of power	☒

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• Construction/mandated closures (structural, not security related closures) • Military movements/activities (e.g., missile launches from Vandenberg AFB) • Bridge strikes • Movable bridge strikes • Movable bridge failures • Derailments • Slow order applications to infrastructure events (e.g., concrete tie replacement, Sperry car, geometry car) • Communication system failures • Signal system failures • Catenary wire down • Broken rail • Theft of property (e.g., copper wire)	
3. What anticipated political activities will impact Amtrak operations?	• Movement of VIPs (e.g., POTUS movements, Pope's visit to D.C. and NY) • Planned demonstrations (e.g., animal/environmental rights activists protesting near train stations or using rail for transport to/from demonstration site) • Current political issues (e.g., Tibet protests against Olympic torch) • Union strikes (Amtrak and freight)	

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• International incidents/policy decisions that might cause terrorist backlash (e.g., Paris riots; Mohammed media cartoons; Israeli/Arab peace talks/conflicts)	
4. What are the threats to transportation nodes in general, and rail nodes in particular?	• International threats • Domestic threats o Threats to employees o Threats to passengers o Threats to facilities	☒
5. What events have occurred which would warrant increased vigilance by Amtrak?	• International terrorist attacks against transportation facilities • Domestic terrorist attacks	☑
6. What criminal activities will impact Amtrak operations?	• Trespassing • Vandalism damaging critical infrastructure • Sabotage • Assault of Amtrak employees • Theft (e.g., recent theft of copper electrical traction returns) • Arson • Bomb threats	☒
7. What domestic or international terrorist organizations are planning on attacking domestic rail facilities, and where will they attack?	• Left-wing terrorism • Right-wing terrorism • Single issue (e.g., ELF or ALF) terrorism • Ethnic terrorism • Religious terrorism (e.g., Islamic radicalization)	☒
8. What terrorism indicators have occurred?	• Surveillance (physical/photographic/IT) • Reconnaissance (physical/digital) • Increase in chatter/threats • Trespassing	☒

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• Theft of security materials (e.g., IDs, uniforms, documents) • Purchase of IED/explosive components • Rehearsals/dry runs • Discovery of suspect devices	

9. What terrorism pre-incident indicators have occurred?	• Surveillance
	  o physical and photographic surveillance
	  o Electronic surveillance (e.g., hacking, phishing, systemic information gathering)
	• Trespassing
	• Theft of security materials (e.g., IDs, uniforms, documents)
	• Discovery of suspect devices
	  o Hoax device(s)
	  o Functional IED(s)
	• Damage to Amtrak assets
	  o Physical infrastructure
	• Assault of Amtrak employees	

11. What public health issues have occurred?	• Geographic flu report • Communicable diseases • CDC bulletins • FDA bulletins	

Table 3. NYPD SHIELD Reports vs. Amtrak Intelligence Priorities and Requirements.

NYPD SHIELD, however, should be recognized as a leader in intelligence and terrorism information sharing. They are, and continue to be, the catalyst in the paradigm shift from law enforcement agencies traditionally reluctant to share information outside of their circles to one that shares with other non-law enforcement public sector entities,

the private sector, and the intelligence community. NYPD SHIELD punched a hole in the wall of separation[100] between law enforcement, the intelligence community, and the private sector.

D. THE NYPD SHIELD MEGACOMMUNITY

The earlier sections in this chapter presented a detailed case study on the NYPD SHIELD operation and the intelligence products they disseminate to their members. It included Commissioner Kelly's and NYPD's perspective on protecting the city through intelligence sharing which, as expected, was focused on detecting and deterring another terrorist attack. The case study concluded with an analysis on how well their briefing products fulfill Amtrak's intelligence priorities and requirements. The analysis showed that the incident briefings met only one of Amtrak's ten requirements, but noted that NYPD SHIELD initiated a controversial paradigm shift in intelligence sharing. A list of the top ten reasons as to why their incident briefings are valued by the public and private sectors was also presented. Although this list provides some anecdotal evidence, the real value innovation is their network of government, business, and civil society members. Without realizing it, NYPD SHIELD created a megacommunity. They have strong and weak ties with state and local government agencies, critical private sector businesses, and neighborhood groups. The 22 sectors listed earlier are repeated in Figure 9, but categorized by government, business, or civil society. Again, the position of each entity relative to each other is not important. What is important is the assigned group.

[100] William P. Barr, "Statement of William P. Barr to the National Commission on Terrorist Attacks Upon the United States," *National Commission on Terrorist Attacks Upon the United States*, http://govinfo.library.unt.edu/911/hearings/hearing6/witness_barr.htm (accessed February 29, 2008).

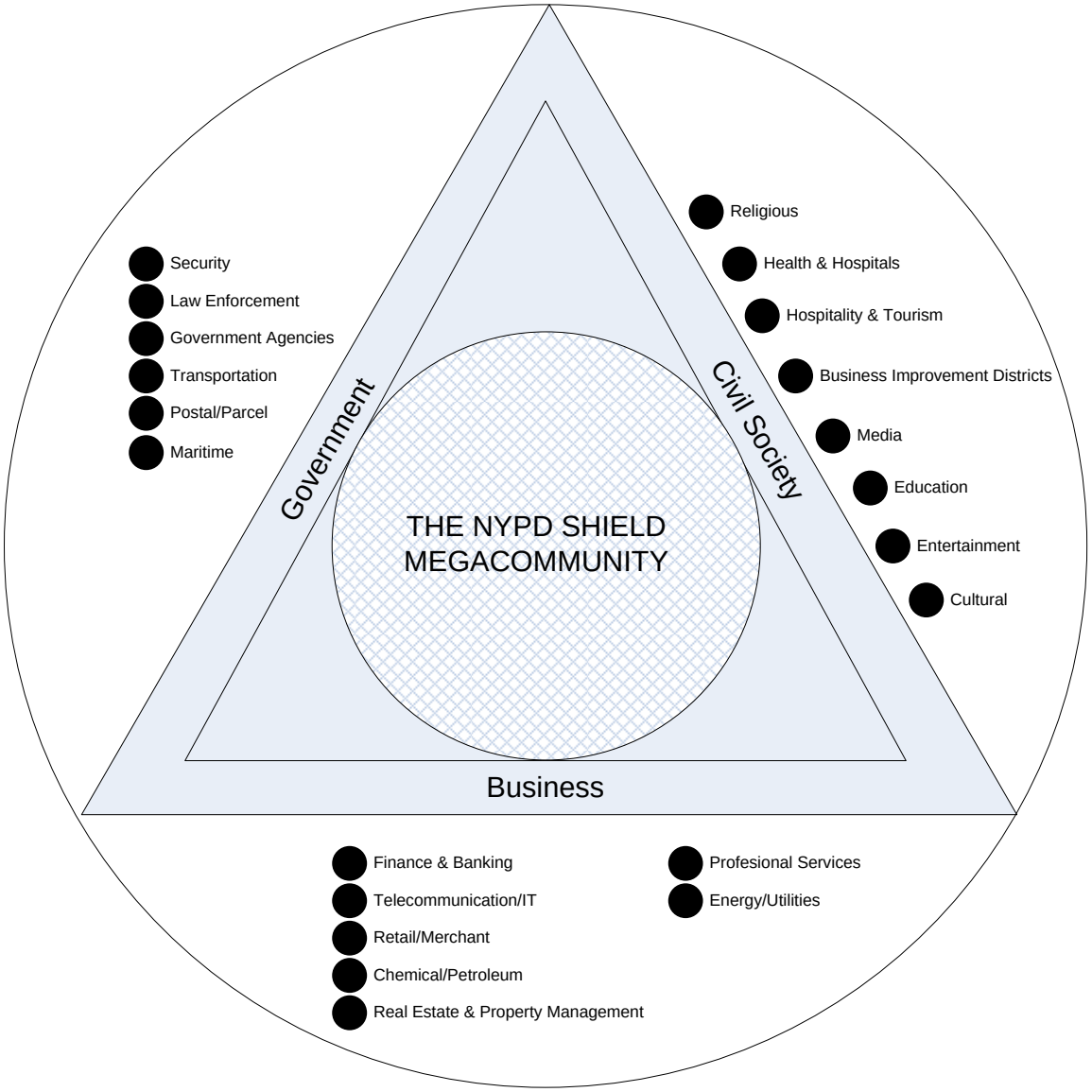


Figure 9. The NYPD SHIELD megacommunity.

NYPD SHIELD built a network of strong and weak ties by hosting sector specific briefings and conferences, providing free onsite training, and direct discussions with the key leadership and front line personnel of state and local governments, private businesses and neighborhood groups. All of this was done without codifying the network. NYPD SHIELD continues to fill a void, and in return, all that is asked is if something is seen, say something. It is a simple social contract built on trust that acts as a catalyst for growing a vast network engaged in intelligence sharing.

E. SUMMARY

This chapter presented a case study on the NYPD SHIELD operation and intelligence products as a potential means of fulfilling Amtrak's intelligence and terrorism information priorities and requirements. The analysis concluded that:

- NYPD SHIELD initiated, and continues to be the catalyst in the paradigm shift from a reluctance to share information with the private sector to intelligence collaboration between the public and private sectors;
- The NYPD SHIELD incident briefings are controversially valued for the following reasons:
    1. No one else is doing what they do;
    2. They produce a product within hours of an international or domestic terrorist incident;
    3. They are widely disseminated with the lowest level of restrictions;
    4. They are brief and to the point;
    5. They include relevant background;
    6. They include excellent photographs;
    7. They include an incident time-line;
    8. They are based on the ground truth (fact based);
    9. They clearly state what they know and what they do not know; and
    10. They have credibility whether you like it or not.
- The NYPD SHIELD briefing reports only meet one of Amtrak's ten intelligence priorities; and
- NYPD has demonstrated what can be accomplished in a community network built solely on trust.

The next chapter will present a case study on the British Transport Police (BTP) Counterterrorism briefing report as a potential example of an intelligence product that could fulfill the intelligence priorities and requirements defined in Chapter IV.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. BRITISH TRANSPORT POLICE MODEL

A. BTP COUNTERTERRORISM UNIT BRIEFING REPORT VS. AMTRAK REQUIREMENTS

With only one of the ten Amtrak intelligence requirements met by the NYPD SHIELD briefing reports, the author researched other intelligence reports more specific to passenger rail. One potential model is the British Transport Police (BTP) Counterterrorism Unit briefing shown in Appendix C. Although the BTP Counterterrorism briefing report, and the information it contains, is specific to British Rail, a comparative analysis of the model, framework, and type of information with Amtrak's intelligence and terrorism information requirements is valuable in the development of Amtrak's intelligence information doctrine. Table 4 compares the BTP Counterterrorism Unit briefing reports with Amtrak's intelligence priorities and requirements. This gap analysis shows that five of the ten questions are routinely answered by their briefing reports.

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
1. What natural events will impact Amtrak operations?	• Weather (predicted or actual – flood, hurricane, wildfire, tornado, earthquake, snow, mud slides, excessive heat or cold, etc.)	☒
2. What infrastructure events will impact Amtrak operations?	• Fire/Explosion (accidental or equipment failure) • Accidents adjacent to/in vicinity of right-of-way (e.g., gasoline tanker accident on adjacent highway) • HAZMAT incidents adjacent to/in vicinity of right-of-way (e.g., gas leaks)	☒

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• Loss of power • Construction/mandated closures (structural, not security related closures) • Military movements/activities (e.g., missile launches from Vandenberg AFB) • Bridge strikes • Movable bridge strikes • Movable bridge failures • Derailments • Slow order applications to infrastructure events (e.g., concrete tie replacement, Sperry car, geometry car) • Communication system failures • Signal system failures • Catenary wire down • Broken rail • Theft of property (e.g., copper wire)	
3. What anticipated political activities will impact Amtrak operations?	• Movement of VIPs (e.g., POTUS movements, Pope's visit to D.C. and NY) • Planned demonstrations (e.g., animal/environmental rights activists protesting near train stations or using rail for transport to/from demonstration site) • Current political issues (e.g., Tibet protests against Olympic torch) • Union strikes (Amtrak and freight)	

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• International incidents/policy decisions that might cause terrorist backlash (e.g., Paris riots; Mohammed media cartoons; Israeli/Arab peace talks/conflicts)	
4. What are the threats to transportation nodes in general, and rail nodes in particular?	• International threats • Domestic threats o Threats to employees o Threats to passengers o Threats to facilities	☑
5. What events have occurred which would warrant increased vigilance by Amtrak?	• International terrorist attacks against transportation facilities • Domestic terrorist attacks	☑
6. What criminal activities will impact Amtrak operations?	• Trespassing • Vandalism damaging critical infrastructure • Sabotage • Assault of Amtrak employees • Theft (e.g., recent theft of copper electrical traction returns) • Arson • Bomb threats	☑
7. What domestic or international terrorist organizations are planning on attacking domestic rail facilities, and where will they attack?	• Left-wing terrorism • Right-wing terrorism • Single issue (e.g., ELF or ALF) terrorism • Ethnic terrorism • Religious terrorism (e.g., Islamic radicalization)	☒
8. What terrorism indicators have occurred?	• Surveillance (physical/photographic/IT) • Reconnaissance (physical/digital) • Increase in chatter/threats • Trespassing	☑

Amtrak Intelligence Priorities & Requirements		
Questions to Answered	***Types of Information***	***Question Adequately Answered?***
	• Theft of security materials (e.g., IDs, uniforms, documents) • Purchase of IED/explosive components • Rehearsals/dry runs • Discovery of suspect devices	

9. What terrorism pre-incident indicators have occurred?	• Surveillance
	  o physical and photographic surveillance
	  o Electronic surveillance (e.g., hacking, phishing, systemic information gathering)
	• Trespassing
	• Theft of security materials (e.g., IDs, uniforms, documents)
	• Discovery of suspect devices
	  o Hoax device(s)
	  o Functional IED(s)
	• Damage to Amtrak assets
	  o Physical infrastructure
	• Assault of Amtrak employees
		☑

10. What public health issues have occurred?	• Geographic flu report • Communicable diseases • CDC bulletins • FDA bulletins	☒

Table 4. BTP CTU Briefing Report vs. Amtrak Intelligence Priorities and Requirements.

B. THE BRITISH TRANSPORT POLICE COUNTERTERRORISM UNIT BRIEFING: A POTENTIAL SOLUTION?

The BTP Counterterrorism Unit briefing is routinely issued for terrorist activity abroad and within their system. The information is more detailed and actionable than the products issued in the U.S., including NYPD SHIELD. The briefings include information on:

1. threat level assessments;
2. legal authority;
3. domestic counterterrorism intelligence including photographs of individuals-of-interest, names, dates of birth, addresses, and incidents;
4. individuals that have a grievance with domestic law enforcement including incident details, photographs, names, dates of birth, and addresses;
5. terrorist tactics;
6. significant terrorism incidents aboard including photographs, maps, names, dates, places and incident details such as timing and delivery method;
7. criminal activity that is used to support terrorism including photographs of individuals-of-interest;
8. standard operating procedures for counter surveillance;
9. counter surveillance observations;
10. reported incidents of suspicious behavior;
11. threats to the rail network; and
12. upcoming events in the area.

The BTP Counterterrorism Unit briefing fits its intended purpose of actionable tactical guidance for their police officers. The intelligence and terrorism information is, for the most part, generated from field information reported using the protocols and systems established during the height of the Irish Republic Army (IRA) bombings within the British rail network. The tactical guidance in the report provides critical intelligence information to the decision and policy makers responsible for developing risk mitigation strategies. It leverages the fact that the British legal system allows investigative

information to be blended with intelligence. The report is updated weekly, and widely disseminated to frontline personnel, but classified "restricted," which is equivalent to the U.S. security sensitive information classification.

A comparative analysis on the threat, culture, governance, agency authority, and laws will be used to determine the applicability of the BTP Counterterrorism Support Unit briefing to Amtrak. As each of the aforementioned areas is a broad topic in-and-of-itself, this analysis will focus only on the relevant facts. It, for example, will not focus on the Constitutional jurisprudence of the *Foreign Intelligence Surveillance Act (FISA)*, but it will discuss the authority of the BTP, and the applicable law as it relates to warrants.

1. The Threat of Terrorism in the United Kingdom

Given the long history of terrorist attacks by the IRA during the 1970s to the late 1990s, the UK is not unfamiliar with terrorism. In a July 2006 strategy for countering international terrorism submitted to Parliament, Prime Minister Blair described the new threat of terrorism as follows:

> The current threat from Islamist terrorism is serious and sustained. It is genuinely international in scope, involving a variety of groups, networks and individuals who are driven by particular violent and extremist beliefs. It is indiscriminate – aiming to cause mass casualties, regardless of the age, nationality, or religion of their victims; and the terrorists are often prepared to commit suicide to kill others. Overall, we judge that the scale of the threat is potentially still increasing and is not likely to diminish significantly for some years.[101]

In the same statement, the Prime Minister made it clear that "The principal current terrorist threat is from radicalised individuals who are using a distorted and unrepresentative version of the Islamic faith to justify violence. . . . They are, however, a tiny minority within the Muslim communities here and abroad. Muslim communities themselves do not threaten our security; indeed they make a great contribution to our

[101] Prime Minister Tony Blair, *Countering International Terrorism: The United Kingdom's Strategy* (London, UK, HM Government, July 2006), 1.

country."[102] In a February 22, 2008 Counterterrorism Support Unit Briefing, the BTP assessed this threat at the *Severe*[103] level or that an attack is highly likely on the railway system.[104]

2. Culture and Multiculturalism

The UK is a multicultural country that is culturally divided. In a December 2006 speech on the duty to integrate, Prime Minister Blair describes the multicultural goal as follows:

> The whole point is that multicultural Britain was never supposed to be a celebration of division; but of diversity. The purpose was to allow people to live harmoniously together, despite their difference; not to make their difference an encouragement to discord. The values that nurtured it were those of solidarity, of coming together, of peaceful co-existence. The right to be in a multicultural society was always, always implicitly balanced by a duty to integrate, to be part of Britain, to be British and Asian, British and black, British and white.[105]

Britain's vision of a multicultural society may be one of harmony and unity, but the statistical data clearly shows a country that is divided along racial, ethnical, and religious lines. The following is a brief summary of some relevant statistics from the 2001 census:[106],[107],[108]

---

[102] Prime Minister Tony Blair, *Countering International Terrorism: The United Kingdom's Strategy* (London, UK, HM Government, July 2006), 1.

[103] The UK uses a threat level indicator with five levels: *Low – an attack is unlikely; Moderate – an attack is possible, but not likely; Substantial – an attack is a strong possibility; Severe – an attack is highly likely; and Critical – an attack is expected imminently.*

[104] British Transport Police, *Counterterrorism Support Unit Briefing* (London, UK: British Transport Police, February 22, 2008), 3.

[105] Prime Minister Blair, "Our Nation's Future – Multiculturalism and Integration," Number 10 Downing Street, http://www.number-10.gov.uk/output/page10563.asp (accessed February 29, 2008).

[106] National Statistics, *Focus on Ethnicity and Religion* (Newport, UK: Office of National Statistics, 2006).

[107] National Statistics, "Age & Sex Distribution," *National Statistics – Focus on Religion*, http://www.statistics.gov.uk/cci/nugget.asp?id=955 (accessed February 29, 2008).

[108] National Statistics, *Focus on Religion – 2004 Summary Report* (Newport, UK: Office of National Statistics, 2004).

- Total population of Great Britain is 57.1 million
- 92% of the population is white with the remaining 8% comprised of:
    - 4.0% Asian
    - 2.0% Black
    - 1.2% Mixed – white/black/Caribbean, white/black/African, white/Asian
    - 0.4% Chinese
- The largest ethnic groups within the population of Great Britain are:
    - 1.8% Indian
    - 1.3% Pakistani
    - 1.0% Black Caribbean
    - 0.8% Black African
- The top four religious groups within the population of Great Britain are:
    - 71.8% Christian
    - 15.1% No religion
    - 7.8% Religion not stated
    - 2.8% Muslim
- 70% of the Muslim population within Great Britain is under the age of 34
- Muslims rank the lowest in terms of social and economic status:
    - Muslims have the largest households with an average of 3.8 people per household compared to 2.3 for Christians
    - 34% of Muslim households contain five or more people
    - 32% of Muslim households were considered to be living in overcrowded accommodations
    - 31% of working age Muslims do not have any educational qualifications
    - 14% and 15% of Muslim men and women, respectively, are unemployed compared to 4% and 4% of Christian men and women, respectively

    - 30% of Muslim men are economically inactive compared to 16% of Christian men
    - 68% of Muslim women are economically inactive compared to 25% of Christian women
- 38% of Muslims live in London

Figure 10 shows the geographic distribution of Christians and Muslims in Great Britain. Overlaying these two figures clearly shows the divide between the two largest religious groups. This is particularly true in London, as shown in the inset.

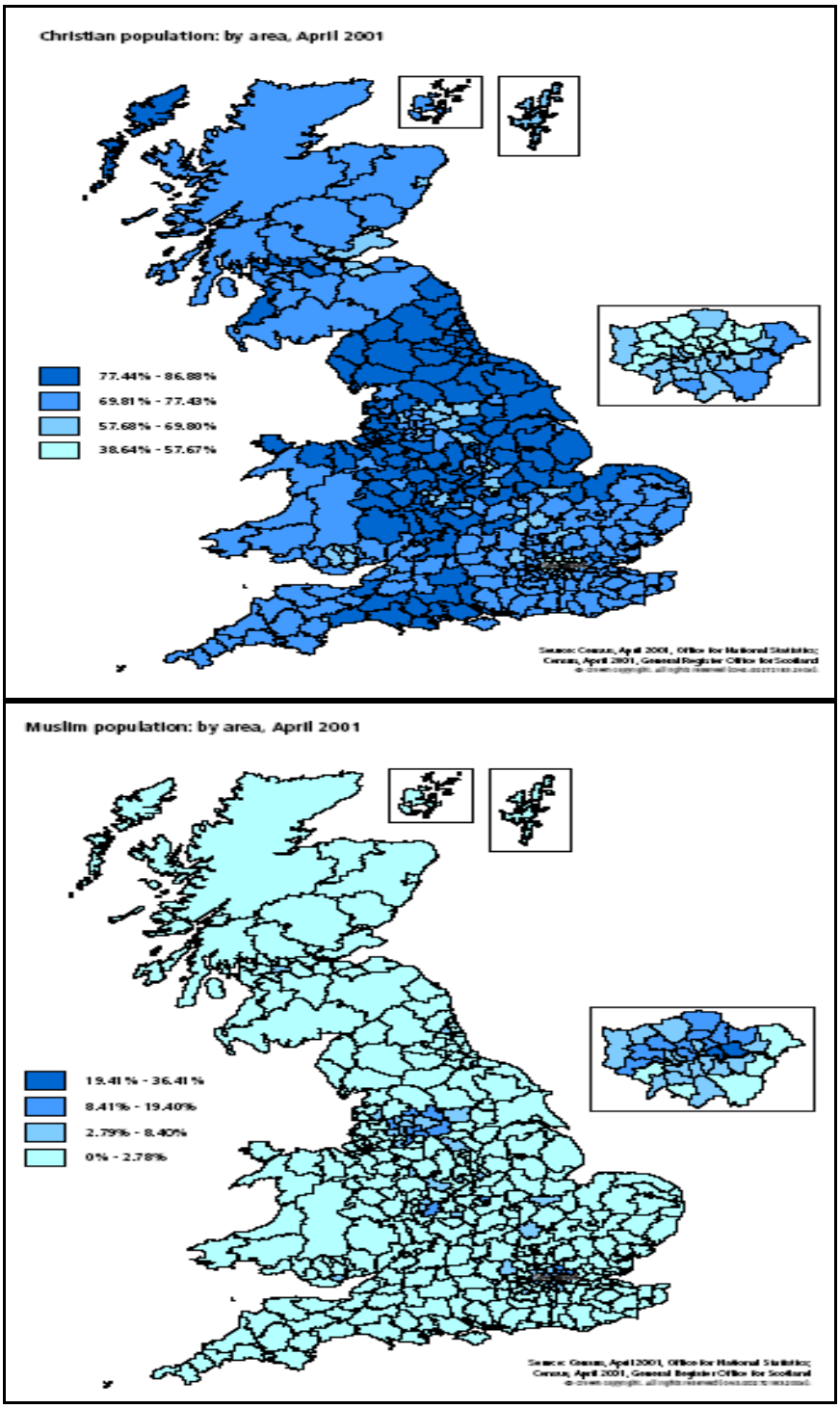


Figure 10. Christian and Muslim population distribution in Great Britain.[109]

[109] National Statistics, "Download Maps: Religion by UA/Local Authority (GB)," *Focus on Religion*, http://www.statistics.gov.uk/statbase/Product.asp?vlnk=13209 (accessed February 29, 2008).

3. Governance

The UK system of government is based on a unitary parliamentary democracy[110] in comparison to the presidential – congressional federalist[111] system in the U.S. The difference between the two systems is defined by the location of the executive power. In the British system, it resides in the Cabinet, and in the U.S., it resides with the President. The British Prime Minister is elected by winning a majority of seats in the House of Commons. The elected Prime Minister of the majority party forms a Cabinet from the elected members of Parliament. The authority of the Cabinet, and support from the majority in the House of Commons, assures the Prime Minister that legislation, and new policy put forth by the majority party controlled Ministries is passed. Whereas, in the U.S., legislation must be passed by an independently elected Senate and House before going on to conference, and approval by the President.

In the framework of counterterrorism, homeland security, and civil liberties, the fundamental difference between the UK and U.S. systems of government is the absence of a written constitution specifying the rights of the people in the UK system. The British Parliament has final authority and looks to Acts of Parliament, standards, and long-standing traditions for the basis of their governance. The U.S. Supreme Court has final authority over the constitutionality of U.S. laws including those involving counterterrorism, homeland security, and civil liberties. This difference is further highlighted by the Fourth Amendment to the U.S. Constitution:

> 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.[112]

---

[110] The Oxford dictionary definition of unitary is *a political system that advocates national or political unit.*

[111] The Oxford dictionary definition of federalism is *a political system that favors a strong central government.*

[112] United States Congress, "The Constitution of the United States," 22nd Edition of the Pocket Version (Washington: U.S. Government Printing Office, 2006), 22.

The amendment presumes that a search or seizure is unreasonable unless a warrant has been issued by the court after showing probable cause on a case-by-case basis. Whereas, under the British system of government, Parliament has enacted laws that effectively delegate this authority to the police if they have reasonable suspicion that a crime has been, or is about to be committed.

4. Agency Authority & Laws

The BTP has its roots in the law enforcement divisions of the railway companies formed in the 19th century by the British Parliament. (If there is interest in this history, the BTP website[113] is recommended as a good introduction to the topic.) The 1949 *British Transport Commission Act* brought the various railway police organizations under the control of the British Railways Board (BRB). The BTP is responsible for policing the railways[114] in Great Britain as well as the London Underground, the Docklands Light Railway, Croydon Tramlink, and the Midland Metro, which are considered tramways.[115] The BTP's geographic area of responsibility includes England, Scotland, and Wales, but not Northern Ireland. Its oversight agency is the British Transport Police Authority (BTPA), which is currently a 13-member board that reports to the Secretary of State for the Home Department. Figure 11 depicts the details of these relationships.

---

[113] British Transport Police, "BTP History Archive," http://www.btp.police.uk/History%20Society/history%20society%20main.htm (accessed February 24, 2008).

[114] Britain's Transport and Works Act of 1992 defines a railway *as a system of transport employing parallel rails which –*

> *(a) provide support and guidance for vehicles carried on flanged wheels, and*
>
> *(b) form a track which either is of a gauge of at least 350 millimeters or crosses a carriageway (whether or not on the same level), but does not include a tramway.* http://www.opsi.gov.uk/acts/acts1992/ukpga_19920042_en_6 (accessed February 24, 2008).

[115] Britain's Transport and Workers Act of 1992 defines a tramway as a system of transport used wholly or mainly for the carriage of passengers and employing parallel rails which,

> *(a) provide support and guidance for vehicles carried on flanged wheels, and*
>
> *(b) are laid wholly or mainly along a street or in any other place to which the public has access (including a place to which the public has access only on making a payment).* http://www.opsi.gov.uk/acts/acts1992/ukpga_19920042_en_6 (accessed February 24, 2008).

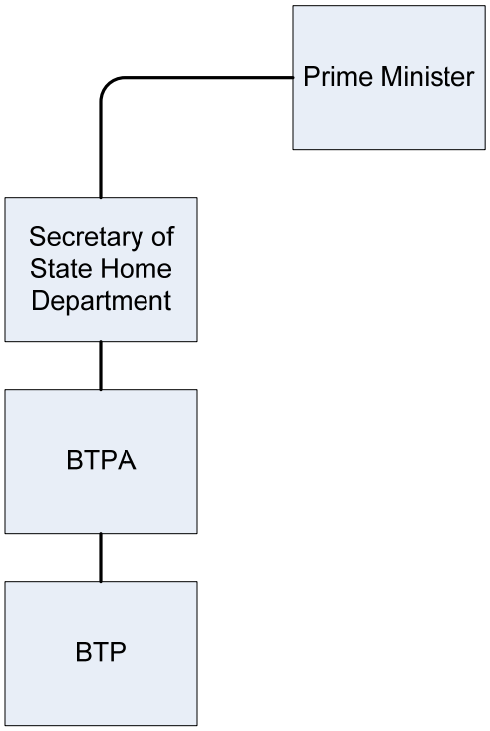


Figure 11. BTP reporting structure.

The *Railways and Transport Safety Act 2003* authorized the establishment of the BTPA and the BTP:

> 20 Establishment of Police Force
>
> The [British Transport Police] Authority shall secure the maintenance of an efficient and effective police Force –
>
> (a) to be known as the British Transport Police Force, and
>
> (b) to police the railways.[116]

Section 31 of the Act specifies the police constables' jurisdiction to include all the powers and privileges of a constable:

> (a) on track,
>
> (b) on network,
>
> (c) in a station,

[116] House of Commons, *Railways and Transport Safety Act 2003 (c.20)*, (London, UK: July 10, 2003), 9.

(d) in a light maintenance depot,

(e) on other land used for purposes of or in relation to a railway,

(f) on other land in which a person who provides railway services has a freehold or leasehold interest, and

(g) throughout Great Britain for a purpose connected to a railway or to anything occurring on or in relation to a railway.[117]

It also grants the police constable authority to enter track, a network, a station, a maintenance depot, and railway vehicles:

(a) without a warrant,

(b) using reasonable force if necessary, and

(c) whether or not an offence has been committed.[118]

The *Anti-terrorism, Crime & Security Act 2001* and the *Police Reform Act 2002* extended these powers beyond the railways, and effectively gave them local police powers:

> (2) Members of the British Transport Police Force have in any police area the same powers and privileges as constables of the police force for that police area—
>
> (a) in relation to persons whom they suspect on reasonable grounds of having committed, being in the course of committing or being about to commit an offence, or
>
> (b) if they believe on reasonable grounds that they need those powers and privileges in order to save life or to prevent or minimise personal injury.[119]

The only conditions the Act prescribes on these powers is that the police constable must be in uniform, have proper identification, and where waiting on a local police constable would frustrate or seriously prejudice the need to exercise the powers.

---

[117] House of Commons, *Railways and Transport Safety Act 2003 (c.20),* (London, UK: July 10, 2003), 14.

[118] Ibid.

[119] House of Commons, *Anti-terrorism, Crime & Security Act 2001,* (London, UK: December 14, 2001), Part 10, Section 100.

C. COMPARATIVE ANALYSIS CONCLUSIONS & JUSTIFICATION

Although the governance, laws, and policing authorities differ between the U.S. and the UK, the global threat of terrorist attacks against passenger rail is the same. In the case of the UK, however, the threat is amplified by the stark cultural, sociological, and economic divide between the Christian and Muslim populations. The BTP Counterterrorism Unit briefing follows Britain's traditional application of intelligence and law enforcement information sharing. Under the *Patriot Act*, the U.S. has significantly shifted its laws and policies towards the long-standing practices of the UK. The intelligence and law enforcement information sharing practices in the two countries is founded in substantively different laws and governance, but they arrive at the same end. Both allow for intelligence and criminal investigation information to be shared between the respective groups under specific circumstances.

D. SUMMARY

This chapter presented a case study on the BTP Counterterrorism Unit briefing as a potential example of the type of intelligence product that could fulfill Amtrak's intelligence priorities and requirements: The analysis concluded that:

- The BTP Counterterrorism Unit briefing fulfills five of the ten intelligence requirements defined in Chapter IV;
- The BTP Counterterrorism Unit briefing is a smart practice[120] that has been successfully applied in a culturally, sociologically, and economically divided country; and
- The BTP Counterterrorism Unit briefing is an example of the type of intelligence product required, but not being produced, in the passenger rail transportation sector.

The next, and final, chapter of this thesis will conclude with recommended resources required to:

1. Produce intelligence products that meet all ten of the requirements using the BTP briefing report as a model; and
2. Implement and execute the strategy proposed in Chapter III.

[120] In *A Practical Guide for Policy Analysis*, Eugene Bardach defines a smart practice as *an expression of some underlying idea – an idea about how the actions entailed by the practice work to solve a problem or achieve a goal.*

THIS PAGE INTENTIONALLY LEFT BLANK

VII. IMPLEMENTING THE STRATEGY

A comparison of Amtrak's intelligence needs against the two dominant intelligence solutions for protecting the public and critical infrastructure shows that a modified BTP system will work best for Amtrak. The BTP Counterterrorism Unit briefing fulfills five of Amtrak's ten intelligence requirements whereas the NYPD SHIELD briefings only fulfill one. The BTP Counterterrorism Unit briefing is a smart practice, and an example of the type of intelligence product required, but not being produced, for the U.S. passenger rail transportation sector. An example of an intelligence product that meets all ten of Amtrak's requirements is shown in Appendix D.

A. AMTRAK'S INTELLIGENCE & TERRORISM INFORMATION UNIT

With the intelligence community and federal, state, and local law enforcement agencies focused and consumed by their respective jurisdictional intelligence requirements, limited resources remain to meet the specific intelligence requirements of the passenger rail transportation sector. Absent adequate external assistance, a dedicated intelligence unit, fully integrated into railroad operations, is urgently required to meet the requirements defined in this thesis. Therefore, it is recommended that an intelligence unit be added to Amtrak's Office of Security Strategy and Special Operations. The duties and responsibilities of this intelligence unit will be focused on five key missions:

1. Be Amtrak's primary source for intelligence products that specifically meet the requirements defined by the foregoing research;
2. Be Amtrak's single point of contact for all threat information from the national intelligence community;
3. Be Amtrak's primary point of contact for collaborative intelligence sharing with state and local law enforcement agencies;
4. Be the passenger rail industry leader in international smart counterterrorism practices; and
5. Be Amtrak's source for federal security clearances.

A minimum of ten (10) qualified intelligence experts who have demonstrated their abilities in all-source intelligence analysis and one (1) qualified expert Facility

Security Officer (FSO) will be assigned to the intelligence unit. The individuals assigned to this unit will possess the necessary experience, skills, and current security clearances required to achieve the five missions successfully. All of the analysts will have experience in passenger or freight rail intelligence and security.

1. Meeting Amtrak's Intelligence Requirements

The first key mission of Amtrak's intelligence unit is to establish and institutionalize the complete intelligence cycle. This includes establishing responsibilities, priorities, methods, procedures, common operation terminology and practices, standard operating procedures (SOPs), classified and unclassified intelligence libraries, record keeping systems, filing procedures, and reporting procedures. It will also include designing and developing intelligence workbooks and databases.

Amtrak's intelligence unit will manage a planning process that includes an initial assessment, preparing templates of specific terrorist courses of action, determining indicators of terrorist activities that support each template, identifying intelligence gaps, periodic reviews to update this planning and management effort. They will also manage Amtrak's intelligence collection plan by identifying intelligence priorities, defining every possible collection source, and determining their capabilities and suitability for each intelligence requirement. They will specifically task and request multiple agencies according to priorities, capabilities, and suitability. The intelligence unit will monitor and manage this plan to ensure information flow continues and supports the collection plan objectives.

The intelligence analysts will process and analyze information by evaluating information for relevancy, urgency, accuracy, and reliability, and by using historical information to develop source profiles. They will record information and compare it to current intelligence holdings, request clarification or substantiating information to assess suspect reports accurately. The intelligence analysts will specifically determine terrorist capabilities, weaknesses and vulnerabilities, strength, composition, disposition, tactics, training, doctrine, and personalities. They will define, assign, and update as required, the appropriate course of action for each piece of information. The intelligence analysts will

disseminate intelligence using appropriate methods to inform the end user. They will ensure that all information is analyzed and its significance clearly articulated in the dissemination method used so that the end user need not guess at its intelligence value.

The intelligence unit will protect and maintain the integrity of all sensitive information for the corporation through the proper handling, storage, marking, and dissemination of all materials. They will obtain and circulate all relevant policies, regulations, orders, and directives regarding the handling and storage of sensitive information. They will establish classification and access controls and compliance procedures commensurate with all applicable references outlined in the foregoing. The intelligence unit will institute a series of checks and balances to ensure all sensitive information is protected accordingly.

2. Liaison with National Level Intelligence Community

This second key mission of Amtrak's intelligence unit is to establish a physical liaison presence at, but not limited to, the following national level intelligence agencies: the ODNI - NCTC, DHS – OI&A, FBI - NJTTF, FBI – JTTF, and other intelligence related organizations and associations such as think tanks, universities, and private sector entities. The intelligence analysts assigned to the national intelligence community will represent Amtrak's intelligence interests at these organizations by establishing personal contacts with key personnel and analysts. They will communicate Amtrak specific intelligence requests and influence the integration of Amtrak specific requirements into the collection activities of these agencies.

The intelligence analysts will also educate key personnel at each organization on Amtrak's specific intelligence needs. They will review the organizations' historical databases, files, and other holdings as well as their current intelligence workflow to identify sources of information relevant to Amtrak's needs. The intelligence analysts will integrate themselves into the workflow of incoming intelligence information to identify immediate, or perishable information relevant to Amtrak. They will also integrate themselves into the workflow of intelligence production to maintain current appreciation of intelligence trends and analyses.

Lastly, as part of this mission, the intelligence analyst will attend briefings, seminars, and meetings as required. The cumulative result of this effort will be used to conduct briefings as defined in Chapter IV.

3. Collaborative Partnerships with Fusion Centers and Local Law Enforcement

The third key mission involves intelligence unit personnel establishing collaborative relationships with federal, state, and local law enforcement officers to facilitate the rapid flow of information relevant to Amtrak's security needs. They will travel to state and local fusion centers and critical law enforcement agencies to brief key personnel on Amtrak's specific needs by explaining the congruency of Amtrak's needs with the law enforcement agency requirements. They will discover the methods, procedures, and capabilities of the various law enforcement agencies, and determine how best to integrate these into the overall intelligence collection plan. The intelligence unit personnel will determine the intelligence holdings and relevancy of current intelligence workflow inputs and products. They will participate in law enforcement training, seminars, and briefings to gather information relevant to Amtrak's security needs. They will also gain access to law enforcement intelligence organizations, agencies, and offices such as NYPD SHIELD that can support Amtrak's security needs.

Intelligence analysts will participate, as necessary, in law enforcement agency intelligence analysis and production efforts. They will informally evaluate each law enforcement agencies level of significance, accuracy, and timeliness in sharing intelligence and information. The historical results are used to make the most of favorable situations or to devote more effort to developing closer ties.

4. Collaborate with Foreign Intelligence and Law Enforcement Agencies

The fourth key mission for the intelligence unit is to travel to foreign countries to establish professional relationships with intelligence and law enforcement agencies that can provide intelligence and historical information (photos, after action reviews, debriefings, interrogation reports, event analyses) on terrorist activities against passenger rail service. The intelligence unit staff will attend international seminars, briefings,

conferences, and reviews that provide awareness and insight into terrorist tactics, techniques, and procedures in foreign countries. They will actively seek out information on opportunities to gain introductions to foreign law enforcement and intelligence personnel who may be visiting the U.S.

The assigned staff will solicit invitations to seminars, briefings, and conferences where they may be guest speakers or in general attendance. The intelligence unit staff will review foreign intelligence and law enforcement periodicals, newspapers, bulletins, and broadcasts to identify key personnel in cooperating countries who may be able to provide information on terrorist tactics, techniques, and procedure used against passenger rail services.

5. Security Clearance Management

The fifth and final key mission of Amtrak's intelligence unit is to administer and manage Amtrak's federal security clearances, and security clearance application program. This includes, but is not limited to, clearance custodial operations, reinvestigation tracking and assistance, and maintenance of National Industrial Security Program Manual (NISPOM) mandated standards (DOD 5220.22-M). They will also verify federal clearances of assigned personnel through multiple federal agencies.

B. DELIVERABLES

Intelligence becomes valuable when it meets the priorities and requirements of the end user or consumer. Analysts must be proficient across a wide spectrum of oral and written methods of dissemination. These disseminated deliverables must be clear, concise, factual, and specifically note the differences between fact, unconfirmed information, and the intelligence expert's analysis or conjecture. The analysts must be capable of providing their analysis in such a manner as to be easily understood by personnel who do not have an intelligence background. Amtrak's intelligence unit will have the capability to prepare any one, or a combination of the following deliverables:

- Formal collection plans
- Intelligence requests
- Organizational capabilities briefings to external agencies
- General intelligence briefings
- Intelligence tasks
- VIP briefings
- Oral and written periodic intelligence summaries
- Spot reports
- PowerPoint presentations
- Funding justification analysis
- Spontaneous oral and written analysis
- White papers
- Decision papers
- Intelligence annexes to plans and orders
- Tactical briefings
- Personnel briefings
- After action report input
- Intelligence training and supporting lesson plans
- Training scenarios
- Red team exercises
- Role playing profiles

C. SUMMARY

The final chapter in this thesis argues that Amtrak is in a unique position, with its well-established relationships at the federal level, in 46 states, and 525 communities, to develop and foster an intelligence and terrorism information sharing network based on the megacommunity framework. It recommends that Amtrak establish an internal intelligence unit to meet the intelligence requirements defined by the foregoing research. It presented five key missions for this new intelligence unit:

- Be Amtrak's primary source for intelligence products;
- Be Amtrak's single point of contact for all threat information from the national intelligence community;
- Be Amtrak's primary point of contact for collaborative intelligence sharing with state and local law enforcement agencies;
- Be the passenger rail industry leader in international smart counterterrorism practices; and
- Be Amtrak's source for federal security clearances.

D. FINAL THOUGHTS

When I set out to write a thesis on public – private sector intelligence and terrorism information sharing some 18 months ago, I had two underlying objectives: (1) to develop an effective strategy for intelligence and terrorism information sharing within

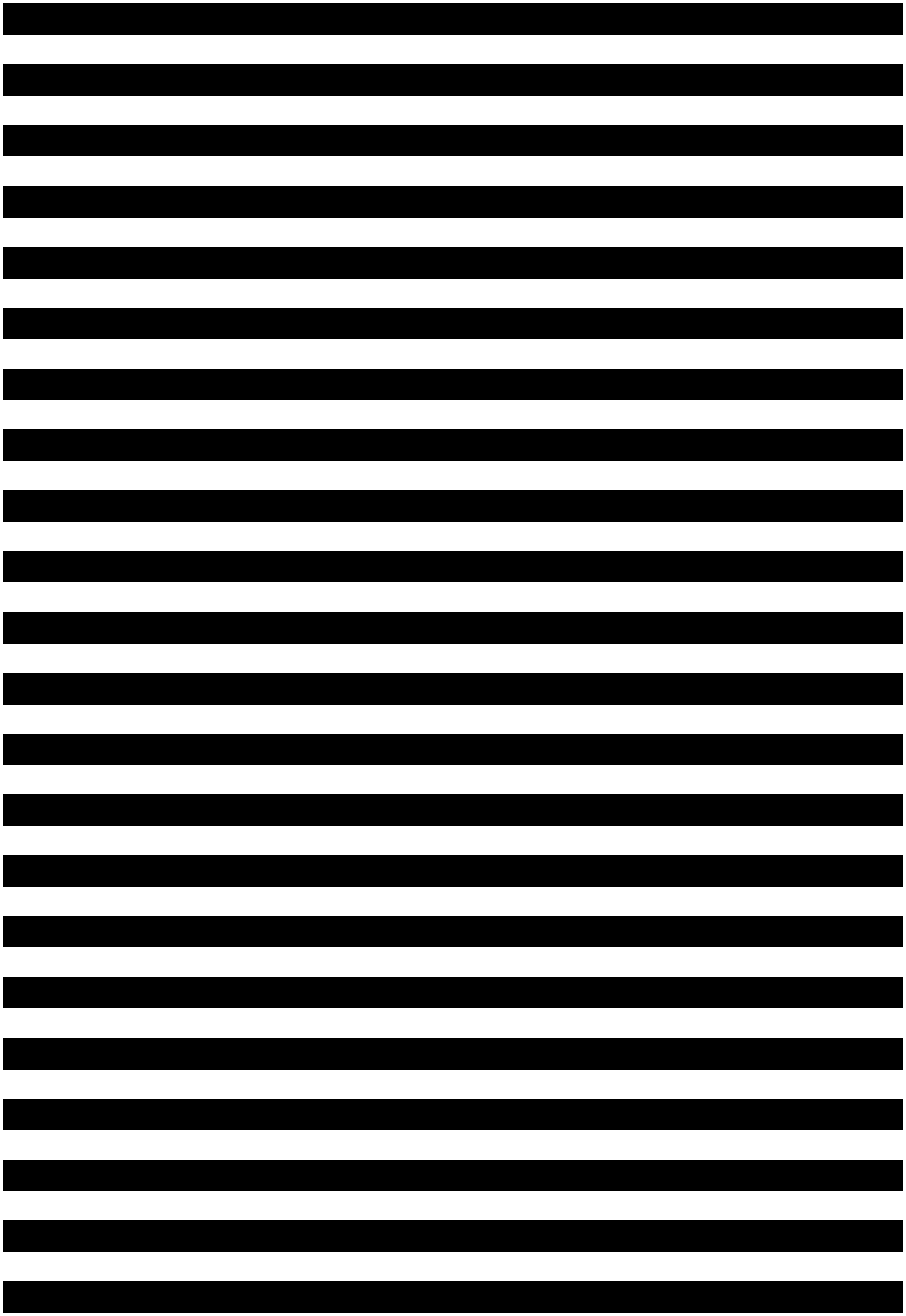
the nation's passenger rail transportation sector; and (2) to define and develop an intelligence product that helps to protect the public and the nation's critical railroad infrastructure. The strategy presented in Chapter III accomplishes the first objective by leveraging the power of informal networks in the context of the abstract megacommunity framework. Absent a solution from the DHS, it provides a practical solution to intelligence and terrorism information sharing between the federal intelligence community, state and local law enforcement, and the private sector. The intelligence requirements defined in Chapter IV (Table 2) and a product similar to the BTP Counterterrorism Unit briefing presented in Chapter VI fulfill the second objective. The outcome from both of these objectives is evidence driven, and based on what works on the front lines of passenger rail transportation. I hope you will find them pragmatically useful.

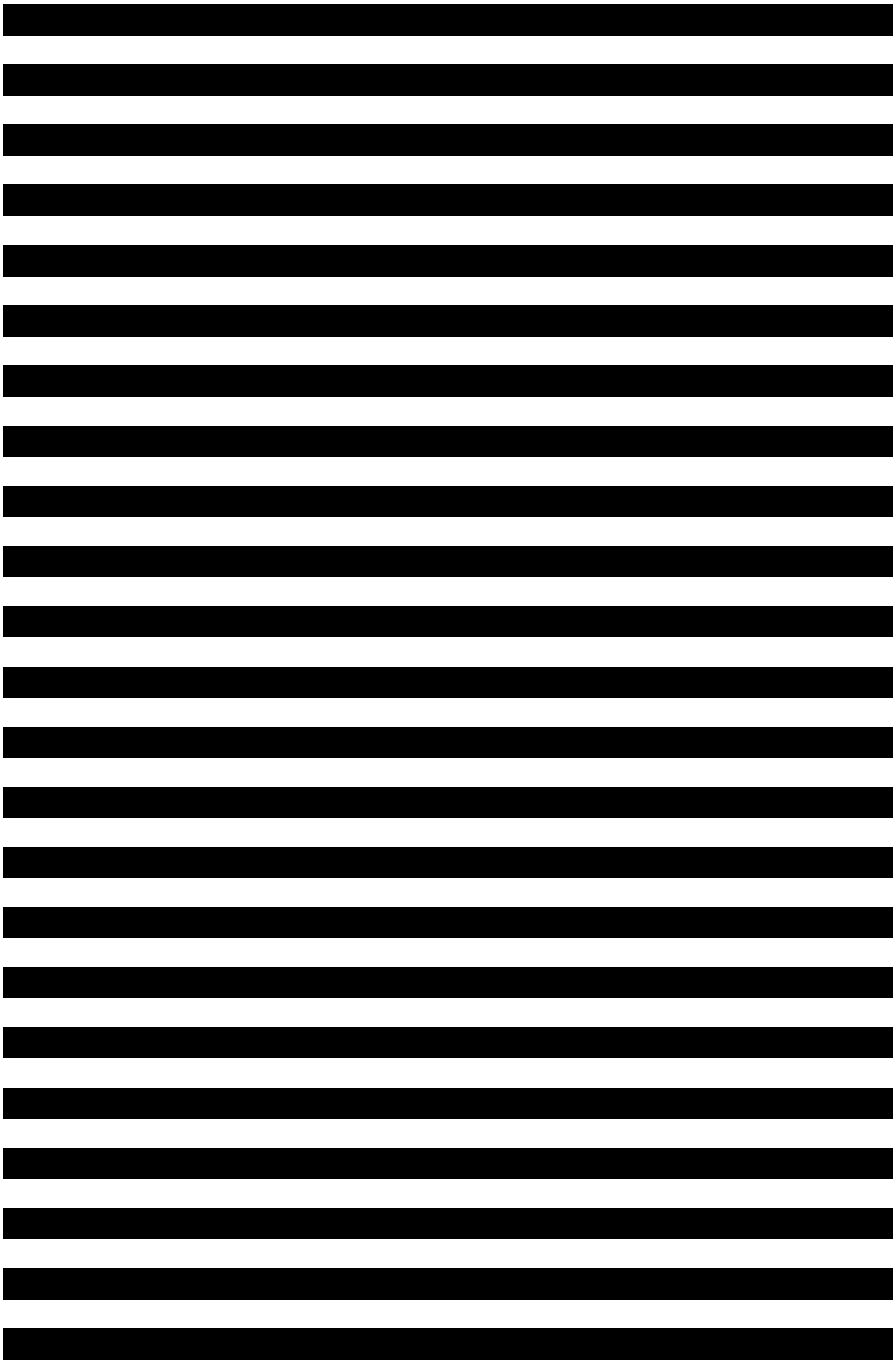
THIS PAGE INTENTIONALLY LEFT BLANK

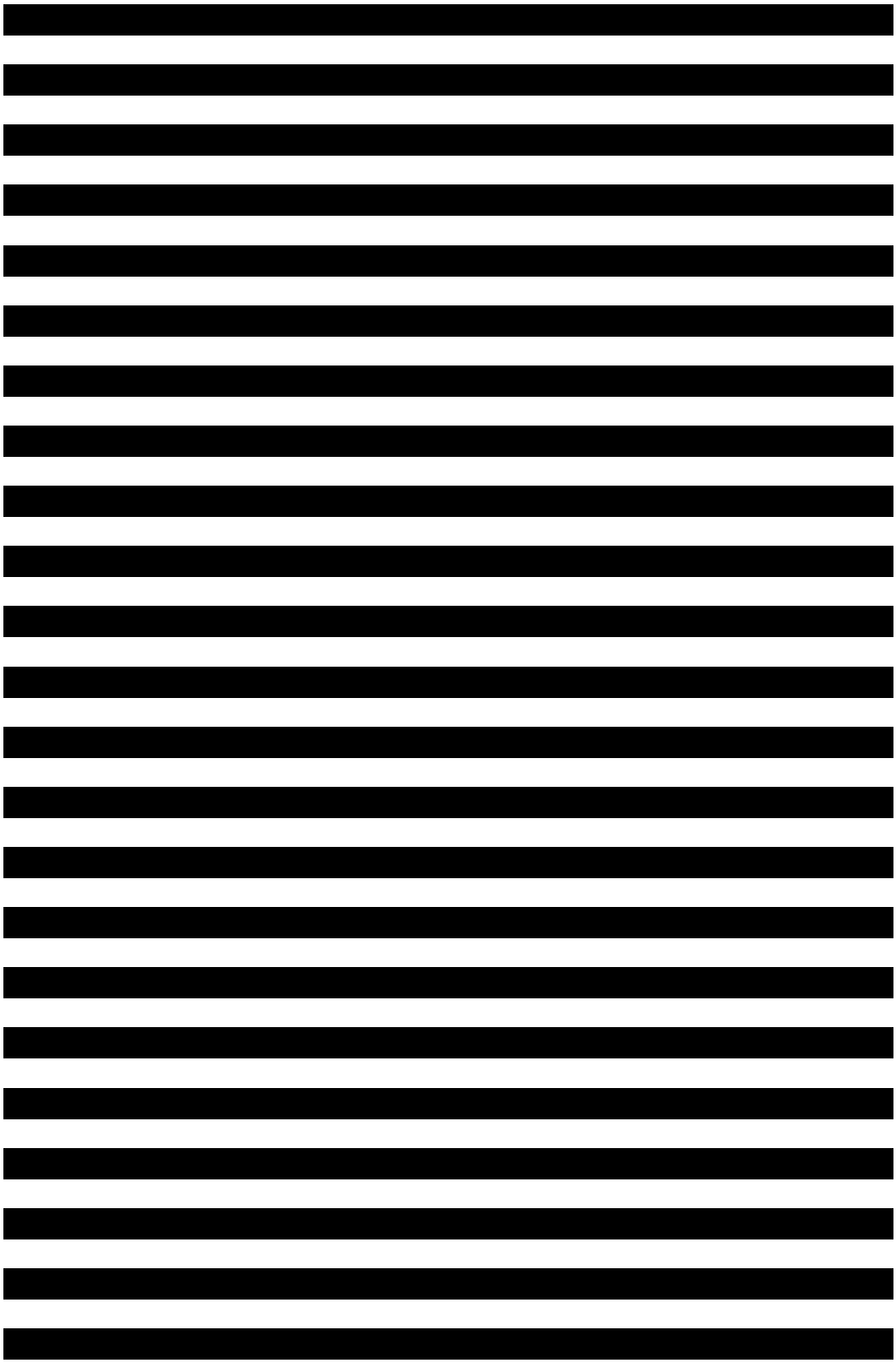
APPENDIX A. [redacted]

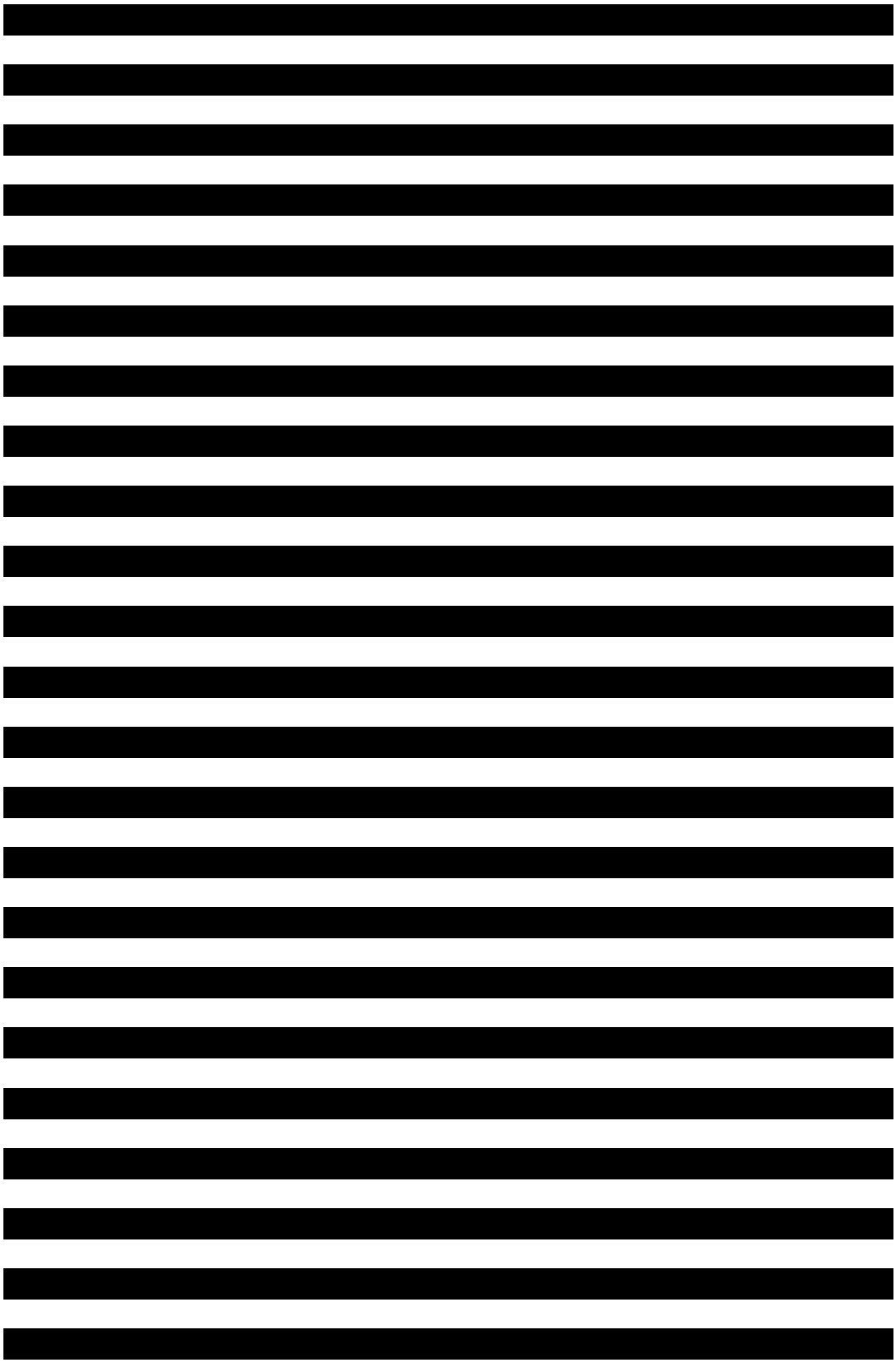
Appendices A – D have been reissued under separate cover

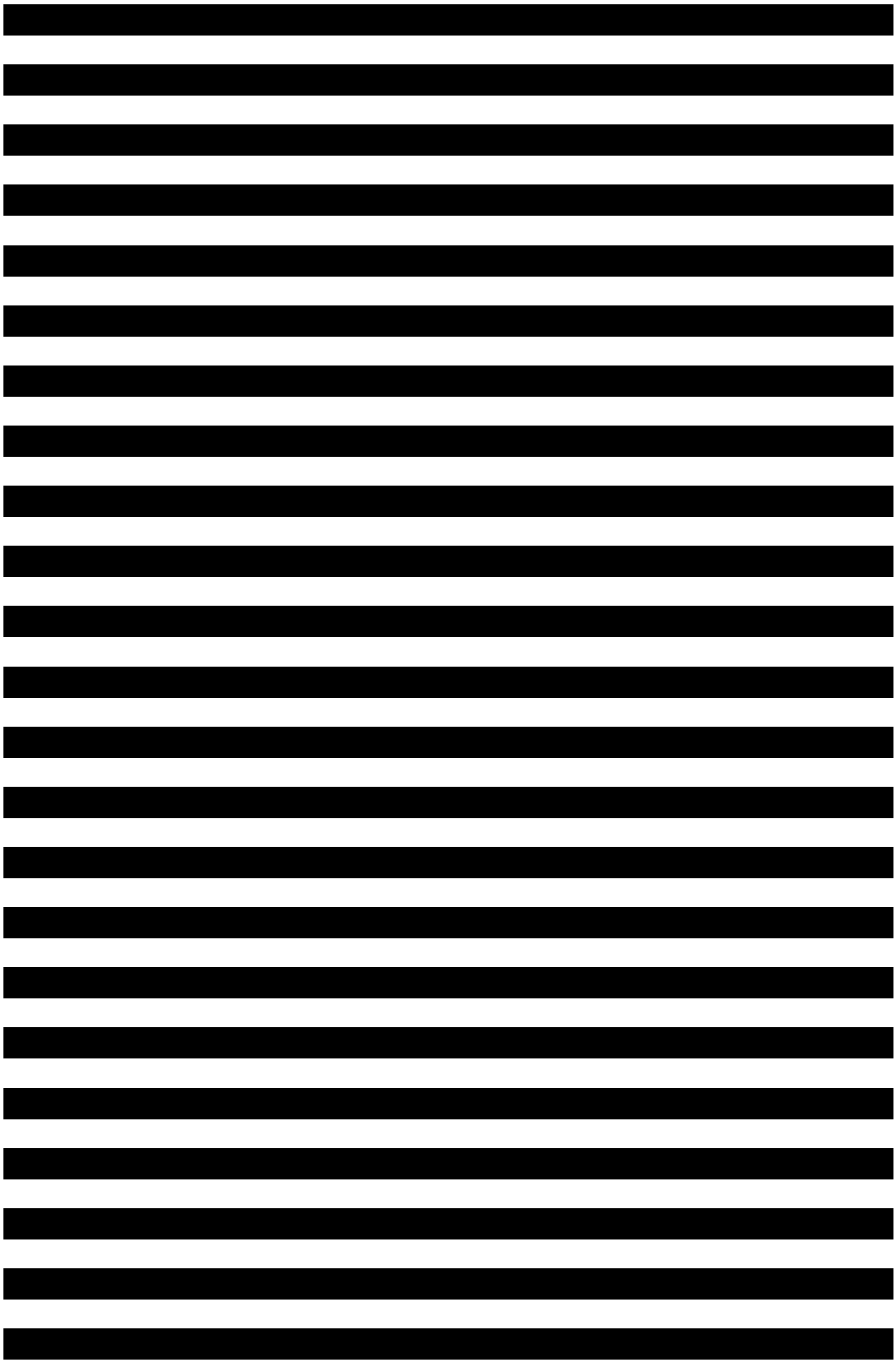
[redacted]

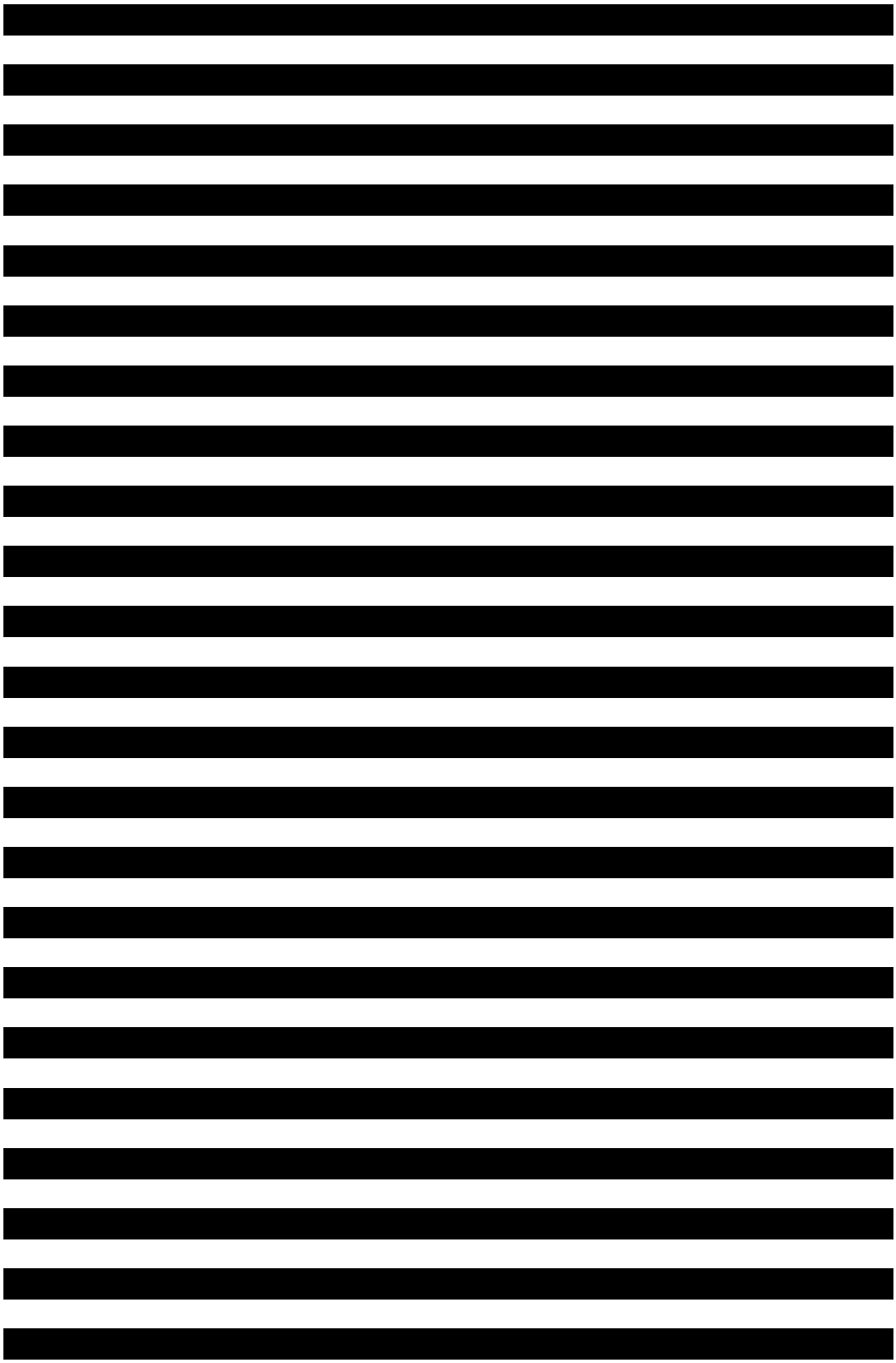






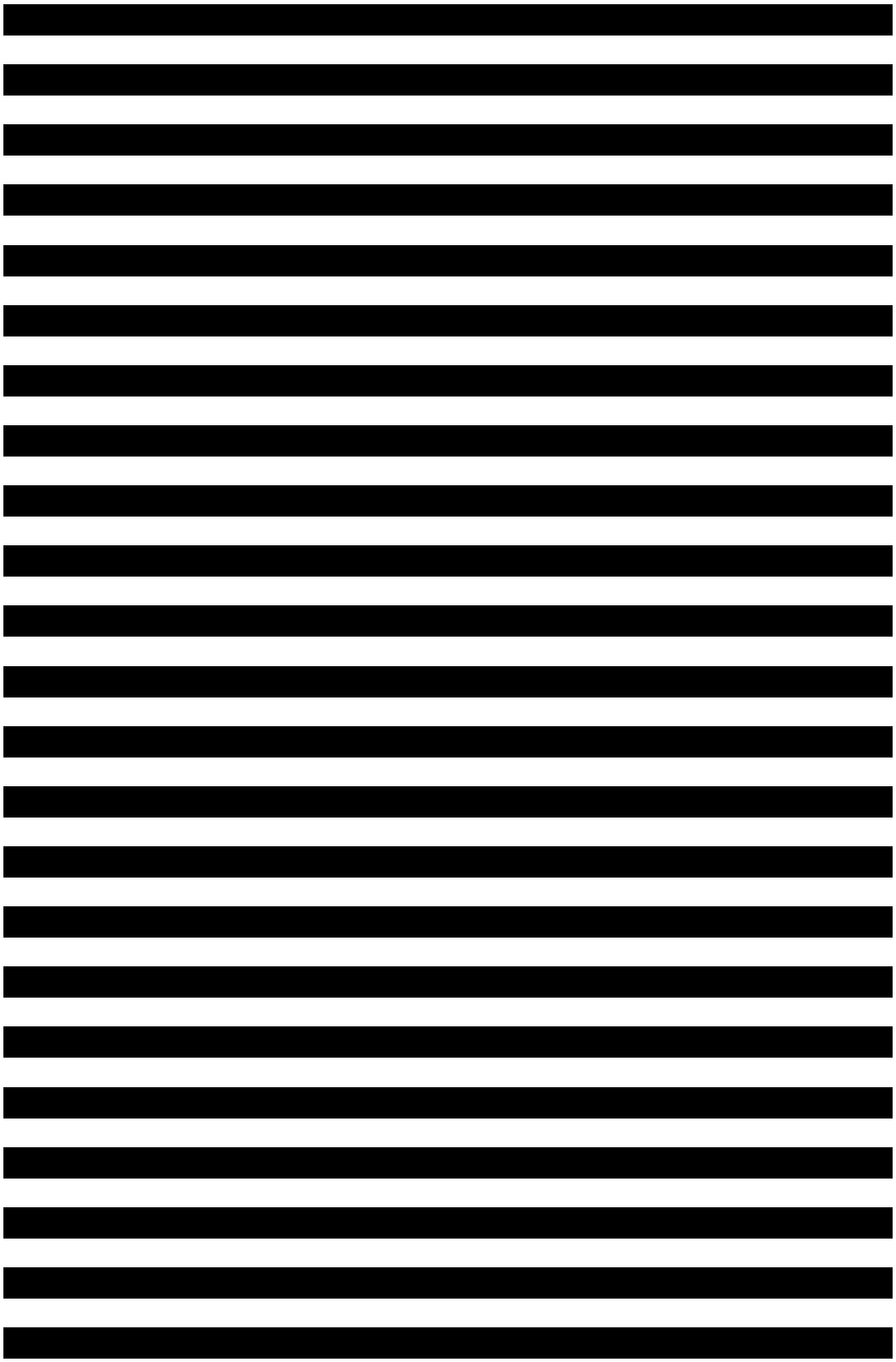


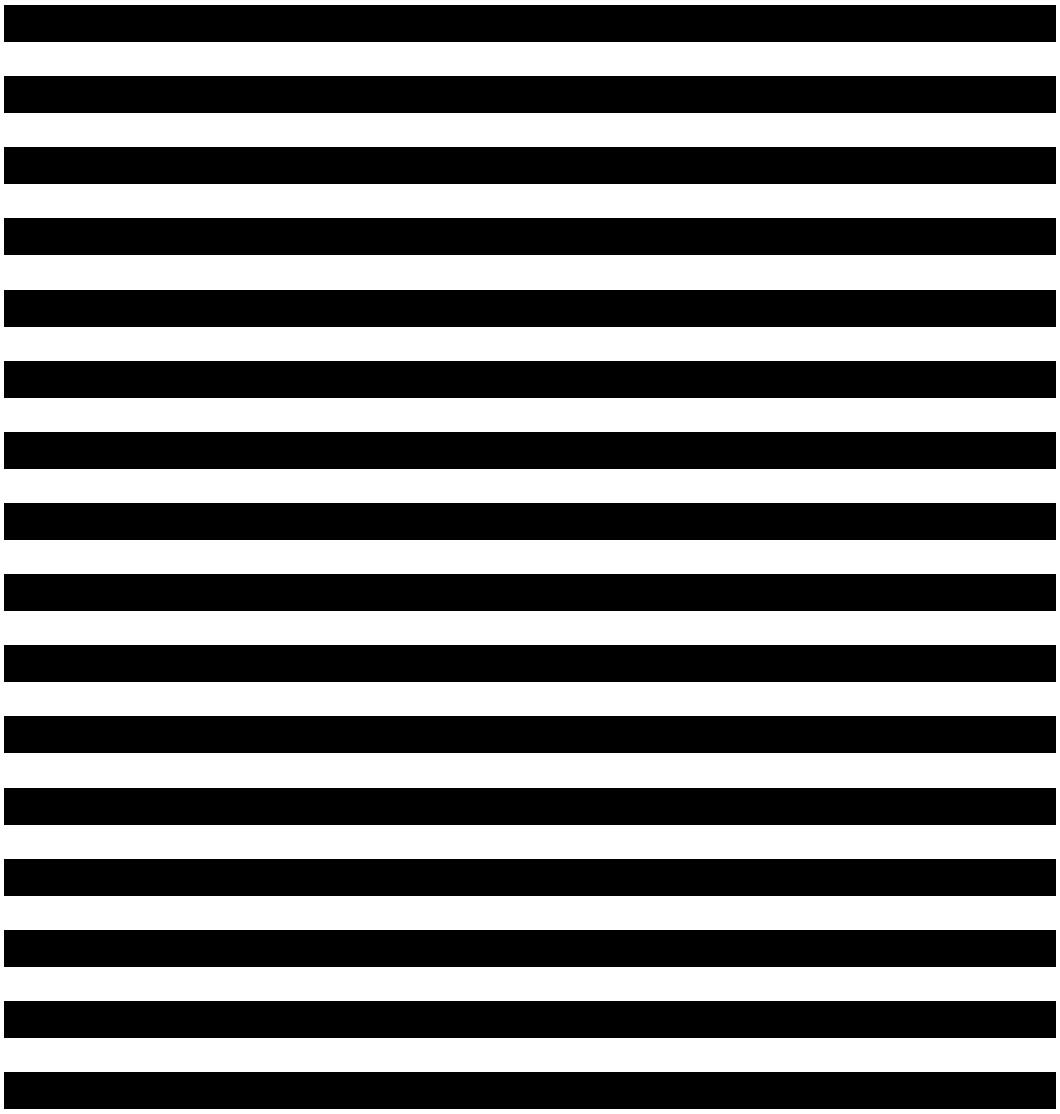




[redacted]

[redacted]



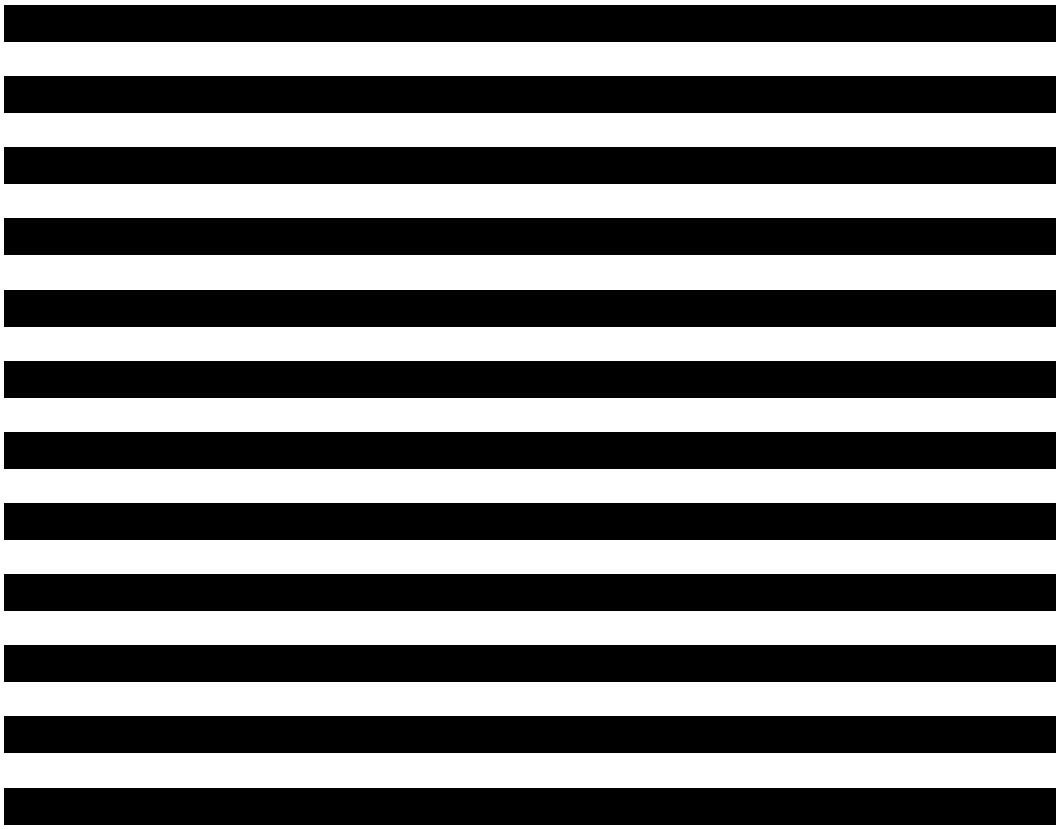


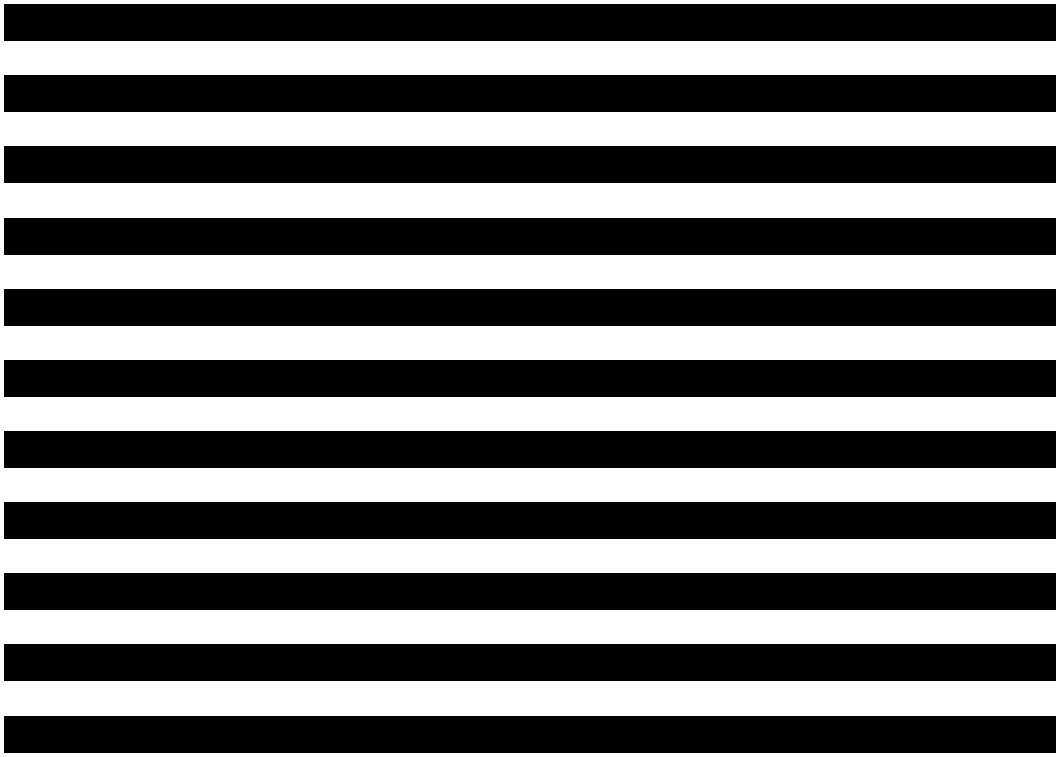
THIS PAGE INTENTIONALLY LEFT BLANK

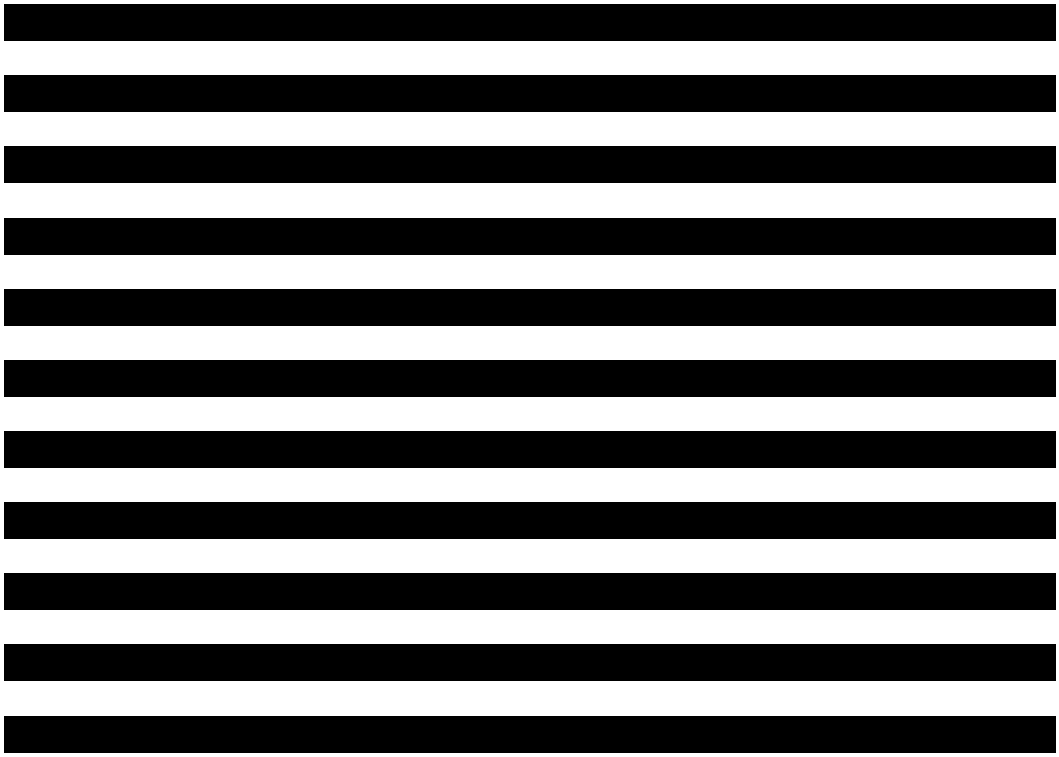
APPENDIX B. [redacted]

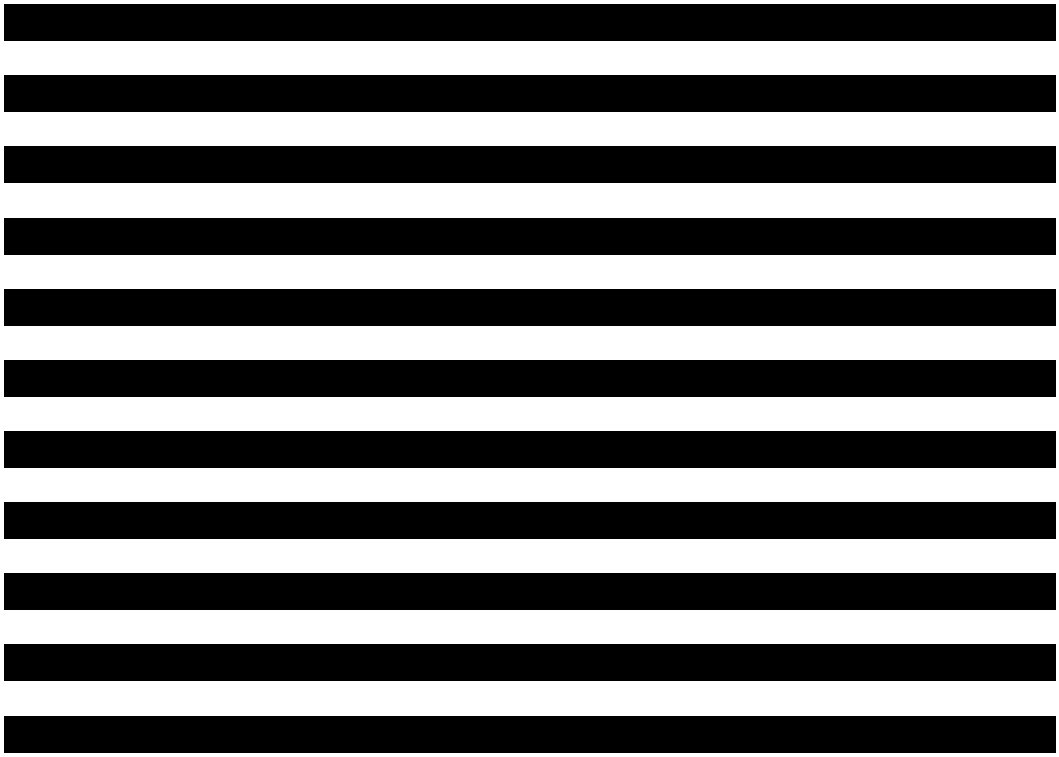
Appendices A – D have been reissued under separate cover

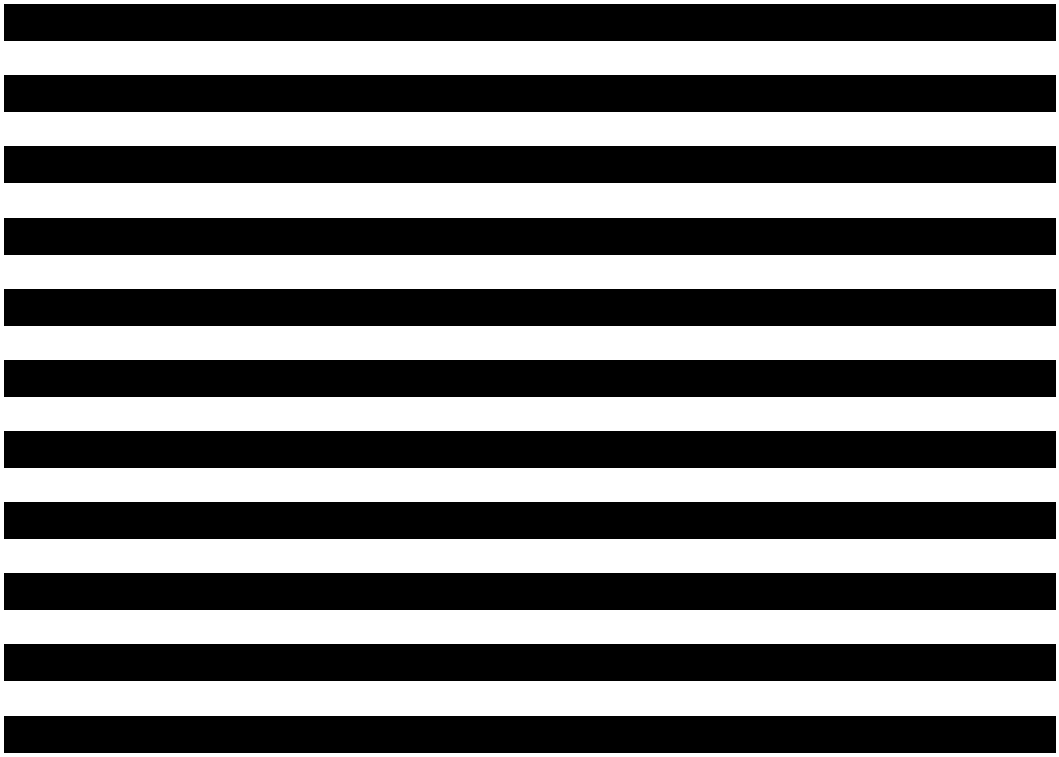
[redacted]

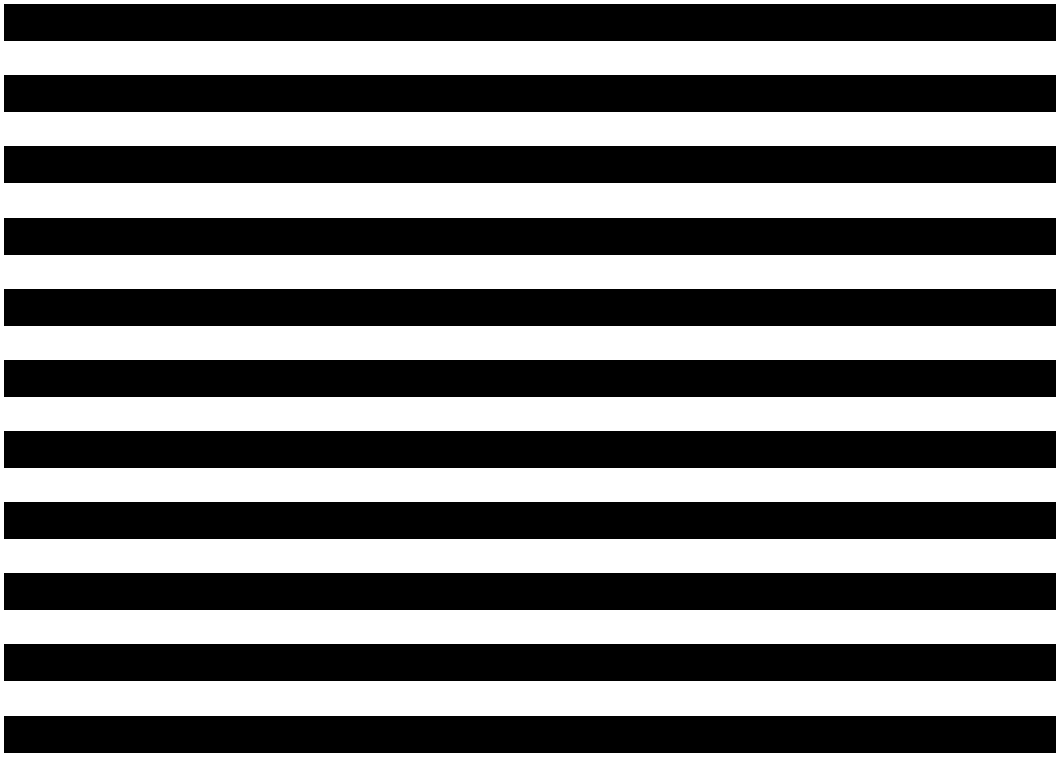


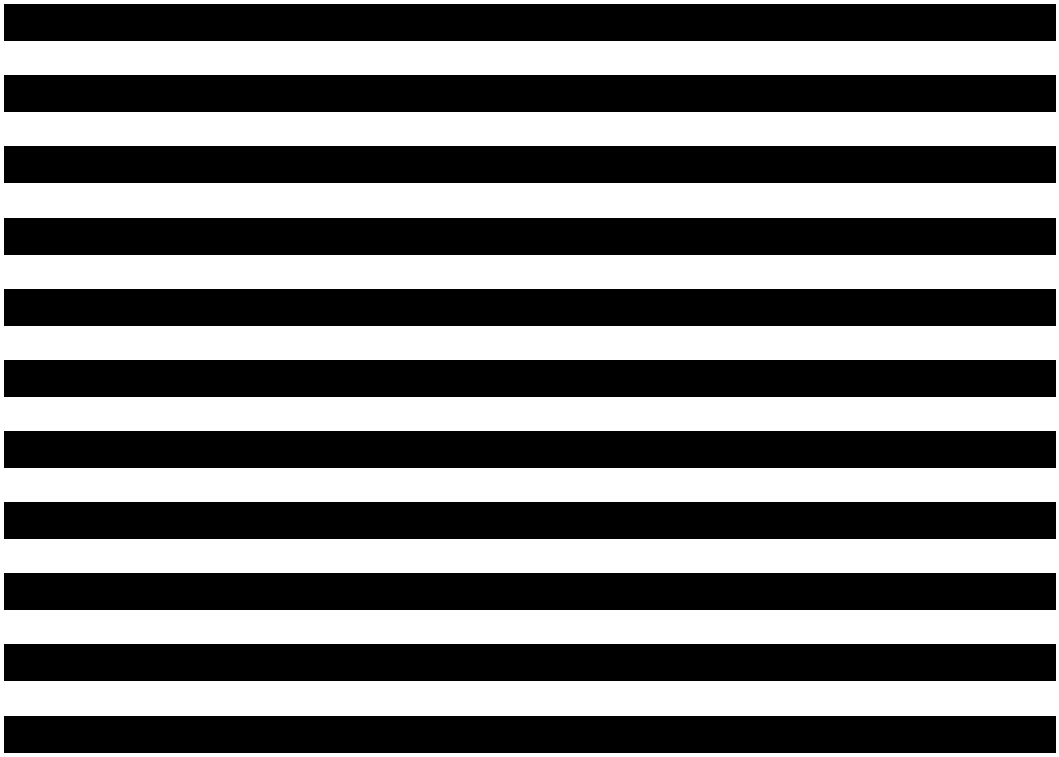


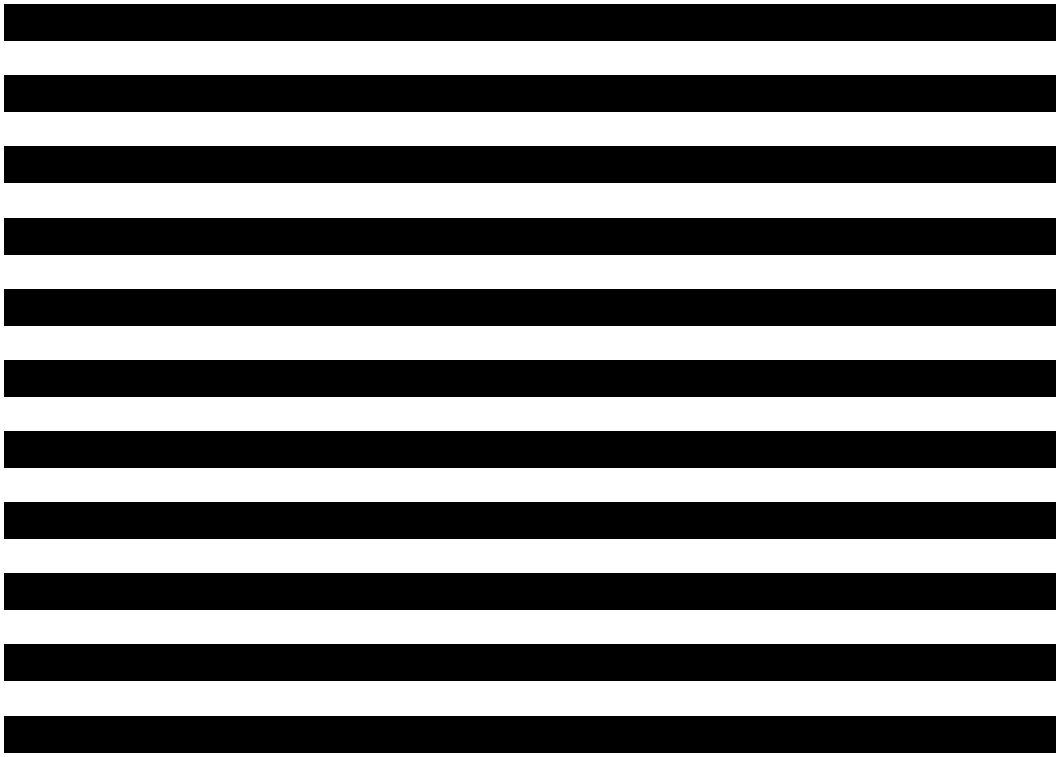


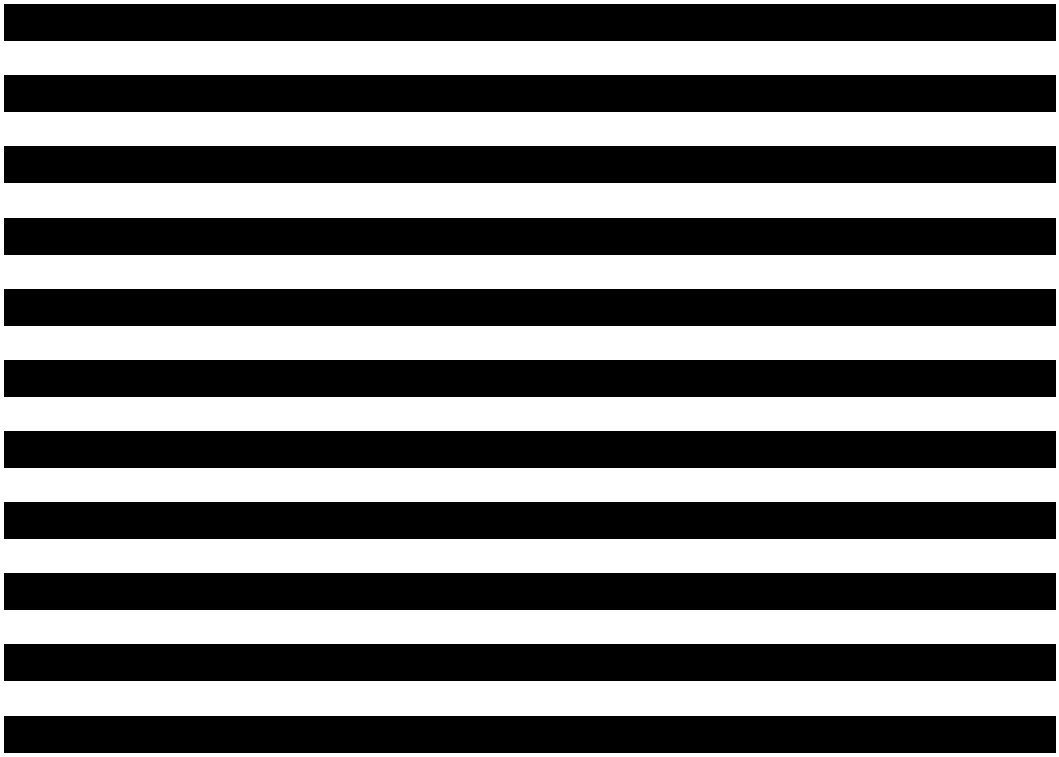


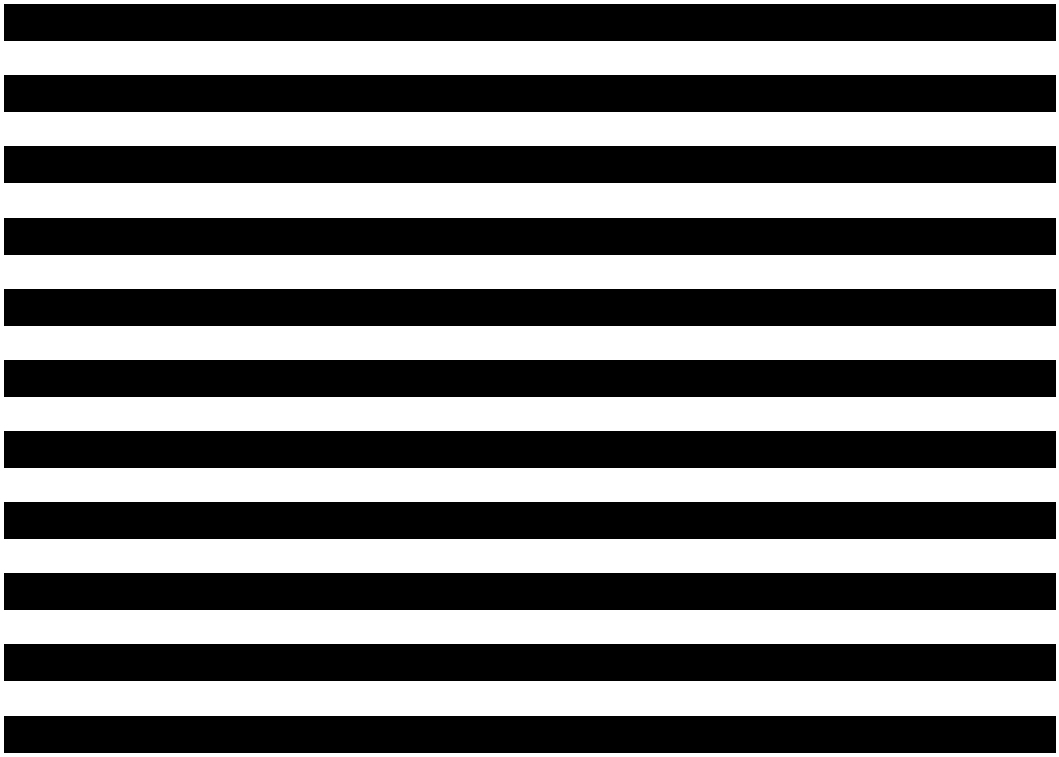


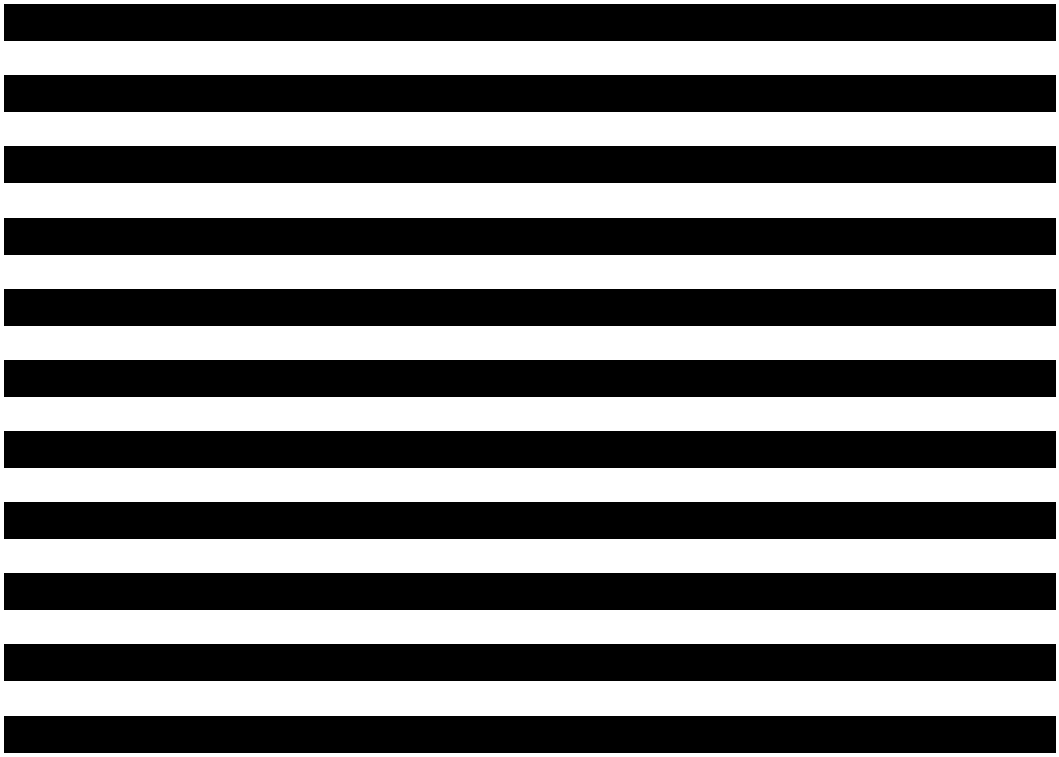


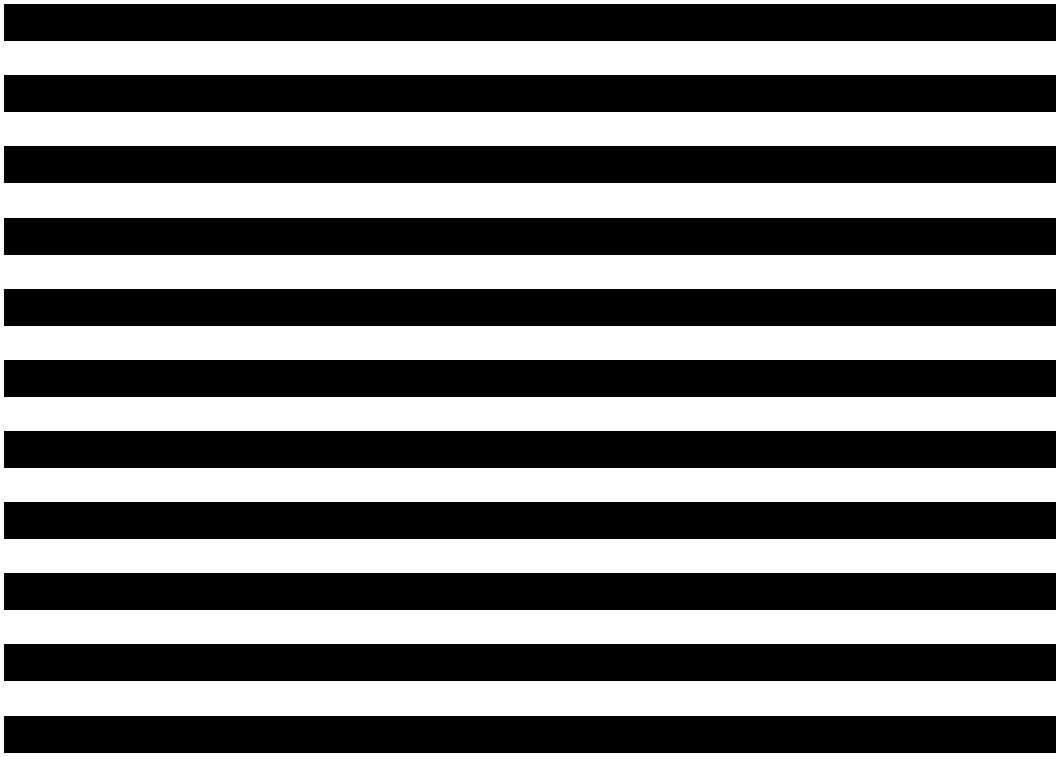


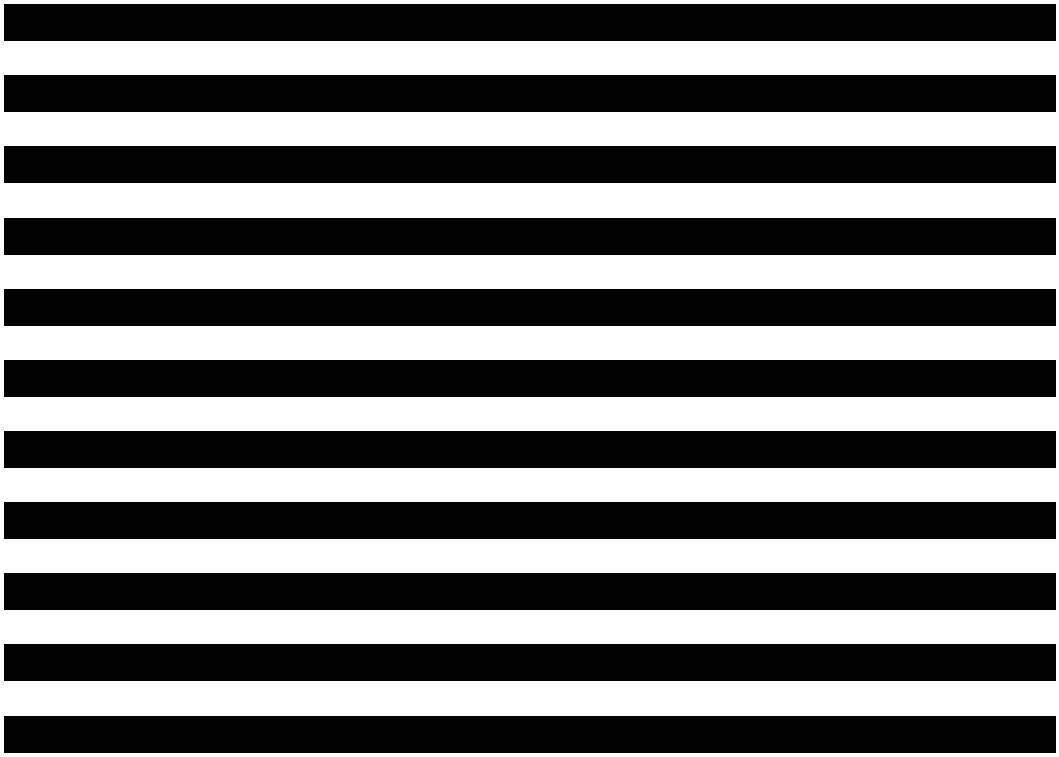


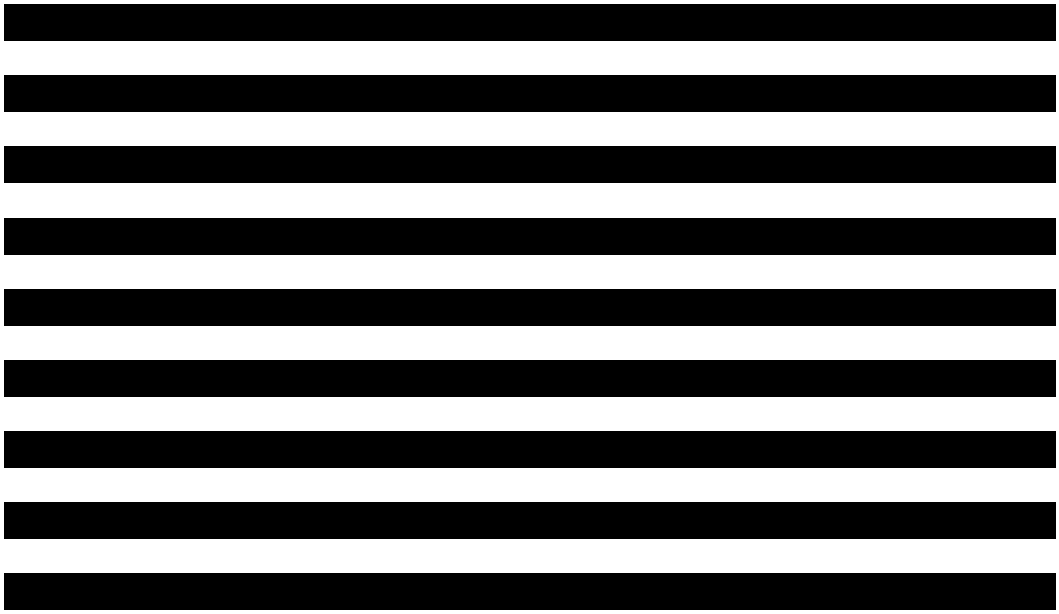


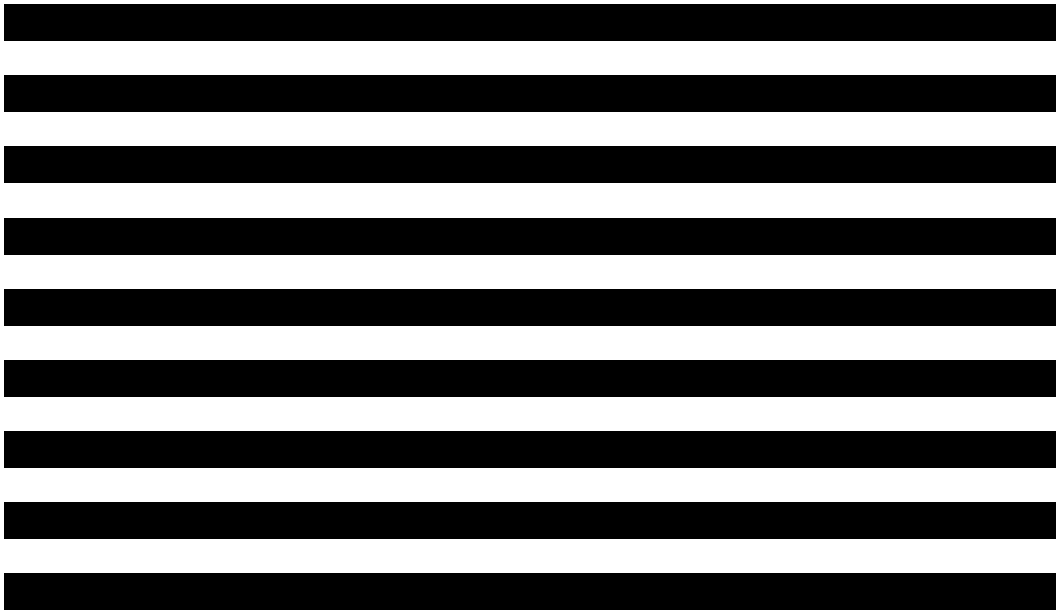


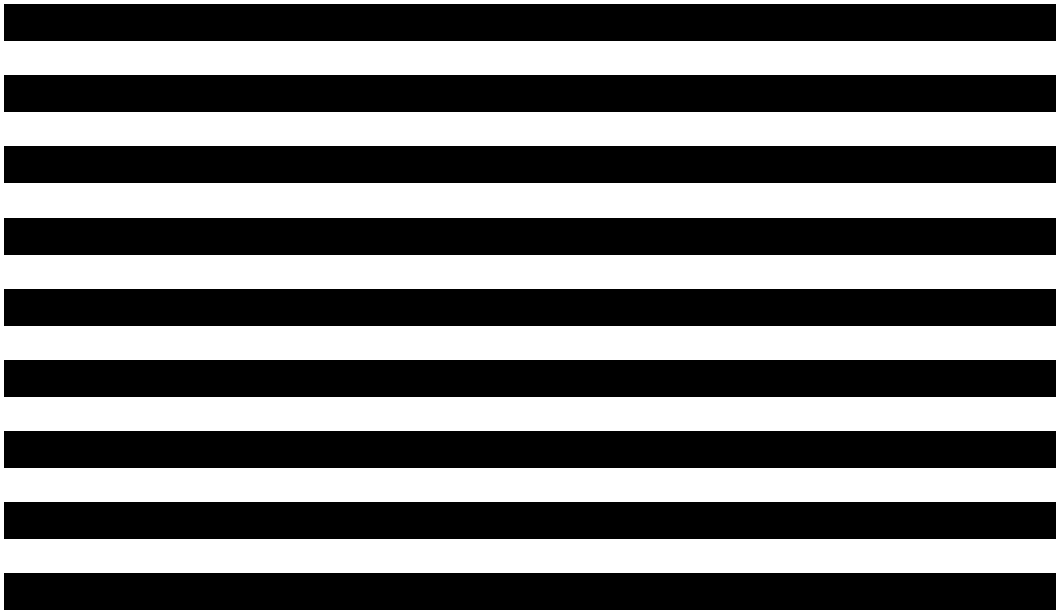


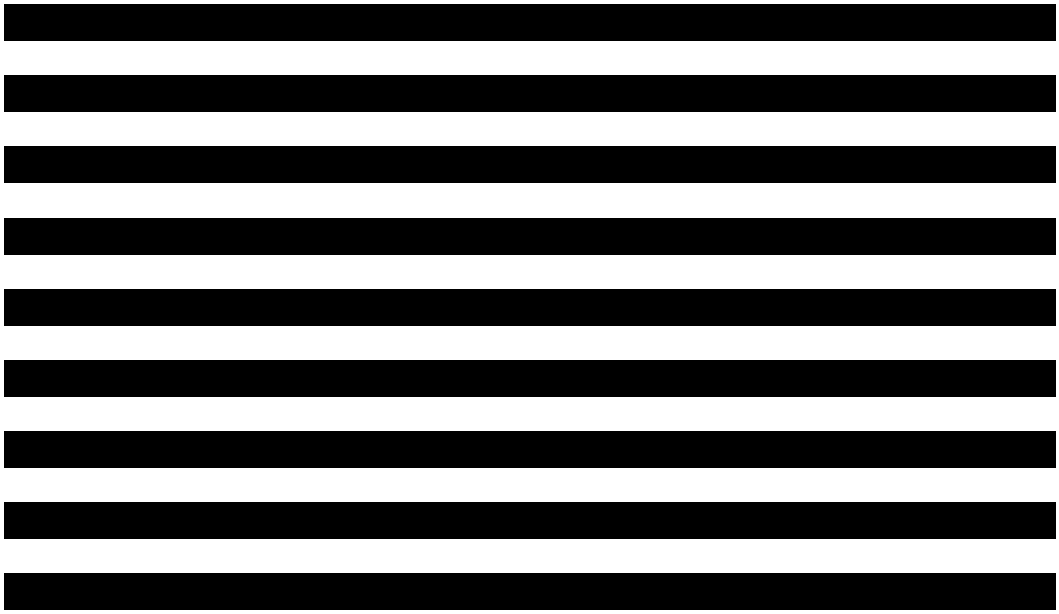


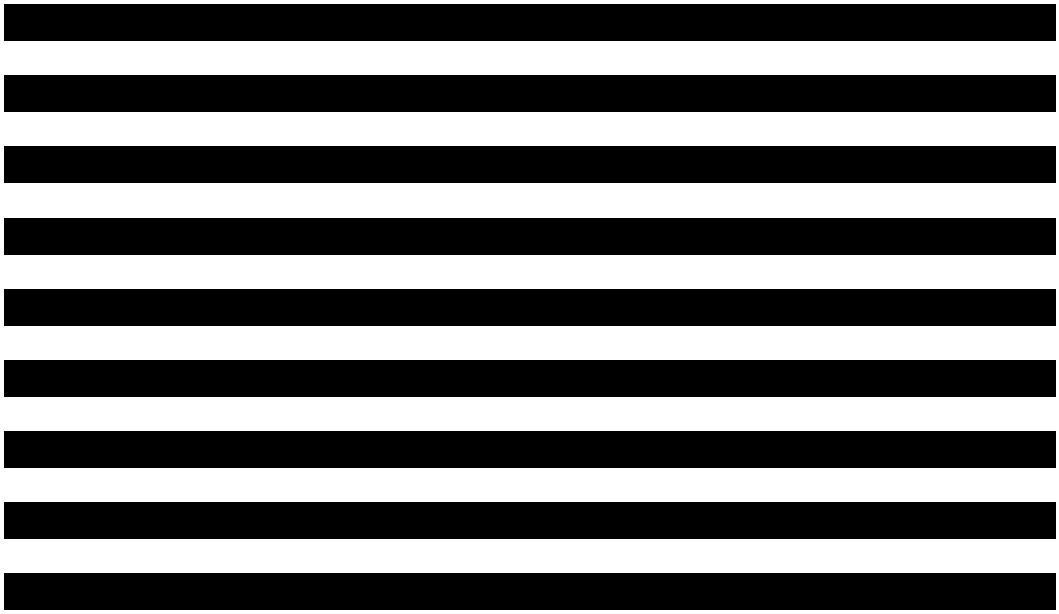


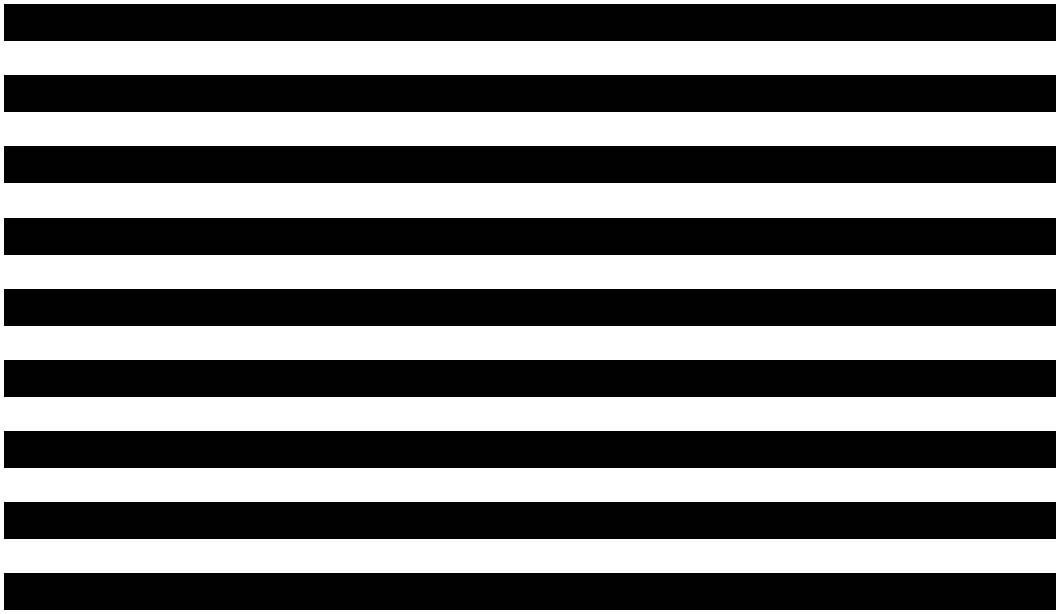


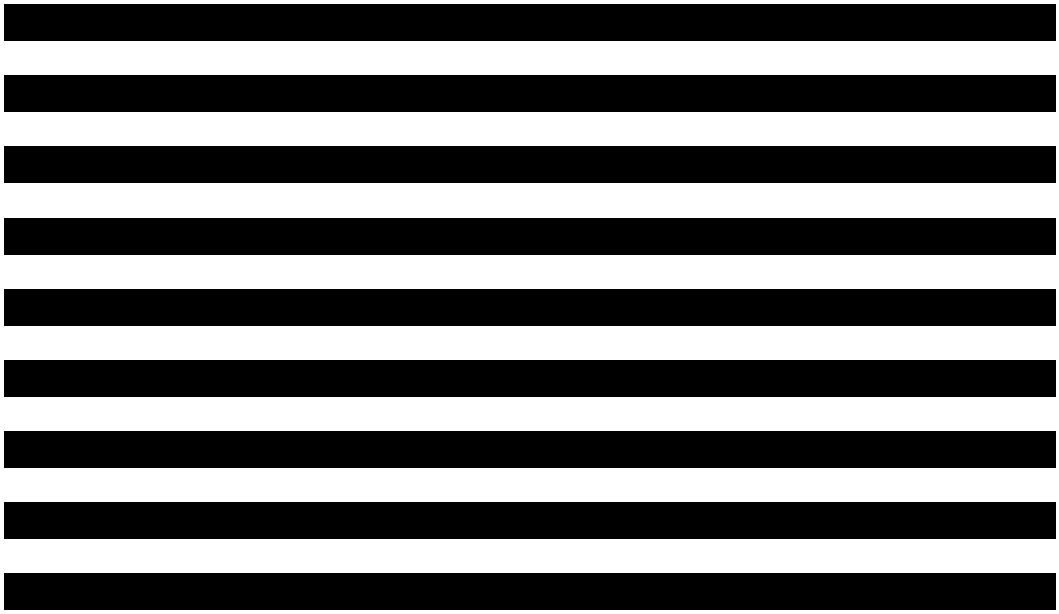


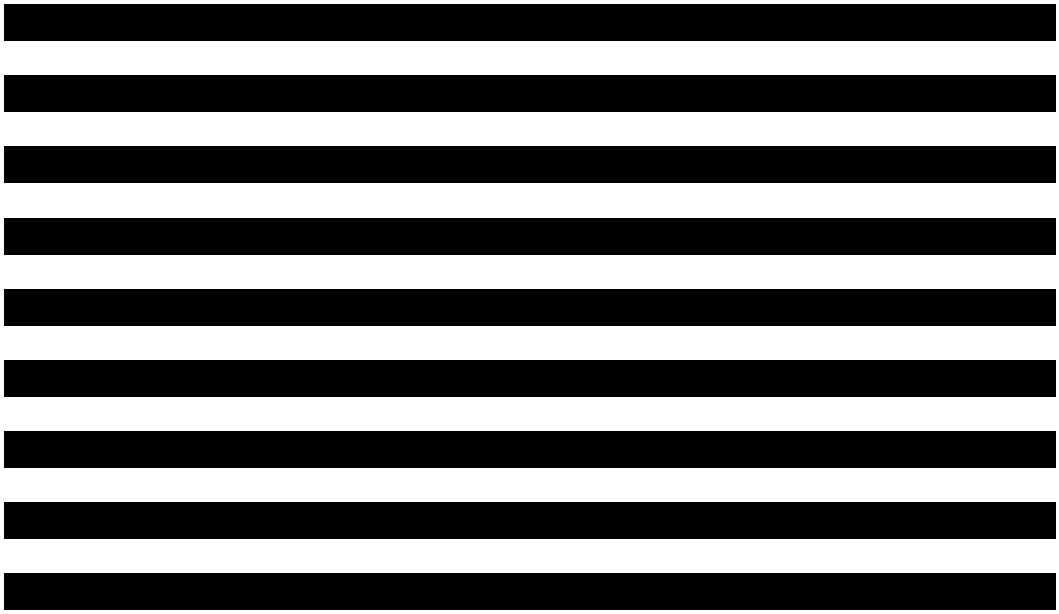


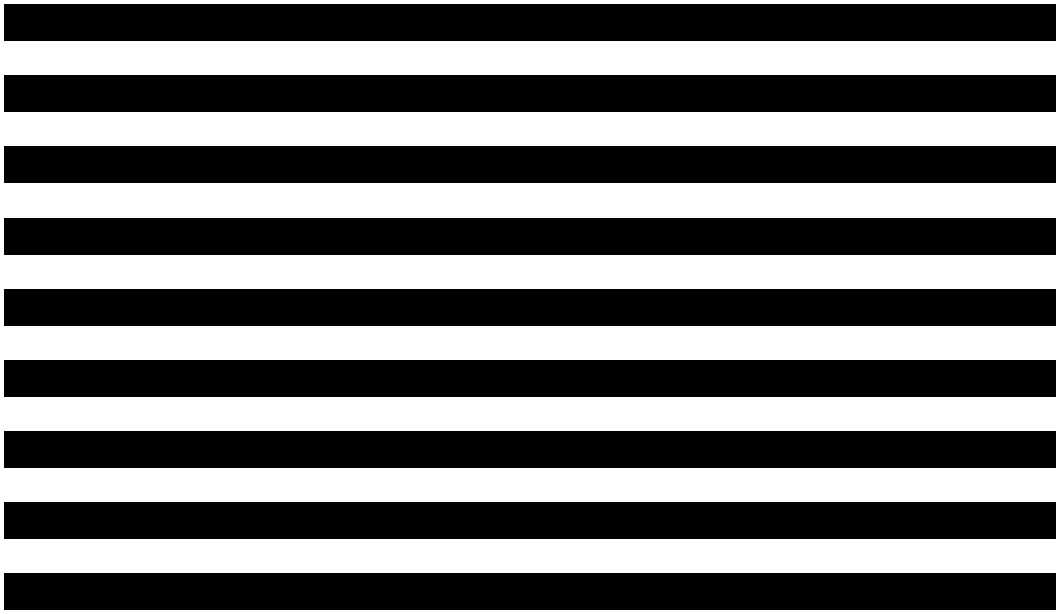


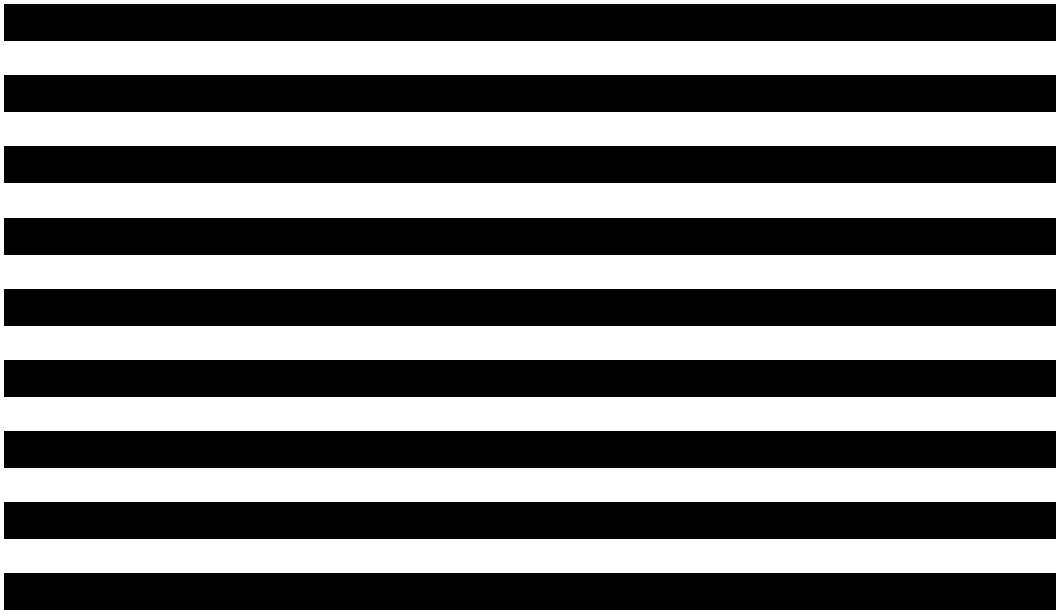












APPENDIX C. [redacted]

Appendices A – D have been reissued under separate cover

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

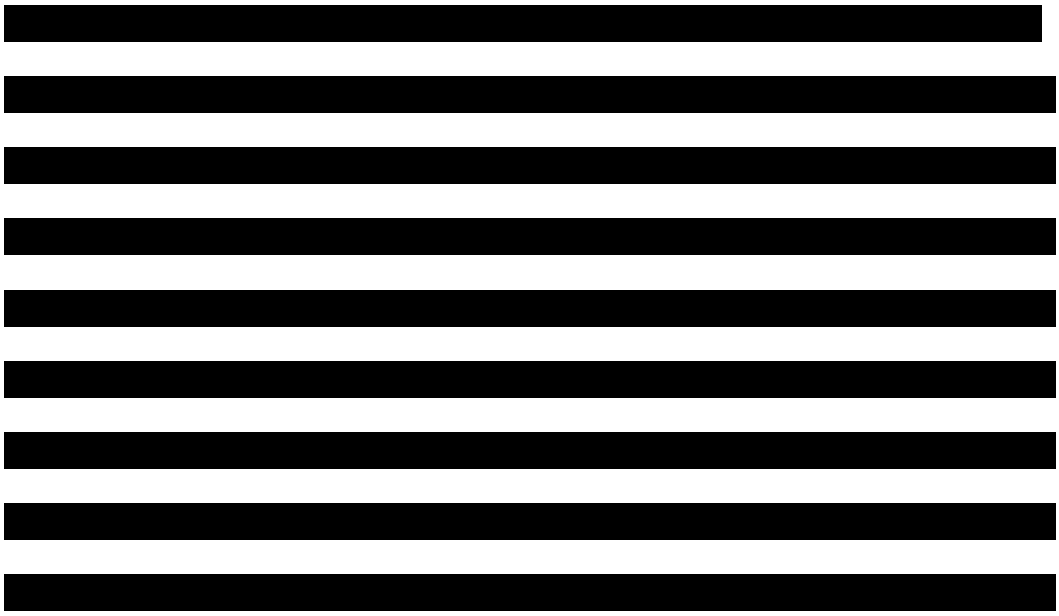
[redacted]

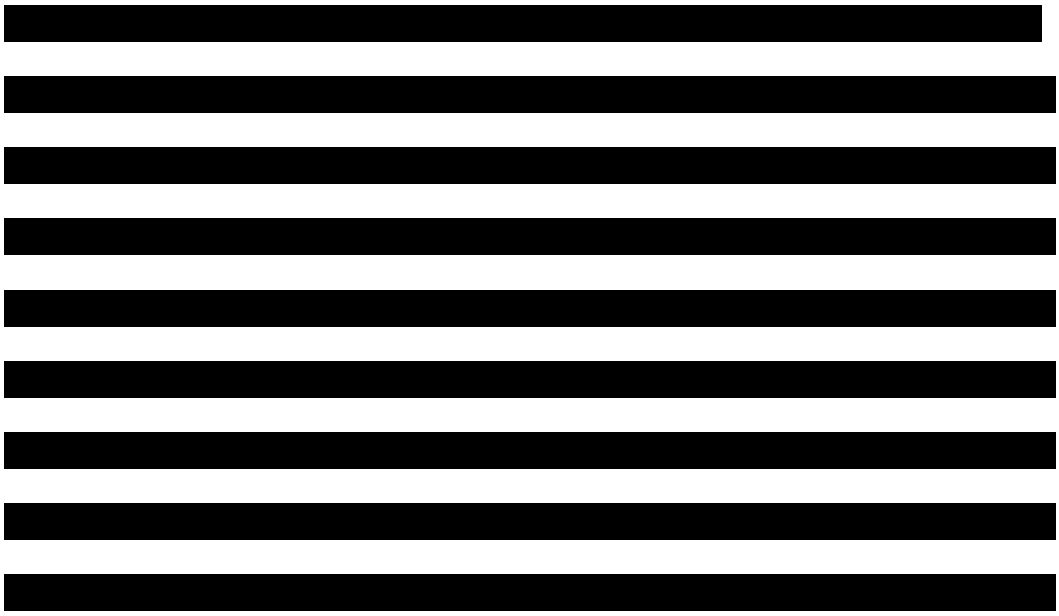
THIS PAGE INTENTIONALLY LEFT BLANK

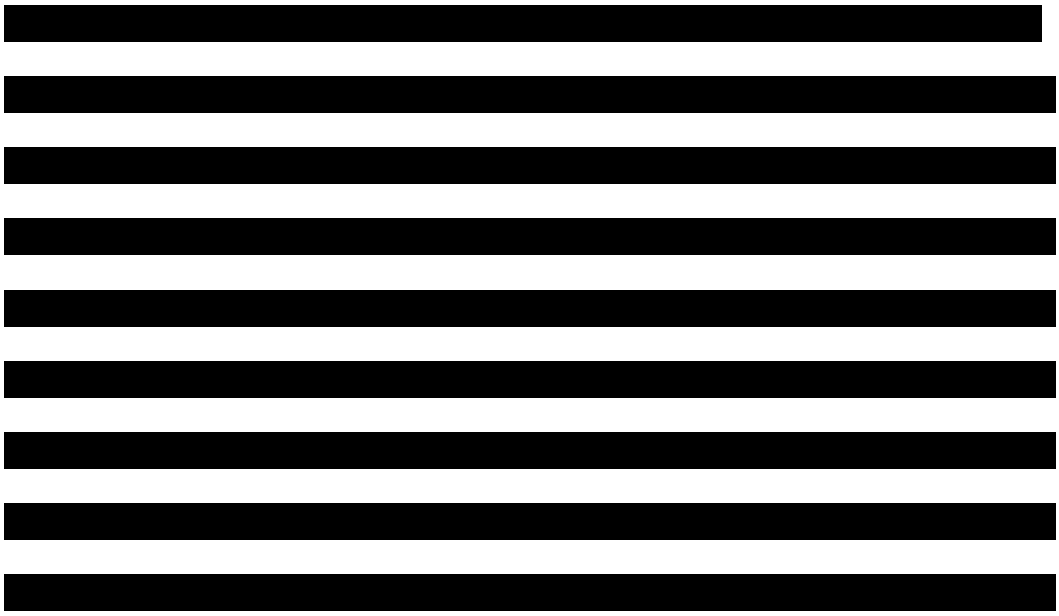
APPENDIX D. [redacted]

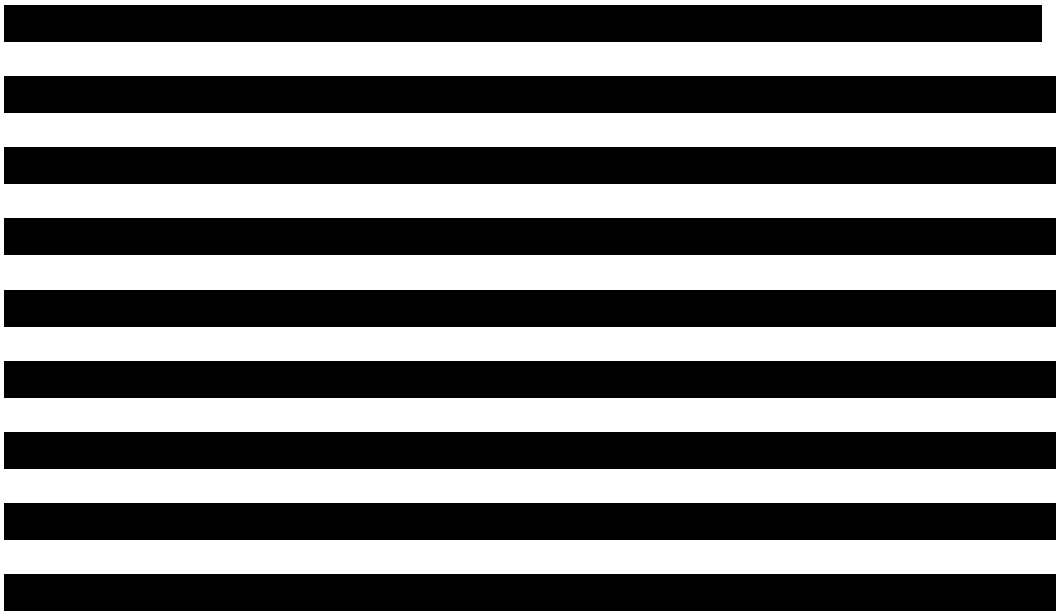
Appendices A – D have been reissued under separate cover

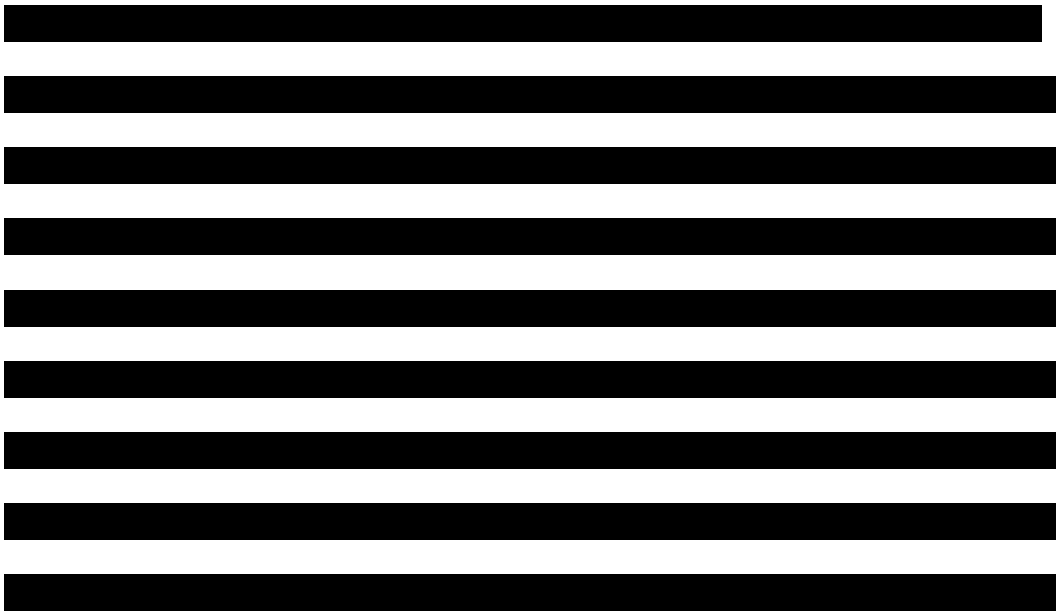
[redacted]











LIST OF REFERENCES

9/11 Commission. *The 9/11 Commission Report.* New York, NY: W.W. Norton & Company, 2004.

Arquilla, John, and David Ronfeldt. *Networks and Netwars: The Future of Terror, Crime, and Militancy*. Washington, D.C.: RAND Corporation, 2001.

Arquilla, John, David Ronfeldt and Michele Zanini. "Networks, Netwar, and Information-age Terrorism." In *Countering the New Terrorism*, edited by Ian O. Lesser, 39 – 84. Santa Monica, CA: RAND, 1999.

Barabási, Albert – László. *Linked.* New York, NY: Penguin Group, 2003.

Bardach, Eugene. *A Practical Guide for Policy Analysis – The Eightfold Path to More Effective Problem Solving.* Washington, D.C.: CQ Press, 2005.

Barr, William P. "Statement of William P. Barr to the National Commission on Terrorist Attacks Upon the United States." *National Commission on Terrorist Attacks Upon the United States*, http://govinfo.library.unt.edu/911/hearings/hearing6/witness_barr.htm (accessed February 29, 2008).

Barrett, Larry and Sean Gallagher. "Case 113 - What Sin City Can Teach Tom Ridge." *Baseline* (April 2004).

Bradley, Ed. "Inside the NYPD's Anti-Terror Fight." *60 Minutes*, http://www.cbsnews.com/stories/2006/03/17/60minutes/main1416824.shtml (accessed June 17, 2008).

Brafman, Ori, and Rod A. Beckstrom. *The Starfish and the Spider*. New York, NY: Penguin Group, 2006.

British Transport Police. "BTP History Archives." *British Transport Police*, http://www.btp.police.uk/History%20Society/history%20society%20main.htm (accessed February 24, 2008).

[redacted]

Bryson, John M. *Strategic Planning for Public and Nonprofit Organizations.* San Francisco, CA: Jossey-Bass, 2004.

Corporate Emergency Access System. "Home Page." Corporate *Emergency Access System*, http://ceas.com/ (accessed April 20, 2008).

Covey, Stephen M.R. *The Speed of Trust*. New York, NY: Free Press, 2006.

Cross, Rob, and Andrew Parker. *The Hidden Power of Social Networks*. Boston, MA: Harvard Business School Publishing, 2004.

Customs and Border Patrol. "Trusted Traveler Programs." *Customs and Border Patrol*, http://www.cbp.gov/xp/cgov/travel/trusted_traveler/ (accessed April 20, 2008).

Department of Homeland Security and Federal Bureau of Investigation. *Mumbai Mass Transit Bombings Share Similarities with London and Madrid*. Washington, D.C.: Department of Homeland Security, 2006.

Department of Homeland Security Office of Intelligence and Analysis. *Strategic Sector Assessment – The Terrorist Threat to the U.S. Commercial Passenger and Freight Rail System.* Washington, D.C.: Department of Homeland Security, 2006.

Department of Homeland Security. *Information Sharing Strategy*. Washington, D.C.: Department of Homeland Security, 2008, http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf (accessed June 8, 2008).

Department of Homeland Security. *Information Sharing Strategy*. Washington, D.C.: Department of Homeland Security, 2008, http://www.dhs.gov/xlibrary/assets/dhs_information_sharing_strategy.pdf (accessed June 8, 2008).

Doyle, Charles. *The USA PATRIOT Act: A Legal Analysis – Report RL31377*. Washington, D.C.: Congressional Research Service, 2002.

Eden, C., and F. Ackermann. *Making Strategy: The Journey of Strategic Management*. Thousand Oaks, CA: Sage, 1998.

Friedman, Thomas L. *The World is Flat: A Brief History of the Twenty-first Century.* New York, NY: Farrar, Straus, and Giroux, 2005.

Gerencser, Mark, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly. *Megacommunities.* New York, NY: Palgrave MacMillan, 2008.

Government Accountability Office. *Critical Infrastructure Protection – Improving Information Sharing with Infrastructure Sectors.* Washington, D.C.: GAO, 2004.

Government Accountability Office. *Critical Infrastructure Protection – Establishing Effective Information Sharing with Infrastructure Sectors.* Washington, D.C.: GAO, 2004.

Government Accountability Office. *Passenger Rail Security – Enhanced Federal Leadership Needed to Prioritize and Guide Security Efforts*. Washington, D.C.: GAO, 2005.

Granovetter, Mark. "The Strength of Weak Ties: A Network Theory Revisited." *Sociological Theory* (1983): 202.

Hearing Testimony: Private Sector Information Sharing: What Is It, Who Does It, and What's Working at DHS?. 110th United States Congress. House of Representatives Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment. (July 2007).

Homeland Security & Defense Business Council. "Council Vision, Mission, and Value Statement." *Homeland Security & Defense Business Council*, http://www.homelandcouncil.org/aboutus.php (accessed July 12, 2008).

Homeland Security Act of 2002. Public Law 107-296. 107th United States Congress. (November 2002).

Homeland Security Advisory Council. *Homeland Security Information Sharing between Government and the Private Sector Final Report*. Washington, D.C.: Department of Homeland Security, 2005.

Homeland Security Advisory Council. *Homeland Security Intelligence and Information Fusion*. Washington, D.C.: Department of Homeland Security, 2005.

Homeland Security Advisory Council. *Intelligence and Information Sharing Initiative Final Report and Recommendations*. Washington, D.C.: Department of Homeland Security, 2004.

Homeland Security Advisory Council. *Lessons Learned Information Sharing Initiative: Homeland Security Intelligence Requirements Process*. Washington, D.C.: Department of Homeland Security, 2005.

House of Commons. *Anti-terrorism, Crime & Security Act 2001*. London, UK: HM Government, 2001.

House of Commons. *Railways and Transport Safety Act 2003 (c.20)*. London, UK: HM Government, 2003.

House of Commons. *Transport and Works Act 1992 (c.42)*. London, UK: HM Government, 1992.

Implementing Recommendations of the 9/11 Commission Act of 2007. Public Law 110-53. 110th United States Congress. (August 2007).

Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458. 108th United States Congress. (December 2004).

Kim, W. Chan, and Renée Mauborgne. *Blue Ocean Strategy*. Boston, MA: Harvard Business School Press, 2005.

Krebs', Valdis. "Uncloaking Terrorist Networks." *First Monday*, http://www.firstmonday.org/Issues/issue7_4/krebs/ (accessed May 29, 2008).

Lahneman, William. *The Seven Step Intelligence Cycle.* Monterey, CA: Naval Postgraduate School, 2007.

Lowenthal, Mark. *Intelligence – From Secrets to Policy.* Washington, D.C.: CQ Press, 2006.

Metropolitan Transit Authority. "If You See Something, Say Something." *Metropolitan Transit Authority*, http://www.mta.info/mta/security/index.html (accessed December 25, 2007).

Miller, Patrick. "How Can We Improve Information Sharing Among Local Law Enforcement Agencies?" Master's Thesis, Naval Postgraduate School, 2005.

National Commission on Terrorism. *Countering the Changing Threat of International Terrorism*. Washington, D.C.: Government Printing Office, 2000.

National Infrastructure Advisory Council. *Evaluation and Enhancement of Information Sharing and Analysis*. Washington, D.C.: NIAC, 2004.

National Infrastructure Advisory Council. *Public-Private Sector Intelligence Coordination*. Washington, D.C.: NIAC, 2006.

National Statistics. "Focus on Religion – Age & Sex Distribution." *National Statistics*, http://www.statistics.gov.uk/cci/nugget.asp?id=955 (accessed February 29, 2008).

National Statistics. "Focus on Religion – Download Maps: Religion by UA/Local Authority (GB)." *National Statistics*, http://www.statistics.gov.uk/statbase/Product.asp?vlnk=13209 (accessed February 29, 2008).

National Statistics. *Focus on Ethnicity and Religion.* Newport, UK: Office of National Statistics, 2006.

National Statistics. *Focus on Religion – 2004 Summary Report.* Newport, UK: Office of National Statistics, 2004.

Office of the Director of National Intelligence. *U.S. Intelligence Community Intelligence Sharing Strategy*. Washington, D.C.: Office of the Director of National Intelligence, 2008. http://www.dni.gov/reports/IC_Information_Sharing_Strategy.pdf (accessed June 8, 2008).

Oxford English Dictionary. "OED Online." *Oxford English Dictionary*, http://dictionary.oed.com.libproxy.nps.edu/entrance.dtl (accessed February 29, 2008).

Posner, Richard A. *Countering Terrorism*. Lanham, MD: Rowman & Littlefield Publishing Group, 2007.

Posner, Richard A. *Preventing Surprise Attacks.* Lanham, MD: Rowman & Littlefield Publishing Group, 2006.

Posner, Richard A. *Uncertain Shield – The U.S. Intelligence System in the Throes of Reform.* Lanham, MD: Rowman & Littlefield Publishing Group, 2006.

President Clinton. *Presidential Decision Directive 63 – Critical Infrastructure Protection.* Washington, D.C.: The White House, 1998.

President George W. Bush. *Executive Order 13388 – Further Strengthening the Sharing of Terrorism Information to Protect Americans.* Washington, D.C.: The White House, 2005.

President George W. Bush. *Guidelines and Requirements in Support of the Information Sharing Environment.* Washington, D.C.: The White House, 2005.

President George W. Bush. *Homeland Security Presidential Directive 7 - Directive on Critical Infrastructure Identification, Prioritization, and Protection.* Washington, D.C.: The White House, 2003.

President George W. Bush. *National Strategy for the Physical Protection of Critical Infrastructure and Key Assets.* Washington, D.C.: The White House, 2003.

Prime Minister Blair, "Our Nation's Future – Multiculturalism and Integration." Number 10 Downing Street, http://www.number-10.gov.uk/output/page10563.asp (accessed February 29, 2008).

Prime Minister Tony Blair. *Countering International Terrorism: The United Kingdom's Strategy*. London, UK, HM Government, 2006.

Program Manager – Information Sharing Environment (ISE). "Establishing the Interagency Threat Assessment and Coordination Group." *Information Sharing Environment*, http://www.ise.gov/docs/reports/ITACG-CDA.pdf (accessed June 22, 2008).

Program Manager – Information Sharing Environment (ISE). "Guideline 2 – Common Sharing Framework." *Information Sharing Environment*, http://www.ise.gov/docs/guidance/guideline%202%20-%20common%20sharing%20framework.pdf (accessed June 22, 2008).

Program Manager – Information Sharing Environment (ISE). *Annual Report to the Congress on the Information Sharing Environment.* Washington, D.C.: Government Printing Office, 2007.

Program Manager, Information Sharing Environment. *ISE Implementation Plan.* Washington, D.C.: ISE, 2006.

Ratcliffe, Jerry H. "Intelligence-led Policing." Australian Institute of Criminology, *Trends & Issues in Crime and Criminal Justice*, no. 248 (April 2003), http://www.aic.gov.au/publications/tandi/ti248.pdf (accessed April 4, 2008).

Sageman, Marc. *Understanding Terror Networks*. Philadelphia: University of Pennsylvania Press, 2004.

Scott, John P. *Social Network Analysis: A Handbook*. Thousand Oaks, CA: SAGE Publications, 2000.

Senate Select Committee on Intelligence. *The Intelligence Community's Involvement in the Banca Nazionale del Lavoro (BNL) Affair*. Washington, D.C.: U.S. Congress, 103rd Congress, 1st session, 1993.

Transportation Security Administration. *Threat to Passenger Rail Systems – National Railroad Passenger Corporation (AMTRAK) and Alaska Railroad Corporation – SD RAILPAX-04-02*. Washington, D.C.: Department of Homeland Security, 2004.

[redacted]

United States Congress. The Constitution of the United States. Washington: U.S. Government Printing Office, 2006.

Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001. Public Law 107-56. 107th United States Congress. (October 2001).

Watts, Duncan J. *Six Degrees – The Science of a Connected Age.* New York, NY: W.W. Norton, 2003.

Zimbardo, Philip. *The Lucifer Effect*. New York, NY: Random House, 2008.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California