



**NAVAL
POSTGRADUATE
SCHOOL**

MONTEREY, CALIFORNIA

THESIS

**COLLECTING AND CONNECTING THE DOTS:
LEVERAGING TECHNOLOGY TO ENHANCE THE
COLLECTION OF INFORMATION AND THE
DISSEMINATION OF INTELLIGENCE**

by

Patrick A. Burke

September 2009

Thesis Advisor:
Second Reader:

Robert Simeral
Richard Bergin

Approved for public release; distribution is unlimited

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE September 2009	3. REPORT TYPE AND DATES COVERED Master's Thesis	
4. TITLE AND SUBTITLE Collecting and Connecting the Dots: Leveraging Technology to Enhance the Collection of Information and the Dissemination of Intelligence		5. FUNDING NUMBERS	
6. AUTHOR(S) Patrick A. Burke		8. PERFORMING ORGANIZATION REPORT NUMBER	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000		10. SPONSORING/MONITORING AGENCY REPORT NUMBER	
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) Washington D.C. Metropolitan Police Department 300 IN Ave, N.W. Washington D.C. 20001		11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. government.	
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited		12b. DISTRIBUTION CODE A	
13. ABSTRACT (maximum 200 words) <p>Developing a national strategy to effectively coordinate information sharing and the subsequent dissemination of intelligence is paramount in domestic efforts to thwart future acts of terror and suppress crime. Past failures illustrate the need for strong and trustworthy partnerships not only between federal, state, local and tribal law enforcement, but also with relevant partners in the private sector, foreign allies and other government agencies. Standardizing operations and better utilizing technology will improve the efficacy of this effort and will draw upon the domestic law enforcement community as key players in this endeavor.</p> <p>The findings and recommendations proffered in this research identify policies and practices that effectively integrate information sharing in to all aspects of policing and provide for technological solutions to enhance capabilities for collecting information and disseminating intelligence. Integrating intelligence-led-policing in to existing community policing strategies also illustrates the utility of both public and private partners in this effort. Ultimately, the enhanced collection of information and dissemination of intelligence will greatly augment the ability of law enforcement and the myriad of relevant stakeholders to prevent both crime and acts of terrorism.</p>			
14. SUBJECT TERMS Suspicious Activity Reporting (SAR), information sharing, intelligence-led policing, DC Metropolitan Police Department, eGuardian, Federal Bureau of Investigation, dissemination of intelligence, program management information sharing environment (PM-ISE), information sharing environment (ISE), British police service, Joint Terrorism Task Force (JTTF), Joint, Terrorism Analysis Center (JTAC), domestic intelligence			15. NUMBER OF PAGES 107
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	18. SECURITY CLASSIFICATION OF THIS PAGE Unclassified	19. SECURITY CLASSIFICATION OF ABSTRACT Unclassified	20. LIMITATION OF ABSTRACT UU

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

**COLLECTING AND CONNECTING THE DOTS: LEVERAGING
TECHNOLOGY TO ENHANCE THE COLLECTION OF INFORMATION AND
THE DISSEMINATION OF INTELLIGENCE**

Patrick A. Burke
Assistant Chief of Police, DC Metropolitan Police Department
B.S., State University of NY College at Buffalo, 1988
M.S., Johns Hopkins University, 2000

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

**NAVAL POSTGRADUATE SCHOOL
September 2009**

Author: Patrick A. Burke

Approved by: Robert Simeral
Thesis Advisor

Richard Bergin
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Developing a national strategy to effectively coordinate information sharing and the subsequent dissemination of intelligence is paramount in domestic efforts to thwart future acts of terror and suppress crime. Past failures illustrate the need for strong and trustworthy partnerships not only between federal, state, local and tribal law enforcement, but also with relevant partners in the private sector, foreign allies and other government agencies. Standardizing operations and better utilizing technology will improve the efficacy of this effort and will draw upon the domestic law enforcement community as key players in this endeavor.

The findings and recommendations proffered in this research identify policies and practices that effectively integrate information sharing into all aspects of policing and provide for technological solutions to enhance capabilities for collecting information and disseminating intelligence. Integrating intelligence led-policing into existing community policing strategies also illustrates the utility of both public and private partners in this effort. Ultimately, the enhanced collection of information and dissemination of intelligence will greatly augment the ability of law enforcement and the myriad of relevant stakeholders to prevent both crime and acts of terrorism.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I.	INTRODUCTION.....	1
A.	PROBLEM STATEMENT	1
B.	RESEARCH QUESTIONS.....	2
C.	LITERATURE REVIEW	4
D.	VIABLE SOLUTIONS.....	6
E.	RESEARCH METHODOLOGY	8
F.	SIGNIFICANCE OF RESEARCH	9
	1. The Literature	9
	2. Future Research Efforts.....	9
	3. Immediate Consumers.....	9
	4. Homeland Security Practitioners and Leaders Nationally	9
II.	THE CURRENT STATUS OF THE DOMESTIC INTELLIGENCE ENVIRONMENT.....	11
A.	THE INTELLIGENCE PROCESS.....	11
	1. Requirements.....	11
	2. Planning and Direction.....	12
	3. Collection	12
	4. Processing and Exploitation.....	13
	5. Analysis and Production	13
	6. Dissemination	13
B.	THE CURRENT INFORMATION SHARING ENVIRONMENT	15
C.	SIGNIFICANCE OF EXPANDING THE COLLECTION OF INFORMATION AND THE NEED FOR MEGACOMMUNITIES.....	16
D.	THE ROLE OF TECHNOLOGY IN ENHANCING THE INFORMATION SHARING ENVIRONMENT	21
III.	TRANSITIONING TO INTELLIGENCE-LED POLICING	23
A.	THE EXPANDING ROLE OF FUSION CENTERS	23
B.	THE ROLE OF COMMUNITY POLICING.....	26
	1. Introduction and Importance of Community Policing.....	27
	2. Pros and Cons of Maintaining a Focus on Community Policing and Incorporating Intelligence-Led Policing.....	29
	3. Considerations.....	31
C.	COMPARATIVE ANALYSIS: WHAT AMERICA CAN LEARN FROM THE UNITED KINGDOM.....	32
D.	RECOMMENDATIONS FOR IMPLEMENTING IDENTIFIED APPROACHES.....	38
	1. JTTF Model.....	39
	2. Sharing Intelligence	39
E.	EXPANDING THE ROLE OF PUBLIC AND PRIVATE PARTNERS..	41
F.	LEVERAGING TECHNOLOGY TO REACH AN EXPANDING POOL OF CONSUMERS (THE DC EXPERIENCE).....	43

1.	Metropolitan Police Department (MPD) Overview.....	44
IV.	THE FUTURE OF DOMESTIC INFORMATION SHARING.....	47
A.	TEMPERATURE BOARD INITIATIVE—A NEW VIEW IN SHARING.....	47
B.	SUSPICIOUS ACTIVITY REPORTS (SAR)—LAW ENFORCEMENTS BEST HOPE FOR COLLECTING AND CONNECTING THE DOTS.....	50
1.	Administrative.....	52
2.	Legal Criteria	52
3.	Technology	52
4.	Potential Courses of Action / Recommendation Metropolitan.....	52
a.	<i>Status Quo</i>	52
b.	<i>Agencies and Regions Build their own System</i>	53
c.	<i>Use Accepted Technology for Analyzing Data</i>	53
5.	The Institutionalism of a Counterterrorism Outlook for the Law Enforcement Community and Beyond.....	54
C.	TECHNOLOGY STUDY	58
1.	Evaluation of the FBI’s eGuardian Program.....	58
2.	Evaluation of the Program Manager–Information Sharing Environment Program.....	59
D.	BEYOND TECHNOLOGY: IMPLEMENTATION ISSUES AND POTENTIAL REMEDIES TO ADDRESS THEM.....	62
1.	Policy Guidelines.....	62
2.	Training	62
3.	Technology	62
E.	CASE STUDY: THE LOS ANGELES POLICE DEPARTMENT SAR IMPLEMENTATION	63
F.	SAR AND INFORMATION SHARING DURING THE 56TH PRESIDENTIAL INAUGURAL.....	66
V.	REALIZING THE GOALS OF THE NATIONAL STRATEGY FOR INFORMATION SHARING	71
A.	STRATEGY FOR ACHIEVING THE VISION.....	71
1.	Value Innovation for Enhancing the Collection and Dissemination of Domestic Information/Intelligence	71
2.	Blue Ocean Strategy for Enhancing the Collection of Information and Dissemination of Intelligence.....	72
B.	POLICY RECOMMENDATIONS AND CONCLUSION	74
1.	Strategy for Bringing Innovation to Fruition.....	74
a.	<i>Value Innovation</i>	74
b.	<i>Planning</i>	75
c.	<i>Organizational Structure</i>	75
d.	<i>Leadership</i>	75
e.	<i>Collaborative Advantage</i>	77
2.	Interagency Strategic Planning Process for the Implementation of Suspicious Activity Reporting (Synopsis).....	77

C.	LIMITATIONS OF RESEARCH AND RECOMMENDATIONS FOR FUTURE RESEARCH ISSUES.....	78
D.	CONCLUSION	80
	LIST OF REFERENCES	83
	INITIAL DISTRIBUTION LIST	89

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

Figure 1.	FBI Intelligence Cycle (From FBI, 2009)	14
Figure 2.	The Dynamic Tensions Inherent in a Megacommunity (From Gerencser, M., Kelly, M., Napolitano, F. & Van Lee, R. 2009).....	18
Figure 3.	Continuum of Implementation Variables of ILP (From Carter, 2007).....	30
Figure 4.	Notional SAR Process (From BJA, 2008)	51
Figure 5.	Two-Dimensional Typology to Team Information Sharing and Team Outcomes (From Mesmer-Magnus & DeChurch, 2009)	55
Figure 6.	Evaluation Criteria	61
Figure 7.	Value Innovation (From Kim & Mauborgne, 2005).....	71
Figure 8.	Strategy Canvass, Blue Ocean Strategy (From Kim & Mauborgne, 2005).....	72
Figure 9.	Power Versus Interest Grid (From Kim & Mauborgne, 2005).....	74

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

American law enforcement executives are progressively acknowledging the relevance of information sharing and the criticality of intelligence in guiding their decision making pertaining to both crime and counter-terrorism strategies. As roughly three quarters of the state, local and tribal law enforcement agencies in the United States have fewer than 24 sworn officers, they are largely unable to have personnel dedicated to intelligence positions and thus rely on partner agencies, including federal law enforcement, to fill intelligence voids. Concomitantly, as these organizations have close interaction with the communities they patrol on a daily basis, the federal government and non-federal allies equally rely on them to gather and share intelligence and raw information. In order to improve homeland security as well as public safety, law enforcement at the tribal, state and local levels must be equipped with the necessary tools and resources for collecting, receiving and sharing information and intelligence. Technology serves as a significant component of this process and provides for considerable opportunities to include the public sector, private sector and community at large in this collaborative task of safeguarding neighborhoods from both crime and terrorism.

On June 9, 2009, the Secretary of Homeland Security signed a management directive, which identifies the mission, goals and responsibilities for state and local law enforcement under the purview of the Department of Homeland Security. Within that directive, Secretary Napolitano addressed the importance of non-federal partners in Section V, “Policy and Requirements,” which reads in part, “It is the policy of DHS to make state, tribal, and local law enforcement agencies full partners in homeland security policymaking and to coordinate their input of these partners across the Department” (DHS Directive #252-11, Revision #00). Just as the old African Proverb states, “It takes a village to raise a child,” this thesis argues that it takes a community, or what will be referred to as a “megacommunity,” to effectively fight crime and terrorism. Additionally, it will detail the means for achieving this goal.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Few endeavors, whether personal or professional, are both meaningful and possible without the support of those we love, those we work with and those who are committed to making a positive difference in the world. This thesis project and this course work was no exception. My deepest thanks go to my wife, Nora, and our four children, Bride, Molly, Brendan and Claire. Beyond my work hours, they sacrificed greatly to support my academic and professional efforts. I'm extremely fortunate to work for a "meta-leader," Chief Cathy Lanier of the DC Metropolitan Police Department, who grasps the importance of collaboration and breaking down barriers in order to suppress both crime and terrorism. I would also like to thank the men and women of MPD's Homeland Security Bureau—specifically our WRTAC personnel and members of the Special Operations Division—who work tirelessly to keep our city safe and who constantly strive to improve the way we do business.

Special thanks to Commander Joannie McNamara of the Los Angeles Police Department for her work on SAR and guidance in MPD's implementation efforts. Our federal government partners at DHS, DNI and the FBI have also offered exceptional support and guidance in my studies, and I am thankful for their trust and confidence. The faculty and staff at the Center for Homeland Defense and Security have provided their insight, knowledge and commitment to the development of their students as the homeland security leaders of today and tomorrow and are truly remarkable individuals. I owe a special note of gratitude to my thesis advisor, Robert Simeral, and my second reader, Richard Bergin, for their support, wisdom and patience in guiding me through my research.

With the knowledge and support of these many individuals, I am better prepared to look at homeland security from a new perspective and persevere in the challenges that an increasingly complex world present. As remuneration to my mentors and those who

have supported me, I promise to commit myself to serving the public with excellence and empathy, while seeking to make my community and my country a safe and desirable place to live.

I. INTRODUCTION

A. PROBLEM STATEMENT

Homeland Security Presidential Directive (HSPD-8) addresses the topic of national preparedness and, specifically, the need to “prevent and respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal” (Department of Homeland Security [DHS], 2003). Leveraging technology is essential in achieving this preparedness goal and specifically in closing the intelligence gaps, which have been a deficiency for the intelligence community for many years.

Since the terrorist attacks of September 11, 2001, there has been a substantial amount of literature devoted to the failures of the intelligence community. Among the six problems identified by the 9/11 Commission in describing the need to restructure the intelligence community were: the complexity and secrecy of intelligence sharing, the lack of common standards and structural barriers to performing joint intelligence work. In regard to structural barriers, it stated:

National intelligence is still organized around the collection disciplines of the home agencies, not the joint mission. The importance of integrated, all source analysis cannot be overstated. Without it, it is not possible to “connect the dots.” (National Commission on Terrorist Attacks upon the United States [9/11 Commission], 2004, p. 408)

Preventing future terrorist attacks in the United States poses a number of challenges as well as opportunities for today’s homeland security professionals. Strengthening information and collaboration capabilities are paramount in supporting the country’s national preparedness goals under the pillar of prevention. Within the District of Columbia, improving and standardizing the methods to collect, document and analyze information that could be relevant to either foreign or domestic terrorism are a priority for

the Metropolitan Police Department (MPD) in seeking to keep the community safe. This same methodology can be used by law enforcement agencies nationwide to advance their intelligence operations.

The current law enforcement philosophy pertaining to counter-terrorism espouses the belief that the nation's state, local, tribal and federal officers play an indispensable role in preventing terrorism. However, the majority of law enforcement efforts in collecting intelligence have been archaic and inefficient in that the information collected is not adequately handled and passed on for review. Likewise, in situations where intelligence is sufficiently analyzed, in many cases, it is not expediently transformed into a product that is relayed to the officers in the field who need it most. As the 9/11 Commission noted when speaking to the importance of integrated all-source analysis, "No one component holds all the relevant information" (9/11 Commission, 2004, p. 408).

As standardization and common methodology are critical to the information sharing process, a potential solution that has been presented by the Major Cities Chiefs Association is discussed in a recent white paper, in which recommendations are made for remediation, including the standardization and institutionalization of suspicious activity reports (SAR). This recommendation regarding use of SARs, if implemented successfully, has the potential to address the current inadequacies and could provide the link between persons and/or activities with a nexus to terrorist activities. Furthermore, adopting this tenet seeks to transition law enforcement officers from traditional response roles to active participants in prevention (Major Cities Chiefs Association, 2008, p. 5). With over 830,000 police officers interacting with communities on a daily basis, failing to capitalize on using these resources to proactively address terrorism would be a monumental failure (Bureau of Justice Assistance [BJA], 2009).

B. RESEARCH QUESTIONS

This thesis will examine the inadequacies of the existing information sharing environment in the law enforcement community and seek to ameliorate these deficiencies through implementing a program to expand the capacity to collect, analyze and share information through standardized technological solutions. A coordinated information

sharing effort will allow relevant stakeholders to access previously uncollected or inaccessible information and will foster a collaborative, comprehensive information sharing environment. This thesis also seeks to enhance domestic intelligence collection by expanding beyond the law enforcement community. The primary research question that this thesis seeks to answer is:

How can the intelligence community enhance homeland security through an extensive and standardized effort to amass and disperse information? The metric used to define enhance in this context refers to the preempting of future terrorist attacks through increasing the number of partners participating in the information sharing environment.

In seeking to answer this question, this thesis research will also address a second tier of questions including:

1. What types of technology can be leveraged to enhance this process, ensure privacy and provide for the security of classified information?
2. Where are law enforcement communities currently falling short in their mission of collecting and disseminating intelligence and how can they improve these efforts by expanding their pool of resources?
3. How can suspicious activity reporting be implemented and customized to meet agency needs as well as those of the greater information sharing environment?
4. How can current human intelligence (HUMINT) collection at the local level be augmented by reaching out beyond the traditional law enforcement community?
5. How will community policing efforts be impacted by law enforcement's emerging focus on counterterrorism and information collection?
6. What lessons can be learned from other countries and outside the law enforcement realm pertaining to technology, organizational structure and information sharing that can successfully be applied to improve the information sharing environment in the United States?

C. LITERATURE REVIEW

In the fore word of the *National Intelligence Strategy* published in 2005, the Director of National Intelligence, John Negroponte, specifically used the term “collaborative” in describing the new approach to national intelligence (Office of the Director on National Intelligence). While much research has been done on the failures of intelligence and the need to change, there is less exploration into the proven remedies for these shortcomings. The Director of National Intelligence (DNI) further recognized that the domestic intelligence mission would be significantly enhanced when state and local intelligence was combined with that of the intelligence community (Office of the Director of National Intelligence, 2005).

As the need for transforming intelligence is explored in greater depth than the research pertaining to solutions, the first question that this literature review addresses is: Where are law enforcement communities falling short in their mission of collecting and disseminating intelligence? Although the majority of the literature on shortcomings was produced after September 11, in 1996, a Clinton administration commission on the roles and capabilities of the United States intelligence community recognized that “the intelligence must be closer to those it serves” (Commission on the Roles and Capabilities of the U.S. Intelligence Community, 1996). In a joint inquiry into the intelligence community activities before and after the terrorist attacks of September 11, 2001, it was determined that the intelligence communities’ failure to coordinate information in an adequate and timely manner was a critical factor in their inability to detect and preempt these events. The *National Strategy for Homeland Security* also noted the need for comprehensive intelligence in the law enforcement community as part of its strategic objectives (DHS, 2007).

Beyond the collection and dissemination of intelligence, it is also important to distinguish the difference between information and intelligence, as intelligence is essentially information that has been analyzed. As Gregory Treverton (2005, p. 17) points out in a Rand publication, “The need to reshape analysis is dramatic. Current and future threats to the United States are global and adaptive, blurring distinctions between crime,

terrorism and war.” This statement summarizes the magnitude that analysis plays in formulating patterns from information that is almost always incomplete.

One of the challenges in implementing change to rectify this dilemma may lie in the organizational structures of law enforcement and intelligence agencies themselves. In her article “Institutional Origins of the 9/11 Intelligence Failure,” Amy Zegart (2005) writes that government agencies were not built to adapt to change as they have “more constraints face more conflicting mission with less managerial discretion and fewer resources than private sector firms do” (p. 492). While she gives a number of examples as to how the situation has improved to some extent, she highlights the need to better understand the organizational weaknesses that are barriers to change.

In characterizing the utility of the available sub-literature to illuminate the historical inadequacies of the intelligence sharing process, the majority of the literature is relatively recent, with a substantial increase subsequent to the terrorist attacks of September 11. While the literature ranges in the breadth of its scope, it is largely undisputed by even those who were criticized as playing a role in the breakdowns. There were two main sectors contributing too much of the research in this area. The first sector was government, who vigorously investigated intelligence failures through methods such as after action reports and congressional hearings. The second sector was academia, through mainly books and scholarly articles. Of the literature covered in this specific realm, the *9/11 Commission Report* (9/11 Commission, 2004), which was written after the review of more than 2.5 million pages of documents in seeking to discern how these events happened, is probably the most prominent record shaping the discourse of this subject. While it does a great service in documenting the causes leading to the failures of the intelligence community pertaining to this specific event, it fails to give explicit guidance on successfully implementing reforms throughout the law enforcement population.

D. VIABLE SOLUTIONS

The next set of sub-literature on this topic addresses the question of how to address the self failures of the intelligence community. More precisely, this research pertains to the role of law enforcement within the intelligence community and the current deficiencies in the collection and dissemination of information. Since the attacks of September 11 there has been much more discussion in this arena. The majority of the literature was made up of journal articles and papers written by academia, government officials and police professionals seeking to correct the problem. In searching for methods to improve police response in supporting the war on terrorism through intelligence sharing, fusion centers have emerged as a regularly accepted method of meeting this task. The Department of Homeland Security is currently seeking to further this process by creating a national network of fusion centers. This federally supported effort is designed to assist state, local and tribal law enforcement in standardizing practices and improving their capacity to both receive and share information.

Fusion centers, such as the Washington Regional Threat Analysis Center in Washington, D.C., seek to provide centralized, multi-agency, information and intelligence sharing, along with analysis of data to enhance the operational effectiveness and efficiency of the myriad of agencies in the National Capital Region (NCR) in both crime prevention and homeland security. As these centers continue to mature, there is frequent discussion as to what constitutes best practices in this discipline as well as the materialization of virtual fusion centers.

Intelligence-led policing (ILP) is also an emerging topic of discussion in the law enforcement community, which seeks to assimilate intelligence into the agency mission. While many agencies are practicing this doctrine, it remains largely undefined in policy and will remain this way until it is recognized as more than philosophy and ingrained in agency guidelines. It is characterized as:

An underlying philosophy of how intelligence fits into the operations of a law enforcement organization. Rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the overall mission of the organization. (Carter, 2007, p. 1)

Groups with significant status in the law enforcement community, such as the International Association of Chiefs of Police, Major Cities Chiefs Association, the Police Foundation and the National Organization of Black Law Enforcement Executives have embraced this philosophy and recognize the value of intelligence in thwarting both crime and homeland security threats. In a Bureau of Justice Assistance document, which discusses intelligence-led policing (2005), the value of patrol officers is recognized as a vital source for the collection of information. Likewise, this document highlights the fact that many law enforcement agencies lack the guidance, policies and technical acuity to further these objectives.

While the sub-literature addressing options for fixing the intelligence problems offer a number of alternatives that appear fundamentally accepted, the implementation of these alterations are relatively new or still in the process of being executed. As many programs and projects are still in the formative stages, there are many questions that remain unanswered in this quest to benchmark what would be perceived as a best practice in the industry. In the domain of intelligence collection, for instance, there were a variety of opinions on who should be collecting intelligence. The Center for Policing Terrorism, for example, perceives firefighters to be an integral tool in the collection and dissemination of terrorism related intelligence.

In researching different fusion center concepts, the core questions that came to mind dealt with the analysis and dissemination of information. Specifically, one of the lingering issues is the role of the professional intelligence analyst in police work and the possibility of replacing police officers with intelligence experts. While an entire thesis could be written on this topic, it is widely agreed that analytical standards are needed along with improved training and enhanced technology to standardize the seamless exchange of information. The National Information Exchange Model (NIEM) is one example of an effort that seeks to improve this electronic exchange through

standardization and consistency in vocabulary and specifications. In an August 2009, meeting of the Major Cities Chiefs Associations Intelligence Commanders Conference, agencies surveyed reported using a variety of analysts, from contractors to injured officers who were serving in this capacity until their return to street duty.

E. RESEARCH METHODOLOGY

Research for this thesis will follow three approaches: a literature review explores smart practices being employed in the current information sharing environment and policy that supports those practices. Secondly, case studies of the suspicious activity reporting implementation and information sharing processes were conducted using the Los Angeles Police Department and the Washington, D.C., Metropolitan Police Department. As the SAR initiative is in its infancy, the Los Angeles Police Department has the most comprehensive program in existence thus far—and will therefore be the primary agency examined. The DC Metropolitan Police Department implemented its SAR initiative just prior to the inauguration of President Barack Obama and used SAR extensively during this event and pre-planning period. These case studies will illustrate the goals, processes, challenges and successes as a result of this information sharing initiative and other technological tools that are currently in use.

In using case studies as a research method for this project, the foundational knowledge approach was used to provide a systematic technique for reviewing events, collecting and analyzing the relevant data and reporting results. This specific methodology was used as the analysis pertains to contemporary events, which included direct observation of the occurrences as well as personal interviews with people involved in these incidents. In Robert K. Yin's book (2008) on case study research, he prescribes the case study method when "how and why questions are to be the focus of the study" as was the case with this particular research project.

As technology plays a vital role in this process, an analysis was also conducted of certain platforms that are currently available to achieve the identified collection and sharing goals of the SAR program. An internal (DC Metropolitan Police Department)

comparison and critique of the Federal Bureau of Investigation's (FBI) eGuardian and the program management information sharing environment (PM-ISE) was also evaluated.

F. SIGNIFICANCE OF RESEARCH

1. The Literature

This thesis proposal will document the efforts of the law enforcement community to implement a quality solution to a challenge that has been vexing the intelligence community for many years. While this remains a work in progress, the literature involved is in the formative stages and will continue to evolve as this process expands.

2. Future Research Efforts

This proposal seeks to stimulate further discussion into smart practices for information sharing between local, state, tribal and federal agencies. Additionally, it provides future opportunities to explore government information sharing initiatives with the public and private sectors.

3. Immediate Consumers

The immediate benefit of this thesis is that it will greatly enhance the amount of information being collected as well as the quantity of information accessible for analysis and subsequent dissemination. Patrol officers, private sector employees and the community at large (to name a few) will play a progressive role as collectors of information. The intelligence community will also be benefactors as it will have access to an expanded pool of information. Law enforcement, government entities and the community at large will ultimately be empowered to take on a proactive posture and collaboratively improve the nation's ability to anticipate and preempt threats.

4. Homeland Security Practitioners and Leaders Nationally

As the gathering and distribution of information has been largely inadequate and perplexing, this research will provide options for both local and national leaders to

address these issues. Furthermore, as standardization and consistency are paramount in enriching this process, this thesis will provide policy guidance for aiding in this progression.

II. THE CURRENT STATUS OF THE DOMESTIC INTELLIGENCE ENVIRONMENT

A. THE INTELLIGENCE PROCESS

The *National Strategy for Information Sharing* (White House, 2007) prescribes that “Our success in preventing future attacks depends on our ability to gather, analyze, and share information and intelligence regarding those who want to attack us, the tactics that they use, and the targets that they intend to attack.” While the terms information and intelligence are used interchangeably in many situations, it is important to distinguish the difference. Perhaps one of the simplest definitions is provided by Dr. David Carter, who describes intelligence as information that has been analyzed. From a law enforcement perspective, he defines intelligence as follows:

In the purest sense, intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy direction to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists and terrorists.” (Carter, 2002)

In describing how the intelligence process works, most experts refer to a cycle, which essentially delineates a process path. At any stage in this cycle, the need may arise to go back to a previous stage for additional information or define additional requirements. Many models of the intelligence cycle include between five and seven stages. The model portrayed below, which is used by the Federal Bureau of Investigation, includes six stages commencing with requirements. The following overview describes the various stages of the intelligence process:

1. Requirements

Requirements consist of the type of information that the policy or decision makers need to help guide their decisions. For local law enforcement, this could include gang

activity or other relevant information that would be essential for protecting a community. On a national scale, the requirements would demarcate the information needed to protect the country. The Director of National Intelligence sets the requirements based on critical information and in participation with key stakeholders such as the Attorney General and Federal Bureau of Investigation. Questions pertaining to how much information should be collected and what priorities exist frequently rely on capabilities and rely on the policy maker to set.

2. Planning and Direction

As the intelligence cycle is consumer driven, **planning and direction** are frequently seen as beginning and end stages as finished intelligence products often result in requirements for new information. This stage of the cycle entails the management of the process from discerning what type of information is needed to meeting the intelligence needs of the consumer.

3. Collection

Collection entails the amassing of raw information that has not yet been processed and analyzed to create an intelligence product. There are a number of collection disciplines that are regularly referred to as the INTs. These INTs include the following: HUMINT: human intelligence, intelligence derived from human sources; MASINT: measurement and signatures intelligence, provided through the analysis of physical attributes of targets; OSINT: open-source intelligence, publicly available information; SIGINT: signals intelligence, information obtained from data transmissions including communications, electronics and foreign instrumentation and IMINT/GEOINT: image intelligence/geospatial intelligence, information used to describe, depict and locate physical features and human activities taking place anywhere on earth. Each of these disciplines has obvious advantages and disadvantages. Due to cost or complexity, many of these would be unavailable to the majority of state, local and tribal law enforcement agencies. Activities such as interviews and surveillance are more habitually utilized at this level.

4. Processing and Exploitation

Processing and Exploitation consists of translating the raw information from an array of sources into a format that is functional for the intelligence analysts. This process may include language translation and the reduction in the volume of data available for analysis.

5. Analysis and Production

The process of converting the raw information into an intelligence product is known as **analysis and production**. In this stage, subject matter experts (analysts) evaluate the relevance and veracity of the available information in order to create an intelligence product and make assumptions pertaining to potential inferences derived from their conclusions.

6. Dissemination

Dissemination is the relatively standardized process that involves the moving of the intelligence product from the producers to the consumers. Agencies typically have a product line to handle the needs of the consumer they are preparing the intelligence for. This would consist of products such as briefings, bulletins and longer-term estimates. The FBI for example, disseminates information in three standard formats: "Intelligence Information Reports (IIRs), FBI Intelligence Bulletins, and FBI Intelligence Assessments. FBI intelligence products are provided daily to the Attorney General, the President, and to customers throughout the FBI and in other agencies" (Federal Bureau of Investigation [FBI], 2009). See Figure 1.



Figure 1. FBI Intelligence Cycle (From FBI, 2009)

While this process may not be flawless and may not provide a complex multi-dimensional overview, it does accurately portray the essential ingredients of the intelligence cycle. The greater issue in this process seems to lie in the dissemination of the intelligence product. Additional hindrances such as the over-classification of intelligence products, structuring analytic techniques for improving intelligence analysis and failing to share intelligence with all relevant stakeholders remain a continuing challenge. In March of 2009, the U.S. government released a tradecraft primer, which provides a formative overview of the analytic techniques. In May of 2009, the White House issued a press release to the heads of executive departments and agencies in reference to classified and controlled unclassified information seeking recommendations

for increased transparency and provide for greater public disclosure of information. These documents represent the foundation for improving the intelligence and information sharing process.

B. THE CURRENT INFORMATION SHARING ENVIRONMENT

While the creation of the Department of Homeland Security in November of 2002 sought to remedy the complexities involved with the lack of unity between an abundance of agencies in protecting the United States, over six years later, there are a number of issues yet to be resolved. From an intelligence perspective, the major change that took place was the creation of the Director of National Intelligence (DNI), which occurred in 2004—subsequent to the release of the *9/11 Commission Report*. Considered by many to be the largest intelligence restructuring in the United States since World War II, the DNI was essentially deemed the head of national intelligence.

The impetus for the Intelligence Reform and Terrorism Prevention Act of 2004 was “the concern that agencies did not share intelligence well” (Lowenthal, 2006). Unlike the director of central intelligence preceding him, the DNI is not connected to any specific agency but has control over all of them and is tasked with insuring that the agencies are sharing intelligence throughout the intelligence community. With 16 agencies comprising the U.S. intelligence community (IC), one of the challenges for the DNI is to work through some of the existing territorial issues that inhibit operational effectiveness. The executive branch agencies and organizations that comprise the IC are responsible for providing intelligence that is necessary for the protection of the national security of the United States. The intelligence they collect is imparted to the President, National Security Council, Secretaries of State and Defense, as well as other officials of the executive branch of government. The government consequently uses this intelligence to guide policy on national security issues to include military actions and international negotiations.

Another effort aimed at improving intelligence sharing in the United States involves the expansion of Joint Terrorism Task Forces (JTTFs). Initially created in 1980 (New York City) with an emphasis on crime, these task forces are now operating in 100

cities throughout the United States and play a major role in tracking down leads relating to terrorism. Working through the National Joint Terrorism Task Force, these groups combine the resources of federal, state, local and tribal law enforcement to comprehensively investigate all acts related to terror. Among the successes claimed by JTTFs is the breaking up of cells on American soil to include the “Lackawanna Six,” the “Portland Seven” and the Northern Virginia Jihad. In Washington, D.C., members of the Metropolitan Police Department assigned to the JTTF regularly respond to bomb threats, white powder calls and incidents with a nexus to terrorism, while also handling an array of cases to include those with ties to international terrorism. Fusion centers and suspicious activity reports (SAR’s) are also adding to this list of initiatives and are described in subsequent chapters of this paper.

While the efficacy of JTTFs can be debated, one of the clear impediments is that it would be impossible for every law enforcement agency to have representation. Therefore, greater efforts are required to share information with agencies that are not currently included. Likewise, with tightening budgets at all levels of government, many state, local and tribal leaders are evaluating the performance of task force members to see if they could better be utilized for local functions.

C. SIGNIFICANCE OF EXPANDING THE COLLECTION OF INFORMATION AND THE NEED FOR MEGACOMMUNITIES

With the decentralization of many criminal and terrorist entities, the domestic intelligence capacity of the law enforcement community should evaluate its current practices and consider embracing change in order to keep up with the predicament that devolution from an organization to a network poses. Sharing information between agencies, both horizontally and vertically are essential as local, national and international borders do not apply to these expanding criminal networks. Expanding networks thus require the law enforcement community to use similar arrangements to address this quandary and shift from traditional policing paradigms. Likewise, law enforcement networks must consider expanding beyond the law enforcement community to cast out a virtual net that will include an array of both public and private sector agencies—as well

as the community at large—in an effort to enhance the volume of information collected. According to Secretary Napolitano in her confirmation statement, “The federal government can’t do this alone” (Napolitano, 2009). This same principle may apply to all levels of government. As the private sector has responsibility for roughly 85 percent of the nation’s critical infrastructure, partnerships are not only needed, but are critical. This network includes facilities such as hospitals, laboratories, chemical plants and power companies. The individuals responsible for handling sensitive materials must be trained to identify and report suspicious behavior or purchases that require circumspection.

Counterterrorism strategies, including information sharing initiatives, may require innovative approaches that call for greater integration and holistic leadership to look at the big picture as opposed to working within the confines of agency walls. As stated on President Barack Obama’s White House Home Page (2009), “The information we collect must be analyzed as well as shared, and we must invest in our analytic capabilities and our capacity to share intelligence across all levels of government.” Beyond the law enforcement community and governmental organizations, both the business community and civil society have important roles in keeping our nation safe. In the book *Megacommunities* (Gerencser, M., Kelly, M., Napolitano, F. & Van Lee, R., 2008) this interdependent approach is explored in depth and offers a compelling argument for greater collaboration to address increasingly complex issues. Former President George W. Bush proclaimed the importance of information sharing in a 2003 speech in which he stated:

All across our country we’ll be able to tie our terrorist information to local information banks so that the front line of defeating terror becomes activated and real, and those are the local law enforcement officials. We expect them to be a part of our effort; we must give them the tools necessary so they can do their job.” (Department of Justice, 2008)

While this statement underscores the realization that the federal government has to work beyond traditional boundaries, the law enforcement community as a whole should consider the benefits of forming collaborative information sharing networks with both public and private partners to attain a more comprehensive depiction of existing threats. This megacommunity approach to combating terrorism through a broadening of

communities and organizations espouse the belief that a change in orientation is needed as no individual agency or community can achieve this goal on its own.

As homeland security is a shared issue in which all communities have both a stake, as well as some sense of urgency, the foundation exists to create and sustain a viable conduit. With all groups working in the same space and required to balance decision making responsibilities as well as roles, they operate and maintain what is referred to as a “dynamic tension” that is channeled and sustained through a cross-culture dialogue. The concept of dynamic tension is illustrated in Figure 2.

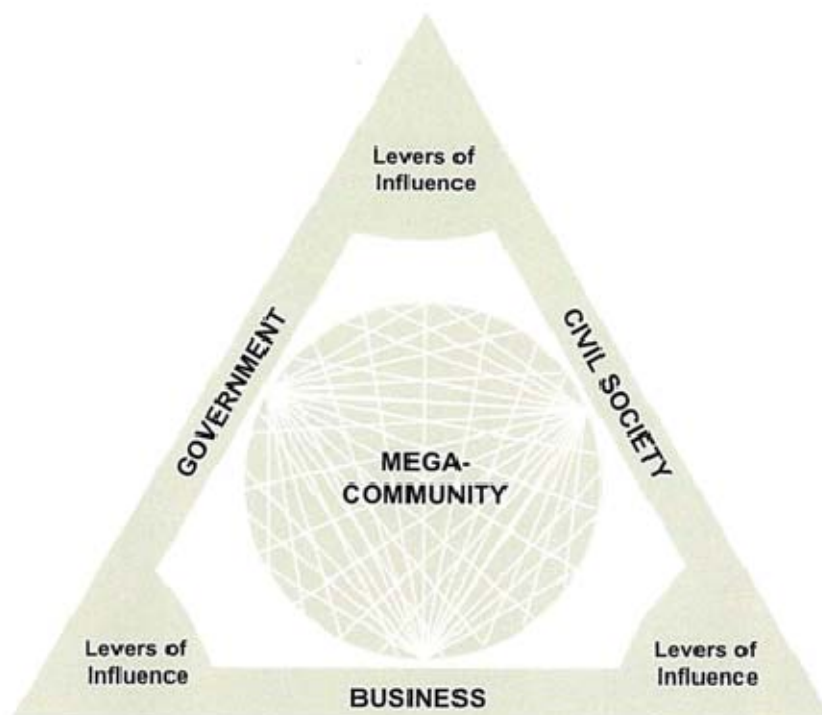


Figure 2. The Dynamic Tensions Inherent in a Megacommunity (From Gerencser, M., Kelly, M., Napolitano, F. & Van Lee, R. 2009).

One of the challenges in maintaining this dynamic tension is that no one sector should dominate as a constant state of negotiation needs to take place. With government at the forefront of this effort, leadership from this segment needs to be cognizant of the requisite to relinquish power in order to maintain the balance. This does not mean an abdication of responsibility for spearheading this relationship, as “initiators” are essential

to put implementation processes in place. Instead, it requires that the initiators be prepared to relinquish their leadership roles as the community comes together. Just as “Starfish systems,” as described by Braffman and Beckstrom (2006) in their book *The Starfish and the Spider*, work together as a network; there is no centralized hierarchy and, thus, no president or CEO of the megacommunity. This seemingly chaotic environment allows for unhindered innovation and encourages creativity that would otherwise be muted in a traditional hierarchy.

Within these “megacommunities,” there are five elements identified that are deemed critical and needed to move this strategy forward:

1. **Tri-Sector Engagement** includes the civil society element, which is frequently missing in conventional public-private partnerships. From an information sharing perspective, this would include education and strong outreach to the community.
2. **Overlapping in Vital Interests** pertains to the mutual interest that individual communities have in a particular issue, which compels them to work in a megacommunity environment for the common good. As homeland security permeates all three sectors, this common interest exists, but must receive a heightened sense of urgency.
3. **Convergence** describes the mutual commitment to action that all community members must maintain as a goal.
4. **Structure** portrays the necessary guidelines that enable the group to congregate around essential interests in which there is mutual overlap. This structured governance will set standards for the network to follow, and provide for the technology and resources to meet those standards.
5. **Adaptability** refers to the ability for the three sectors to be both flexible and balanced in order to meet the needs of the other participants as well as their individual group requirements. (Gerencser et al., 2008)

Changing leadership styles to meet the demands of today and in the future is also a consideration for immediate as well as long term success. Within this framework, a leadership definition that meets this classification is what is known as “meta-leadership.” As described by authors Marcus, Dorn and Henderson (2005), meta-leaders are people “who are able to influence and accomplish such collaboration of effort across organizations—multijurisdictional, multiagency and public/private.” With the emerging

threats of terrorism and asymmetric methods for carrying out attacks, meta-leaders must be responsive to their organization as well as the community at large. According to the authors, “These leaders connect with, influence, and integrate the activities of diverse agencies, thereby motivating interaction, enhancing communication, and engendering the sort of cross-organizational confidence necessary for effective terrorism preparedness and emergency response” (Howitt & Piangi, 2003).

In order to implement this strategy of creating a megacommunity to amend the existing information sharing process and preempt future acts of terror, the five elements listed above must all take shape with each sector taking part and assigning capable leaders to the various roles. As this network has many interactive elements and relies on a dynamic synergy it can be classified as a “complex system.” As Snowden and Boone (2007) write, “Complexity is poised to help current and future leaders make sense of advanced technology, globalization, intricate markets, cultural change, and much more.” Effectively leading within a complex context requires law enforcement to: engage in interactive communications, establish rules for the group, encourage “attractors”—to gain and encourage momentum—encourage debate and diversity and manage starting conditions, while monitoring for emergence of new opportunities.

With the major law enforcement entities adopting the suspicious activity report process to improve the communication between law enforcement agencies, the initial steps are in place to duplicate efforts within the other sectors of the megacommunity. In order to maintain trust, it is crucial to ensure that all partners are well-educated as to the goals, objectives and responsibilities that each party bears and to ensure that all privacy policies are being strictly followed. Failing to do so, could result in a retreat or complete withdrawal from this network. On the contrary, achieving this goal can result in an immensely powerful counterterrorism tool, which has the potential to dramatically alter the safety of the nation.

D. THE ROLE OF TECHNOLOGY IN ENHANCING THE INFORMATION SHARING ENVIRONMENT

With over 18,000 tribal, state and local law enforcement agencies committed to the homeland security mission, one of the reasons customary practices in collecting and sharing information have proved ineffective is the improper or under-utilized use of technology. Beyond the complexities of information classifications and the lack of personnel with adequate clearances, archaic systems have impeded the ability to get information to the appropriate platform for analysis. Likewise, once information is converted into an intelligence product, dissemination methods are often not capable of reaching vast amounts of relevant personnel, who may have the ability to take preventive action. As the American system of government empowers non-federal law enforcement agencies to take responsibility for the safety of their individual communities, it is equally important that they are equipped with the tools and knowledge needed to accomplish that mission.

In the information sharing domain, there are a number of unclassified as well as secret level and top secret—sensitive compartmented information (TS/SCI) level computer systems. At the unclassified level, many law enforcement agencies now have access to resources such as the Homeland Security Information Network (HSIN), which is the Department of Homeland Security's network for both developing threat information and distributing warnings and threat intelligence. Also popular amongst law enforcement is Law Enforcement Online (LEO), which is used by law enforcement professionals as well as the Federal Bureau of Investigation to communicate and share data. The Central Intelligence Agency (CIA), State Department and Department of Defense all maintain unclassified networks as well.

At the secret level and top secret—sensitive compartmented information level—there are 15 separate classified computer systems being used by the myriad of agencies and include networks for a range of consumers to include congress (CapNet), contractors (CWAN) and commonwealth partners (Stone Ghost). There are also six telephone and

fax networks in place for handling sensitive or classified information. Secure terminal equipment (STE's), for example, allow for secure conversations to take place via telephone.

While the intelligence community has evolved from a “need to know” to a “responsibility to provide” philosophy, this voluminous list of independent networks illustrates the need for greater integration of existing systems and a more collaborative information sharing strategy. Past debacles exemplify the fact that no single agency has an accurate portrayal of a real or perceived threat and that all agencies require access to additional sources to provide a truly comprehensive analysis. Likewise, the overwhelming amount of state, local and federal agencies have no access to the majority of these systems, which precludes them from obtaining an all-inclusive awareness of the situation as well. This chapter addresses the research question: *Where are law enforcement communities falling short in their mission of collecting and disseminating intelligence and how can they improve these efforts by expanding their pool of resources?*

Fusion centers have helped to fill some of the existing gaps, as well as “writing for release” to the relevant consumers. Additionally, fusion centers have addressed the research question pertaining to the efforts to improve information collection and dissemination through expanding the pool of resources. However, there are still voids that remain largely unfilled within the existing structure and are due primarily to the sheer volume of agencies. In this new information age, there are wide-ranging technologies available to enhance current processes and exponentially improve the possibilities that are realistically attainable.

Achieving this vision is the challenge for homeland security leaders at all levels. DHS Secretary Janet Napolitano has remarked that it is a priority for her agency to increase the exchange of information with state and local governments. Speaking before a House Committee on Homeland Security, she further stated, “How do we make sure that we have integrated intelligence with state and local officials and are sharing information adequately and on a real-time basis? That is one area that will be a major focus...As a former governor and state attorney general, I appreciate that need” (Napolitano, 2009).

III. TRANSITIONING TO INTELLIGENCE-LED POLICING

A. THE EXPANDING ROLE OF FUSION CENTERS

Beyond the transitions taking place on the federal level, there has also been a significant amount of progress taking place between the federal government and law enforcement at the state, local and tribal levels. *The National Strategy for Information Sharing* (White House, 2007) called for “a national information sharing capability through the establishment of a national network of fusion centers.” Fusion centers, which can be defined as “an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by merging data from a variety of sources,” (Department of Justice, 2003) provide a one-stop location for retrieving vital intelligence to support the needs of the community. These fusion centers, which are run by state and local governments, are continuing to evolve and standardize their capabilities, while simultaneously creating a formal apparatus for sharing information between the federal intelligence community and state/local/tribal governments. Secretary Napolitano told a House Panel in February of 2009, that DHS needs to better utilize information from fusion centers as part of their counterterrorism efforts. (Napolitano, 2009).

With the empowerment of local government to take a seat at the proverbial intelligence table, concerns pertaining to privacy and civil liberties were consequently recognized and continue to be addressed. In 2004, President Bush and the U.S. Congress established the Information Sharing Environment (ISE) “for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties” (Intelligence Reform and Terrorism Prevention Act of 2004). The same act that established the ISE also established the position of “Program Manager” to oversee this process. Since this time, fusion centers have evolved to encompass a wide array of capabilities with many considering or taking on an “all crimes/all hazards” approach. Beyond providing a mechanism for the collection, analysis and dissemination of information/intelligence, fusion centers are

showing promise in advancing efforts to detect, investigate, respond and prevent both criminal and terrorist acts. While their success remains largely unproven, current efforts aimed at establishing baseline capabilities and developing standardized fusion center guidelines is a step in the right direction in seeking to benchmark exceptional applications. An increased focus on collection has been, and will continue to be, paramount in furthering the aspect of prevention. In a Bureau of Justice Assistance publication entitled *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (2006, p. 4), it is recommended that “fusion centers adhere to these guidelines and integrate the key elements of each guideline to the fullest extent, in order to enhance information and intelligence sharing.”

Although these centers are in their relative infancy, incremental strides continue to be made in breaking down the barriers between the federal IC and state, local, and tribal agencies. In a hearing before a Senate Committee on Intelligence Reform in January, 2007, DC Police Chief Cathy Lanier recognized fusion centers as a means for improving information flow between local governments and their federal partners. (Lanier, 2007) Former DHS Chief Intelligence Officer Charles E. Allen also notes the utility of fusion centers, calling them a “key conduit” for sharing federal information and intelligence down to the local level. (Allen, 2007). Under the current system in place within the United States, the cooperative federalism that exists can pose a myriad of obstacles in the realm of information sharing—only some of which have been addressed by innovations such as fusion centers. According to the Bureau of Justice Statistics (2004), there are over 830,000 law enforcement officers in the United States, and nearly 18,000 separate state and local law enforcement agencies. As it would be impossible for every agency to have a person dedicated to a fusion center—or even dedicated to an intelligence function—smaller jurisdictions face even greater challenges gaining access to relevant intelligence.

While the larger metropolitan areas throughout the United States may be considerably more attractive to terrorists due to the critical infrastructure and key resources located within their jurisdictions, much of the planning (as demonstrated by the 9/11 attacks) can take place in suburbs or rural areas with less connectivity to the

intelligence community. This illustrates the need for even the smallest of police departments to seek out and maintain some type of intelligence capacity. The availability and access to current technologies make this potential ordeal a possibility for even those agencies in the most remote areas of the country.

The proliferation of fusion centers, such as the Washington Regional Threat Analysis Center (WRTAC) in Washington, D. C., have been integral in providing centralized, multi-agency, information and intelligence sharing to enhance operational effectiveness and efficiency to the myriad of agencies in the National Capital Region (NCR) in both crime prevention and homeland security. This is evident in the increasing number of agencies assigning analysts to participate in the center. The 15 analysts currently embedded include personnel from Metro Transit, U.S. Capitol Police, DC Department of Health, DC Fire and Emergency Medical Services, FBI, Court Services and Offender Supervision Agency and Montgomery County Police. The distribution of open source products has expanded beyond the U. S. to eight foreign countries, and has grown to serve approximately 30,000 readers. (WRTAC, 2009). In order to increase the effectiveness of this center, and fusion centers nationwide, greater strides need to be taken in the collection and analysis of information. If law enforcement seeks to truly embrace a philosophy of intelligence-led policing, which attempts to provide strategic integration of intelligence into the mission of the organization, the implementation of SAR may be one of the mechanisms for achieving this.

Beyond the institutionalization of counterterrorism in the law enforcement realm, the 72 fusion centers currently operating in the United States have the potential to play a vital role in addressing major crime issues. In a recent address by Homeland Security Secretary Janet Napolitano, she stated in prepared remarks:

At the Department of Homeland Security, information and intelligence sharing is a top priority, and fusion centers play an important role in helping to make that happen. In the world we live in today, it's critical for federal, state, local and tribal entities to know what the others are doing so each can operate effectively and efficiently. (Napolitano, 2009)

B. THE ROLE OF COMMUNITY POLICING

With the burgeoning technology in this post-9/11 world, many state, local and tribal police agencies nationwide are making a logical transition to intelligence-led policing or making greater use of intelligence for police operations. Intelligence-led policing is defined as:

A business model and managerial philosophy where data analysis and crime intelligence are pivotal to an objective, decision-making framework that facilitates crime and problem reduction, disruption and prevention through both strategic management and effective enforcement strategies that target prolific and serious offenders. (Ratcliffe, 2008).

As this transition takes place, the goal is not to replace traditional community policing efforts, but to engage police officers to take on a more active role as “preventers” of crime—rather than mere responders. Just as Chief William Bratton of the Los Angeles Police Department implemented Wilson’s Broken Windows Theory (Wilson & Kelling, 1982) in New York City to combat crime when he served as the chief there, the intelligence-led policing philosophy has the potential to transform police departments into proactive counter-terrorism agencies.

In order for any police agency working in a democratic society to be successful, it is imperative that law enforcement have the respect and trust of the communities it serves. This is why community policing plays such a vital role in law enforcement efforts to thwart future acts of terror. With over 830,000 police officers working in the 18,000 plus departments across the country, (Bureau of Justice Assistance, 2009) there is no one better suited to have the relationships and finger on the pulse than these assets. Sir Robert Peel makes an articulate assessment about the role of the police in his statement, “The police are the public and the public are the police; the police being only members of the public who are paid to give full time attention to duties which are incumbent on every citizen in the interests of community welfare and existence” (R. Peel, n.d., from Law Dog files). This theory reinforces that both the police and the community share a mutual role in the prevention of crime and that some version of community policing will forever be incorporated into currently practiced policing methods.

State, local and tribal law (SLT) enforcement agencies are cognizant of the fact that they cannot rely on the federal government alone to collect and disseminate information and/or intelligence; Hence, the burgeoning number of fusion centers and JTTF's (Joint Terrorism Task Forces) that have emerged. While these projects are still in the formative stages, they have served well to enhance the information sharing capabilities between SLT agencies and the federal government. The ability of non-federal police agencies to obtain information from community members is critical to the success of preemptive counterterrorism efforts and every law enforcement agency in America, regardless of its size, has a role in this national effort.

1. Introduction and Importance of Community Policing

Whether it is an attack on a school by an isolated individual, a homegrown or even foreign-borne threat, the reality is that terrorist or criminal plots are most likely to be detected at the grass roots level—in the communities in which they are planned. With strong connections to the communities through continued community policing efforts, local law enforcement officers are well suited to discern intelligence that will ultimately preempt an attack. Even foreign-born terrorists have shown an effort to assimilate into the communities in which they live in order to remain inconspicuous. In communities where law enforcement officers are well known and trusted, citizens are more likely to report suspicious behavior and approach law enforcement to make that notification.

As police departments transition to take on proactive roles as collectors of information, one of the ancillary challenges becomes what to do with the information they have collected. Putting classified information into a product that can be disseminated to the officer on the street remains a complex issue. Just as the *9/11 Commission Report* identified the federal government's failure to connect the dots, it is equally important that information obtained at the state/local/tribal levels be passed along, analyzed and transformed into actionable intelligence. In the realm of suspicious activity, it can also be argued that there is an active role for every American to be aware of what constitutes suspicious activity/behavior—and to report it when it happens. As police agencies develop intelligence-based collection models, it is imperative that community members,

and both private and public stakeholders, be actively engaged in this information sharing process. Partnerships with the community will forever be an integral part of any successful policing strategy as law enforcement alone does not have the resources to handle the vast amount of crime and disorder issues that inflict many neighborhoods.

Community-oriented policing (or some version thereof) has been the pervasive policing philosophy in the United States for nearly three decades. Mission statements have changed over this period to reflect the importance of maintaining the respect and trust of the community and building strong relationships between the police and the communities they serve. One of the major initiatives that commenced in the United Kingdom in the late 1990s, which is now being studied and implemented in parts of the United States, is the philosophy of intelligence-led policing. While there are a variety of definitions used to describe what constitutes intelligence-led policing, in relation to community policing, the Bureau of Justice Assistance describes it as follows: “Intelligence-led policing is a collaborative enterprise based on improved intelligence operations and community-oriented policing and problem solving, which the field has considered beneficial for many years” (2005). Remaining dominant in community policing efforts are the requisite citizen input, including tailored policing for local communities and the expansion of police functions beyond crime fighting to encompass order maintenance and preemptive crime suppression actions.

Historically, community policing in America has evolved from simple patrol studies to Wilson and Kelling’s (1982) “Broken Windows Theory,” which focused on the importance of police in protecting communities in addition to individual community members. In doing so, they highlighted the role of police in preventing crime rather than just reacting to it. Goldstein’s (1996), “problem-oriented policing” philosophy took community policing to the next level through the active involvement of community members in assessing problems and customizing a response to addressing the issue. Problem-oriented (Bureau of Justice Assistance, 2009) policing (POP) continues to incorporate the community as an active partner in working jointly with law enforcement to design solutions to identified problems as well as ranking the order of problems to be addressed.

CompStat, which is a police management tool that originated in New York City, (Henry, n.d.) continued the evolution of these models and all genres continue to incorporate intelligence aspects that illustrate the compatibility of community policing programs and intelligence-led policing. The successes achieved through these philosophies have resulted in both enhanced community relations as well as safer communities.

2. Pros and Cons of Maintaining a Focus on Community Policing and Incorporating Intelligence-Led Policing

Due to the small size of most American police departments, it may not be practical for every agency to have dedicated intelligence officers and/or analysts. Yet each agency does have a role to play in national intelligence operations and has the capacity to incorporate some level of intelligence-led policing strategy. Among these strategies include: modification of mission statements, adapting intelligence policies, participating in information sharing with state, local, tribal and federal partners and ensuring that legal safeguards are maintained in order to protect civil liberties and privacy. While altering policies and adapting to new ideas can be extremely burdensome, the positive sides of modifying intelligence strategies far outweigh the encumbrance of embracing this change. Emerging technologies allow law enforcement agencies to link to national intelligence databases through technology solutions and dedicated personnel can be assigned to positions as intelligence liaisons. These resolutions allow agencies that cannot staff fusion centers, Joint Terrorism Task Forces or other federal operations centers to both relay information to the relevant authorities and receive intelligence in return. Figure 3 represents the “continuum of implementation values of intelligence-led policing” and illustrates the need for external resources to advance their intelligence capacity.

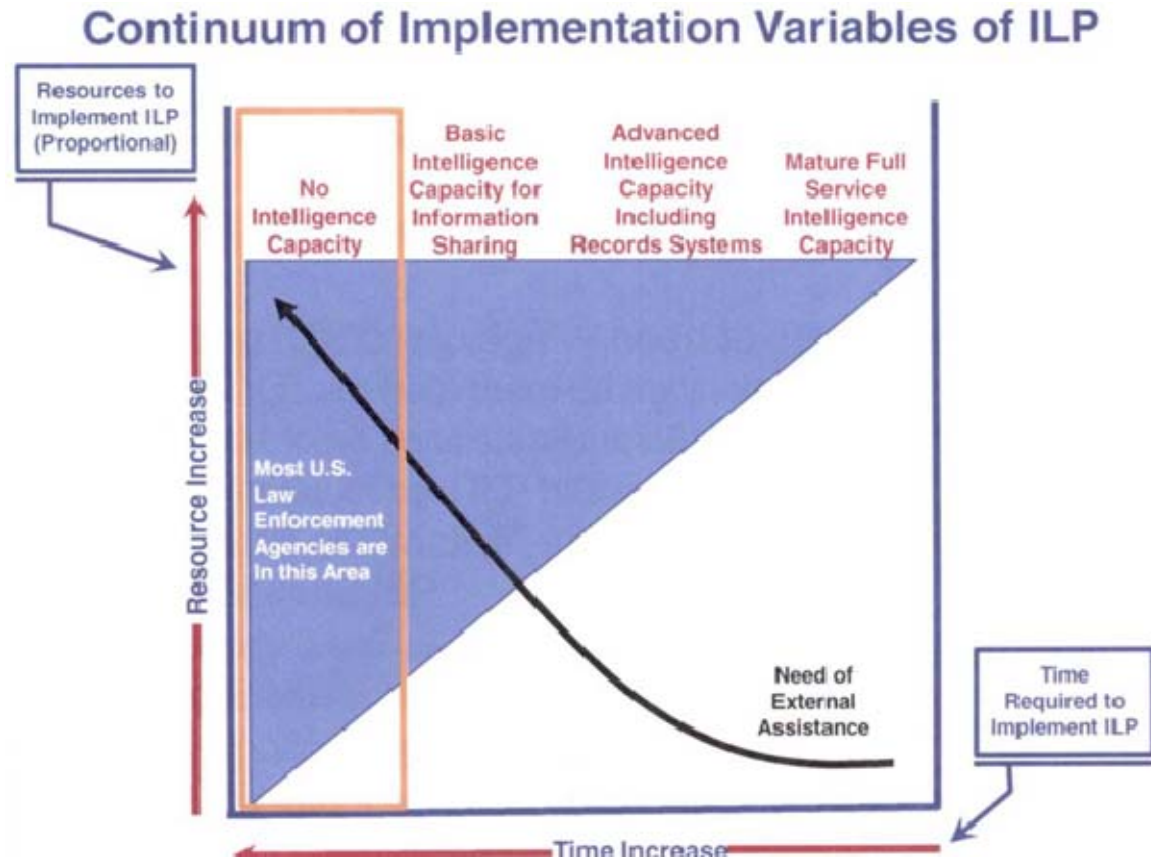


Figure 3. Continuum of Implementation Variables of ILP (From Carter, 2007)

In order for police officers to transition from their traditional roles of first responders to being active collectors of information, it is essential that they are actively engaged and working in close partnerships with the communities they serve. The primary dilemma this new transition promulgates is the retention of public trust while encouraging community members to provide information about suspicious activities occurring in their neighborhoods and potentially by their neighbors. With fusion centers and intelligence-led policing efforts mischaracterized by certain civil liberties groups and uninformed members of the public as secretive intelligence gathering and data mining centers, great efforts need to be made to ensure transparency and compliance with all regulations pertaining to privacy and civil liberties. Executive level support amongst agency heads is also essential in changing the culture of the organization to inculcate intelligence into the daily mission of the department. Once the commitment has been

made to this process, members at all levels of the agency must receive training on criminal intelligence. Consequently, efforts must expand beyond the law enforcement realm to actively employ both the private and public sectors as functional partners in this effort.

Innovative strategies such as anonymous tip lines, text messaging programs and alert systems now provide the public with real-time crime information and the ability to relay information to local law enforcement partners with increasing ease. Listservs, which are forums that transmit messages to a subscribed group via e-mail, also provide individual community members with the capacity to communicate directly with patrol officers assigned to their particular neighborhoods and further build the relationship through open two-way communication. Solid community partnerships will further enable the police to educate the public about activities that comprise suspicious and/or criminal behavior. The more knowledgeable the public is, the better equipped it will be to provide information on potentially illegal activity.

Applying intelligence-led policing strategies to community policing practices may significantly enhance the effectiveness of law enforcement in expanding the amount of information collected for analysis and subsequent dissemination. Beyond the realm of crime, the expansion of terrorist targeting to an array of soft targets including transportation, public health, financial institutions, energy, telecommunications, and a myriad of additional unconventional infrastructures further illustrates the need for increased teamwork in gathering and sharing information. Just as law enforcement bears risk in expanding its information sharing efforts, these policies also impact all partner agencies, who are participating in this endeavor and must also deal with individual agency policies, culture shifts and privacy laws.

3. Considerations

Based upon the need for greater collaboration with communities and the many public and private partners that work closely with law enforcement, executives may consider expanding upon existing community policing practices to ameliorate this issue of underutilized HUMINT. Intelligence-led policing as defined by the Manhattan

Institutes Center for Policing Terrorism (2006) provides the opportunity for all law enforcement agencies (regardless of size) with the ability to assume effective intelligence operations that can be equally applied to both crime fighting and counterterrorism efforts. Opportunities now exist for law enforcement agencies at the state, local and tribal levels to further their collaborative efforts in institutionalizing intelligence-led policing practices and expand the use of suspicious activity reporting processes beyond the police department to both public and private partners. Future research may explore the effectiveness of assigning state, local and tribal law enforcement agencies to play a lead role in regional fusion efforts as well as the benefits of staffing both JTTF and national operations centers. If not practical due to the size or resources of the agency, one option is to have a dedicated person, who can liaison to ensure that vital information is being shared. Advancing contemporary community policing efforts to fit this need will allow police agencies nationwide to bolster their efforts in defending communities against both crime and terrorism. This chapter confirms the role of community in answering the research question: *How will community policing efforts be impacted by law enforcements emerging focus on counterterrorism and information collection?* As law enforcement agencies take on a greater role in counterterrorism efforts and agencies become more reliant on intelligence, community policing will remain a fundamental practice of effective police organizations.

C. COMPARATIVE ANALYSIS: WHAT AMERICA CAN LEARN FROM THE UNITED KINGDOM

The failures of the American intelligence community to prevent the terrorist attacks of September 11, 2001 are well documented and remain fresh on the minds of intelligence professionals. Since that time, many efforts have been undertaken to correct these deficiencies to include the creation of fusion centers and Joint Terrorism Task Forces. The Homeland Security Act of 2002 established the Department of Homeland Security in order to “provide the unifying core for the vast national network of organizations and institutions involved in efforts to secure our nation” (DHS, 2009). In doing so, the Department of Homeland Security brought together over 180,000 persons

from 22 separate agencies into a cohesive entity. In amalgamating these organizations, the President sought to realign what was described as “the current confusing patchwork of government activities” (DHS, 2009).

Among the complex challenges hindering the information sharing process in the United States is the sheer volume of state, local, tribal and federal agencies that comprise and/or interact with the intelligence community. As relationships are integral for effectual sharing of information, the multitudes of agencies alone pose daunting obstacles.

In the United Kingdom, there were also a number of modifications made post September 11 which impacted both the intelligence agencies as well as the police. The transfer of many criminal justice centric accountabilitys from the Home Office to the newly created Ministry of Justice allowed for the Home Office to put greater focus on intelligence gathering, counter terrorism and substantive police operations. A newly created Office for Security and Counter-Terrorism (OSCT) was also created to manage the operations of the Home Office. In the realm of information sharing, the United Kingdom has significantly fewer principal intelligence agencies and law enforcement organizations. Laws in the United Kingdom also allow for greater domestic options for arrest and detention.

While there have been arguments for the creation of a domestic intelligence agency in the United States, which would be comparable to the MI5 in the United Kingdom, this analysis will focus on the United Kingdom’s intelligence-led policing efforts and the sharing of domestic information between the law enforcement and intelligence communities within the existing organizational structures. Consequently, recommendations will be proffered for incorporating the most effective practices identified through this comparative analysis into the American model.

The tragic events of September 11, 2001, had a profound impact on many countries beyond the United States, including the United Kingdom. While the British have a long history in dealing with domestic terrorism, much of which dates back to the early 1900s, this specific occurrence resulted in an increased focus on Muslim extremism. It should be noted that the focus on international terrorism did not occur subsequent to

this attack, as the United Kingdom originally shifted counter-terrorism efforts after negotiating the Northern Ireland peace process. Prior to that point, the British had an evolving strategy to deal with the Irish Republican Army (IRA) terrorist threat, which included tactics such as government censorship, prohibitions on gatherings and the ability to arrest and detain individuals on arrest warrants for prescribed periods of time. These powers, which would run contrary to the United States Constitution, provide for fewer civil liberties but have served as a considerable tool in government efforts to thwart acts of terror. This 42-day holding period allows British authorities adequate time to perform searches and carry out both interviews and IT research that often prove critical in bolstering their case.

Among the immediate changes that did take place in the UK as a result of the 9/11 attacks were a comprehensive review of preparedness and contingency plans and a renewed effort to reinstitute indefinite detention. Beyond the convergence of the intelligence community on the threat of Muslim extremism, the British intelligence community also directed its efforts to the use of unconventional weapons and established a Joint Terrorism Analysis Center (JTAC). Similar to fusion and JTTF efforts undertaken in the United States to increase the capacity for information sharing between government entities, the JTAC is located at MI5 and is staffed with personnel from law enforcement and relevant stakeholder agencies. While the JTAC does not play an operational role, as the JTTFs do in the United States, it relieves the operational agencies of encumbering intelligence as they prepare intelligence briefs for the central government, which is based upon assessments obtained from their intelligence agencies.

Since its inception in 2003, the JTAC has come to be known as an effective analytical resource in addressing international terrorist threats against the United Kingdom and its interests. The JTAC is also responsible for setting the threat level (comparable to the DHS role in the United States) and issuing warnings. According to the UK's intelligence Web site:

The Head of JTAC is accountable directly to the Director General of the Security Service, who in turn reports to the Joint Intelligence Committee on JTAC's performance of its functions. An Oversight Board, chaired by the Cabinet Office, ensures that JTAC meets customer requirements by monitoring the effectiveness of JTAC's systems for engaging with customer departments. (UK Intelligence Community, 2009)

In contrast to the 16 agencies encompassing the intelligence community in the United States, the British system consists of three primary agencies: the MI5, MI6 (Secret Intelligence Service) and the Government Communication Headquarters (GCHQ). The MI5, which is also known as the Security Service, has responsibility for national security and domestic threats. The MI6 has the responsibility for providing the UK government with information on persons, events, etc. on foreign soil. The Government Communications Headquarters handles primarily signals intelligence, including electronic communications. Similar to the U.S. intelligence shifts subsequent to the collapse of the Soviet Union, the United Kingdom has evolved to take on a greater role in issues such as domestic terrorism, drug trafficking and organized crime. Unlike the U.S. system, where the Director of National Intelligence is the sole person with oversight of national intelligence, the MI5 reports to the home secretary, while MI6 and GCHQ report to the Foreign Secretary.

In distinction to the multitude of law enforcement agencies in the United States that have the capacity and authorities to collect intelligence related to terrorism, the UK has streamlined this process. Unlike the U.S., where the majority of agencies have no representative assigned to a fusion center, JTTF or specific intelligence function, all British police agencies have a dedicated unit, which are known as a Special Branch (SB). The officers assigned to SBs are scrutinized, trained and directed by the MI5 to collect intelligence in support of national security investigations. Within the London Metropolitan Police, there are two specific units that address counter-terrorism. The SO12 (Special Operations) was created in the late 1800s in response to violence conducted by Irish Nationalists and the SO13 (also known as the Anti-Terrorist squad). Both of these units were restructured in October of 2006 into the formation of SO15, which is also known as the new Counter Terrorism Command.

The Counter Terrorism Command has a number of goals pertaining to tactical and intelligence accountabilities. Primary intelligence objectives include the following:

- To bring to justice those engaged in terrorist, domestic extremist and related offenses
- To provide a proactive and reactive response to terrorist, domestic extremist and related offenses, including the prevention and disruption of terrorist activity
- Support the National Coordinator of Terrorist Investigations outside London
- To gather and exploit intelligence on terrorism and extremism in London
- To assess, analyze and develop intelligence to drive operational activity
- To engage in partnership with London's communities in order to understand their concerns and to provide reassurance and support where needed
- To provide specialist security advice and services internally and externally
- To provide an explosive ordnance disposal and CBRN capability in London
- To assist the British Security Service and Secret Intelligence Service in fulfilling their statutory roles
- To be the police single point of contact for international partners in counter-terrorism matters
- Assisting in the protection of British interests overseas and the investigation of attacks against those interests (Metropolitan Police, 2009)

The other benefit that British agencies possess is their ability to connect directly to MI5 through an IT link. This network provides for the rapid circulation of intelligence both horizontally and vertically, and incorporates all relevant stakeholders. In essence, the SB's and IT link bestow every police agency in the United Kingdom with access to requisite intelligence. With a much smaller system than in the U.S., the establishment of this link is a far easier task.

According to the UK's Home Office, there are 52 total police forces in England, Scotland, Northern Ireland and Wales (Home Office, 2009). In England and Wales alone, there are "140,500 police officers, 14,000 volunteer special constables and 13,400 community support officers" (Home Office, 2009). The primary difference between the U.S. and its British counterparts is that all police forces in the UK operate under the oversight and direction of the Home Office as opposed to a multitude of state, local and federal government entities. While British chiefs control and direct their regional forces, a central overseer of police operations provides an inherent benefit in ensuring the efficacy of interagency information sharing. The Home Office system also touts the ability to "prevent political interference in policing and avoid giving any single organization power over the entire police service" (Home Office, 2009).

Just as technology has proven to be critical for sharing information across agency boundaries in the United States, the United Kingdom also relies on national databases to facilitate this process. One current initiative is the "IMPACT Programme," which aspires to enhance information sharing of the police service throughout England and Wales. Just as SAR in the United States seeks to standardize information sharing practices, IMPACT also seeks to develop common standards for the management of police information through guidance as well as a statutory code of practice.

In order to ensure that police were effectively capturing relevant information pertaining to crime and/or terrorism in the British Police Service, the now defunct National Criminal Intelligence Service (NCIS) established national priorities through the publication of a National Intelligence Model (NIM). Since that time, the NCIS has been incorporated into the Serious and Organized Crime Agency (SOCA), which continues to use this model (in addition to Law Enforcement Agencies [LEA's]). The priorities recognized as taking precedent under this model include:

- The targeting of prolific offenders through overt and covert means.
- Managing crime and disorder hotspots.
- Identifying and investigating linked series of crime or incidents

- Applying prevention measures that include working with a broad range of other disciplines. (Naval Criminal Investigative Service, 2000) In essence, the intelligence service recognized the importance of intelligence in maximizing the efficiency of police resources by analyzing intelligence to interpret the criminal environment and provide decision makers with the opportunity to address crime hotspots and preempt criminal acts through proactive countermeasures. This effort, which ultimately came to be known as “intelligence-led policing” has altered policing efforts in both the U.S. and the UK in the realms of both crime fighting and homeland security. Within the United Kingdom, intelligence-led policing has become a mainstay in incorporating traditional community policing efforts and terror prevention programs.

Although ILP has been slower to evolve in the United States, this seems to be a logical progression of problem and community oriented policing efforts that recognize the importance of strong police interaction within the communities they serve. While some agencies may view ILP as terrorism-centric, the success of the New York Police Department’s (NYPD) CompStat program illustrated the success of basing deployments of police to areas where they could have the greatest impact on crime—or as Jack Maple (former NYPD) would say, “putting cops on dots” (Maple, 1999). As many pre-operational terrorist activities are likely to be discovered by either communities, the private sector or non-police entities, it is imperative that police agencies have strong relationships in place and the ability to efficiently collect, analyze and share relevant information.

D. RECOMMENDATIONS FOR IMPLEMENTING IDENTIFIED APPROACHES

While there is great disparity in the number of law enforcement agencies within the law enforcement communities of the United Kingdom and the United States and challenges in the coordination of information sharing, there are a number of lucrative efforts in place to advance this process. Leveraging technology to insure expedient exchange of information and providing greater access to information held by other agencies is paramount. Listed below are a number of comparative solutions that can be incorporated to enhance the effectiveness of information/intelligence sharing in the United States.

1. JTTF Model

The JTTF model employed in the U.S. and the JTAC in the UK were established with the intent of breaking down the barriers that can sometimes exist between federal and local law enforcement agencies. While the JTAC is non-operational and the JTTF does not have non-federal police officers from all state and local agencies participating, they both show efficacy in breaking down the communication barriers between federal officials and their counterparts on the state, local and tribal levels. State and local officers in the U.S. are also being assigned to federal counter-terrorism centers to play an even greater role in operations and rapid dissemination of information. In a recent meeting of local counter-terrorism officials with the Federal Bureau of Investigations International Terrorism Operations Center (2009), local officers were briefed on their roles in actively working cases as Task Force Officers (TFO's) and their empowerment to obtain warrants under the Foreign Intelligence Surveillance Act (FISA), and make operational decisions.

Recommendation—In order to increase the cooperation between state, local, tribal and federal agencies, agencies with the opportunity and resources to do so should assign officers to work with the JTTF, International Terrorism Operations Section (ITOS) and maintain desk positions or develop a liaison with both the National JTTF and at the National Operations Center (NOC). Based upon the analysis of the UK, it would be preferential to have every agency in the U.S. with some type of SB representation and an intelligence link to a federal intelligence entity. Nationally, as it would not be pragmatic in the United States to have every law enforcement agency represented within a JTTF, a technological solution to share intelligence, along with a designated point of contact (POC) is paramount to effectively providing intelligence from the higher echelons to the officers on the street. While the recommendation for a primary POC can be handled immediately, the discussion of an IT solution is discussed further in the second recommendation.

2. Sharing Intelligence

While the UK has far fewer IC and police agencies to facilitate information sharing between, the centralized reporting through the Home Office is not a possibility

under the cooperative federalist system in the United States. The U.S. system further complicates the challenges of passing actionable intelligence to the officer on the beat as there are no SB's (or comparable entity) within the vast majority of U.S. police agencies—and thus no counter-terrorism (CT) component.

Recommendation—In order to better facilitate the exchange of information and analysis of intelligence in the United States, it is recommended that the United States continue to employ the use of fusion centers to share information and provide intelligence pertaining to terrorism, criminal activity and all hazards events. Just as the United Kingdom has standardized intelligence and operational structures, it is recommended that a concerted effort be made to standardize best practices pertaining to fusion centers within the United States. With the publication of the U.S. Department of Justice's *Fusion Center Guidelines* and the consequent release of the Department of Justice's (DOJ) *Baselines Capabilities for State and Major Urban Area Fusion Centers*, these efforts are already underway. It is further recommended that the Department of Homeland Security, Department of Justice, and Office of the Program Manager, Information Sharing Environment (PM-ISE) continue to play an active role in coordinating these efforts.

It is equally important that these centers are in compliance with laws regarding the protections of privacy and civil liberties—specifically 28 Code of Federal Regulations (CFR) Part 23. Annual training is recommended to address this issue, and technology should be used to purge information that has no legal justification for being maintained. Law enforcement agencies should consider coordinating efforts with civil liberties groups to provide for transparency in operations and assure that regulations and policies are being appropriately followed.

Based on the United Kingdom experience, it is further recommended that all agencies access and maintain an IT link to a single intelligence service in order to support national security investigations and provide officers with situational awareness. The IT link to MI5 in the United Kingdom fills this void that is currently both widespread and largely unaddressed in the United States. Intelligence-led policing has proven to be a valuable tool in the United Kingdom and should continue to be expanded in the United States in conjunction with existing and evolving community policing efforts. Suspicious

activity reporting should become the standard operational procedure for all agencies in the U.S., regardless of size, with federal assistance and coordination in providing and accessing information from a centralized database. Technology and training are critical to this effort as many agencies lack the acuity and/or finances to implement an effective SAR program. Expanding the utility of law enforcement officers as collectors of information, and consequently private industry and other partners, will exponentially improve the likelihood of preempting the next terrorist attack.

The United Kingdom and the United States share a great commitment in protecting democracy, while at the same time bearing the accountability to keep their citizens safe from terrorism. Information sharing initiatives in both countries are continuing to progress in a manner consistent with the expanding threat. Global cooperation in identifying and bringing terrorists to justice will remain critical to the success and safety of both nations and the role of intelligence will continue to be a decisive factor. This section addressed the research question: *What lessons can be learned from other countries and outside the law enforcement realm pertaining to technology, organizational structure, and information sharing that can successfully be applied to improve the information sharing environment in the United States?* Applying the smart practices, being utilized in the UK and around the world, will aid the relevant agencies in reinventing currently used processes and other inefficiencies that have hindered progress in this realm.

E. EXPANDING THE ROLE OF PUBLIC AND PRIVATE PARTNERS

As intelligence functions in the realm of homeland security are predominantly law enforcement related, the central focus is primarily on tactical intelligence that passes on suspect information and criminal activity. To effectively integrate information sharing into all aspects of counterterrorism events, law enforcement at all levels should consider working beyond traditional paradigms and seek out the expertise of colleagues outside of law enforcement to build a capacity for strategic intelligence. Open source information, which comprises the majority of the products that are worked on, can be easily distributed both vertically and across agency boundaries. This strategic intelligence

approach will improve coordination regionally and proactively in mutual efforts to converge on future threats from an all-hazards perspective.

In working toward the goal of protecting the homeland, it is beneficial that the law enforcement, fire and emergency medical services and other key stakeholders have a general understanding of each other's roles and responsibilities, the history and current threats related to terrorism and the resources available to them. It is equally important that each agency has a select number of key personnel who are readily available, who have the following: specialized equipment, enhanced networking capabilities, specific training to identify signs of terrorism and the capacity to act as a liaison with inter- and intra-agency personnel.

The majority of current recruit and annual training programs are insufficient at keeping personnel abreast of the global trends in terrorist activity. Specific training programs are needed to bridge this gap, enhance inter-agency bonds, improve operational readiness and enhance the common operating picture. A consolidated training program for specially trained inter-agency members within geographical regions is also a necessary component for inter-agency readiness.

The *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing* (White House, 2007), also calls for the development of a collaborative process with input from members of the federal, state, local, tribal agencies and private sector from across the nation. Current systems for the collection of intelligence need to be standardized for credibility and assessed and disseminated in a consequential manner. The risk in neglecting to do so could result in information failing to be passed on to relevant personnel.

In leveraging relationships, information and resources to address terrorist threats as well as criminal incidents, the concerted focus on the collection, analysis and sharing of information should encompass the following course of action:

- Collecting and analyzing important information provided by as many public and private sources as possible;

- Dissemination of information to public and private networks, entities and personnel, based on “need” and “right” to know guidelines and in consideration of the responsibility to share that information;
- Collecting feedback on the information shared from these sources, which will be assessed from their own experiences, observations, contacts and records. More than one round of dissemination/sharing may be accomplished as feedback is received and additional opportunities are created to build upon the initial dissemination;
- Developing more and better information and “pictures” about people, their associates and potential threats (“enrichment”) based upon initial and subsequent rounds of disseminations; and
- End sharing and dissemination processes by circulating final, “enriched” information regarding each tip and lead to federal, state, regional and involved networks to further support individual and collaborative efforts designed to prepare for, mitigate against, respond to and recover from terrorist threats and activities.

F. LEVERAGING TECHNOLOGY TO REACH AN EXPANDING POOL OF CONSUMERS (THE DC EXPERIENCE)

Just a few short years ago, intelligence operations within the DC Metropolitan Police Department were conducted under the purview of the Office of the Superintendent of Detectives and were separated into three distinct entities, which were located at separate sites and with little interaction. While these units produced reports on patterns such as gang activity and affiliation, there were no formal processes in place to pass information on to the consumers or receive information from those same consumers. Information was typically obtained after a crime was committed, and usually when the investigating officer had reason to suspect some type of gang activity. Likewise, intelligence on homeland security related matters was shared at the higher echelons of the department but did not always make its way down to the officers in the field in a timely manner.

An analysis of existing processes indicated the lack of a database specifically to collect suspicious activity reporting. Likewise, the use of PD 76s (stop/contact information) proved insufficient for getting information into the hands of the appropriate personnel in an expedient manner. As this information was documented manually and

subsequently entered in to Columbo (a local police database), the potential existed for information to be lost. Failing to have an automated system also created a roadblock for intelligence analysts or detectives attempting to contact an officer to exchange or collect additional information that could further an investigation.

1. Metropolitan Police Department (MPD) Overview

The Metropolitan Police Department currently has 4,017 sworn members and is the seventh largest police organization in the country. In September of 2007, the Homeland Security Bureau was created by Chief Cathy Lanier and given oversight of both the newly formed Intelligence Fusion Division and Special Operations Division (SOD). The changes to the organizational structure of the MPD created the ability to incorporate an intelligence capacity into the daily activities and major events that are currently handled by SOD personnel. While the MPD has a robust Joint Terrorism Task Force and a small but dedicated Domestic Security Office (DSO), a major challenge was to ensure that all officers were trained and equipped to know the signs of terror and take preemptive measures. By combining MPD resources with the multitude of law enforcement and city agency resources available in the District of Columbia, the MPD has greatly expanded its abilities to deter terrorist events and improve response to both all-crimes and all-hazards situations.

In analyzing MPD's capacity to compete with the demands of committing resources to counterterrorism efforts and meeting the service needs of the community, it is important to understand the severity of crime in the District of Columbia. Like many major cities in the United States, the District has a serious level of crime to address. According to FBI statistics, in 2006, the rate of violent crime in Washington, D.C. was 1445.84 crimes per 100,000 residents (FBI, 2009). Among the cities reporting with a population of 100,000 or more, Washington ranked eighteenth in its rate of violent crime (FBI, 2009). As these numbers illustrate the challenges of committing resources, they also suggest the need for working in partnership beyond traditional boundaries.

Aside from the limitations and failures of federal law enforcement to share information that were identified in the *9/11 Commission Report*, the Commission's

concerns about the accessibility to interagency databases remains a problem. (9/11 Commission, 2004). Although strides with the law enforcement information exchange program (LINX) have improved the situation in the National Capitol Region, much work remains. The LINX program, which was started by the Naval Criminal Investigative Service and launched in DC in November of 2007, allows more than 60 local police agencies to access a common database. The challenge, however, lies in ensuring that members within the MPD, and throughout the region, are trained to use the system, are inputting data into the system and are standardizing policies for use.

Technology has also dramatically improved the ability for law enforcement officers to reach out beyond their walls to access information from both the public and private sectors. Initiatives such as MPD's tip line (888-919-CRIME) and text messaging tool (50-411) allows community members to provide immediate information regarding criminal or terrorist activity through easily accessible and anonymous means. This is in addition to the Terrorist Incident Prevention Program (TIPP), which is currently in place and targets the business community and service agencies.

DC's fusion center, known as the Washington Regional Threat Analysis Center (WRTAC) also provides a variety of intelligence products to law enforcement as well as the public and private sector to increase its levels of awareness and seeks information in return. These products, which rely on technology for distribution include:

- WRTAC Daily Summary: a law enforcement sensitive (LES) publication that is disseminated five times a week (the Monday edition covers Saturday and Sunday). This document provides a summary of local and national crime trends, local significant events, summary of the FBI field intelligence group (FIG) report, summary of closed source fire, health and officer safety-awareness issues. The distribution of this document has increased from 1200 to 5000 recipients since October of 2007.
- A bi-weekly officer safety and criminal intelligence issues product: Also LES, which provides a summary of national officer safety and intelligence related material.
- A weekly or bi-weekly fire watch product that discusses items of interest relating to the fire service, security, safety and terrorism.

- A daily open source brief (DOSB), which is distributed three to five times per week with no dissemination restrictions: This product is a compilation of open source media articles relating to homeland security, terrorism trends, public safety, public health, disaster preparedness and other subjects relevant to decision makers in the public and private sectors. The DOSB is being redistributed on Infr aGuard, Homeland Security Digital Library, Global Incident Map and through numerous local police departments, private businesses and military entities. The total distribution as of June 2009 was approximately 30,000 readers in the U.S. and 8 foreign countries. Notable groups who have requested DOSB distribution include: Naval Postgraduate Students, Senator Lieberman's Office, Pentagon Force Protection Agency, Bank of America Corporate Security and the U.S. DOE National Nuclear Security Administration.
- An MPD most wanted vehicles used in violent crimes bulletin: this law enforcement sensitive document is distributed weekly or more frequently as needed to citywide and regional law enforcement agencies with special attention to patrol divisions. This bulletin enhances the awareness of patrol officers for vehicles wanted in violent crimes throughout the city. These bulletins have also enabled cross-border enforcement initiatives, information sharing, and facilitation of arrest and recovery of property.

These products are augmented by an array of services, programs and initiatives, which seek to keep the relevant stakeholders well informed and equipped with the knowledge they need to protect themselves as well as their community. They also exemplify how human intelligence can be improved at the local level by reaching out to a greater number of both internal and external customers, which addresses the research question: *How can current human intelligence (HUMINT) collection at the local level be augmented by reaching out beyond the traditional law enforcement community?* Beyond the materials provided, structured meetings enhance the partnerships and allow for the stakeholders to further participate in this collaborative security effort.

IV. THE FUTURE OF DOMESTIC INFORMATION SHARING

A. TEMPERATURE BOARD INITIATIVE—A NEW VIEW IN SHARING

Disseminating information and actionable intelligence throughout an agency and across agency boundaries can pose a number of obstacles. Police officers, for example, are inundated with excessive information pertaining to crime, wanted persons, vehicles, etc. on a daily basis. With a short time typically allocated in roll calls to discuss these issues, as well as daily in-service training and other priority information, ancillary means of communicating vital information to the rank and file creates a dilemma. As roll calls are typically conducted at the beginning of an officer's shift, this sets an additional challenge of communicating information to officers that occurs subsequent to the time that they have taken their assignments. While communicating to officers via radio is one frequently used option, it can use substantial air time and is a one-dimensional method of communication, which may not be readily acted upon—pending the time of the particular simulcast.

One of the strategies recently implemented by the DC Metropolitan Police Department in order to improve this process and keep members abreast of real-time actionable intelligence, entails the use of “temperature boards.” While this is one tool in an arsenal, it has proved effective in accelerating regional information to critical stakeholders. In e-mail surveys completed by District commanders and command staff from their respective districts, they described the temperature board as an “excellent” means of providing up-to-date information and aiding in the arrest of numerous wanted subjects that are posted to the boards (Sgt. D. Jones, personal communication, July, 2009). As of July, 2009, more than 4,200 pictures and profiles of wanted persons have been displayed on internal and regional temperature boards. (Sgt. D. Jones, personal communication, July, 2009). Beyond the District of Columbia, the Washington Metropolitan Region is the eighth largest district in the United States with more than five million residents, while the District of Columbia is home to nearly 600,000 people. All three branches of the U.S. federal government are housed in the District of Columbia in

addition to 12 universities, the World Bank and the International Monetary Fund. As the nation's capital, Washington, D.C., has a significant number of museums, monuments, military bases and critical infrastructures that are considered high value targets for terrorists. The National Capital Region is also vulnerable to a myriad of hazards including infrastructure disruptions, hazardous material spills and severe weather. The District is also served by one of the nation's most frequently used public transportation systems (Washington Metropolitan Area Transit Authority) with an estimated 33 percent of the District's labor force using public transportation on a daily basis. As the Metropolitan Police Department plays a vital role in ensuring the safety of district residents, workforce and the roughly 20 million visitors that visit the city each year, the use of technology to disseminate information and intelligence is critical in carrying out this mission.

The amount of information available to law enforcement continues to increase exponentially. Specifically, the DC Metropolitan Police Department produces numerous threat reports, intelligence bulletins, crime information reports, etc. on a daily basis and provides a far greater amount of information than can possibly be consumed. Since the *9/11 Commission Report* identified unity of effort in information sharing as a priority, tremendous steps have been made to share information horizontally between the federal government and state, local and tribal law enforcement. The proliferation of fusion centers has also fostered a culture of collaboration that has moved beyond law enforcement to include agencies such as emergency management, health and fire. With the expanding base of collectors and consumers, the quantity of information continues to grow immensely.

With multiple systems and massive amounts of data available, current systems for providing actionable intelligence to patrol officers have been inadequate. Improvements in exchanging information and intelligence horizontally have not corresponded with an equally enhanced vertical flow of intelligence. The utilization of the temperature board is part of a comprehensive approach for improving both the horizontal and vertical

information and intelligence sharing process. As a robust intelligence system will further empower first responders to play a greater role as first preventers, technological applications must play a significant role.

In essence, the temperature board concept commenced using electronic liquid crystal display (LCD) temperature boards that were installed in each district roll call and executive complex to support the display of official department information. In order to provide real-time information to officers on the beat, the program was expanded to include mobile digital computers (MDC's), which are positioned in the scout cars and serve a variety of functions.

Temperature boards were designed to display current citywide department information on the left vertical half of the screen and unit specific information on the right vertical half of the screen. They were also designed to accommodate the display of scrolling administrative and lookout ticker information horizontally across the lower portion of the screens. This allows for officers to obtain immediate information pertaining to lookouts, wanted vehicles, etc. from a screen, which is literally at their fingertips. In addition to displaying information specific to events in Washington, DC, this concept has now expanded to include timely lookouts from jurisdictions within the National Capital Region as well as flash information on national or international incidents that may have either a direct or an indirect impact on the city.

The next stage for this program seeks to enhance situational awareness beyond the police department by expanding the temperature board initiative to local and federal law enforcement partners, as well as DC fire and other key partners. The expansion of this initiative will enable agencies to quickly gauge the "real-time" status of events/incidents occurring in and around the District of Columbia. Additionally, it will improve agency ability to disseminate actionable intelligence, provide real-time 911, computer assisted dispatch (CAD) and emerging crime trend information occurring within the National Capitol Region. The content for the temperature boards can be customized to fit the needs of the participating agencies and include only information deemed relevant to their mission.

B. SUSPICIOUS ACTIVITY REPORTS (SAR)—LAW ENFORCEMENTS BEST HOPE FOR COLLECTING AND CONNECTING THE DOTS

Improving and standardizing current methods to collect, document and analyze information that could be relevant to either foreign or domestic terrorism are a priority for ensuring a coordinated effort in keeping the nation safe. One of the promising programs currently underway in the United States is the nationwide SAR initiative. This project, which is sponsored by the Program Manager Information Sharing Initiative (PM-ISE) has garnered the support of all major law enforcement agencies including the International Association of Chiefs of Police, the Major Cities Chiefs Association (MCCA) and the National Sheriff's Association. While the concept of operations (CONOPS) was released in December 2008, substantial planning has been done and expectations are high for moving this project forward. *The National Strategy for Information Sharing* (White House, 2007) called for the federal government to “support the development of a nationwide capacity for gathering, documenting, processing, analyzing and sharing terrorism-related suspicious activity reports (SARs) generated at the local, regional, state or federal levels in a manner that rigorously protects the privacy and civil liberties of Americans.”

The Major City Chiefs Association (2008) released a white paper pertaining to the adoption of SAR entitled *Twelve Tenets to Prevent Crime and Terrorism*, which states:

Suspicious Activity Reports represent not only the means to identify and measure activities with a possible nexus to terrorism, but also the potential thread to connect fusion centers nationwide. As such, they should be standardized and institutionalized and, eventually, considered for inclusion in the Uniform Crime Reporting program, for a true information sharing environment. Undertaking this institutionalization and standardization of SARS will also support the transition of local law enforcement from their traditional role of “first responders” to the role of “first preventers” of a broad range of crimes including terrorist acts.

The SAR process essentially seeks to standardize this process and gives non-federal law enforcement a primary role in the collection of information. Technological support is also a critical component of this initiative as SARs are consequently posted to a server where they can be accessed by local, state, tribal and federal government as well

as fusion centers and other relevant stakeholders. Unleashing the largely untapped potential of America's front line law enforcement officers greatly enhances the potential to preempt crime or terrorism. Figure 4 illustrates how the SAR functional standard facilitates the information sharing process.

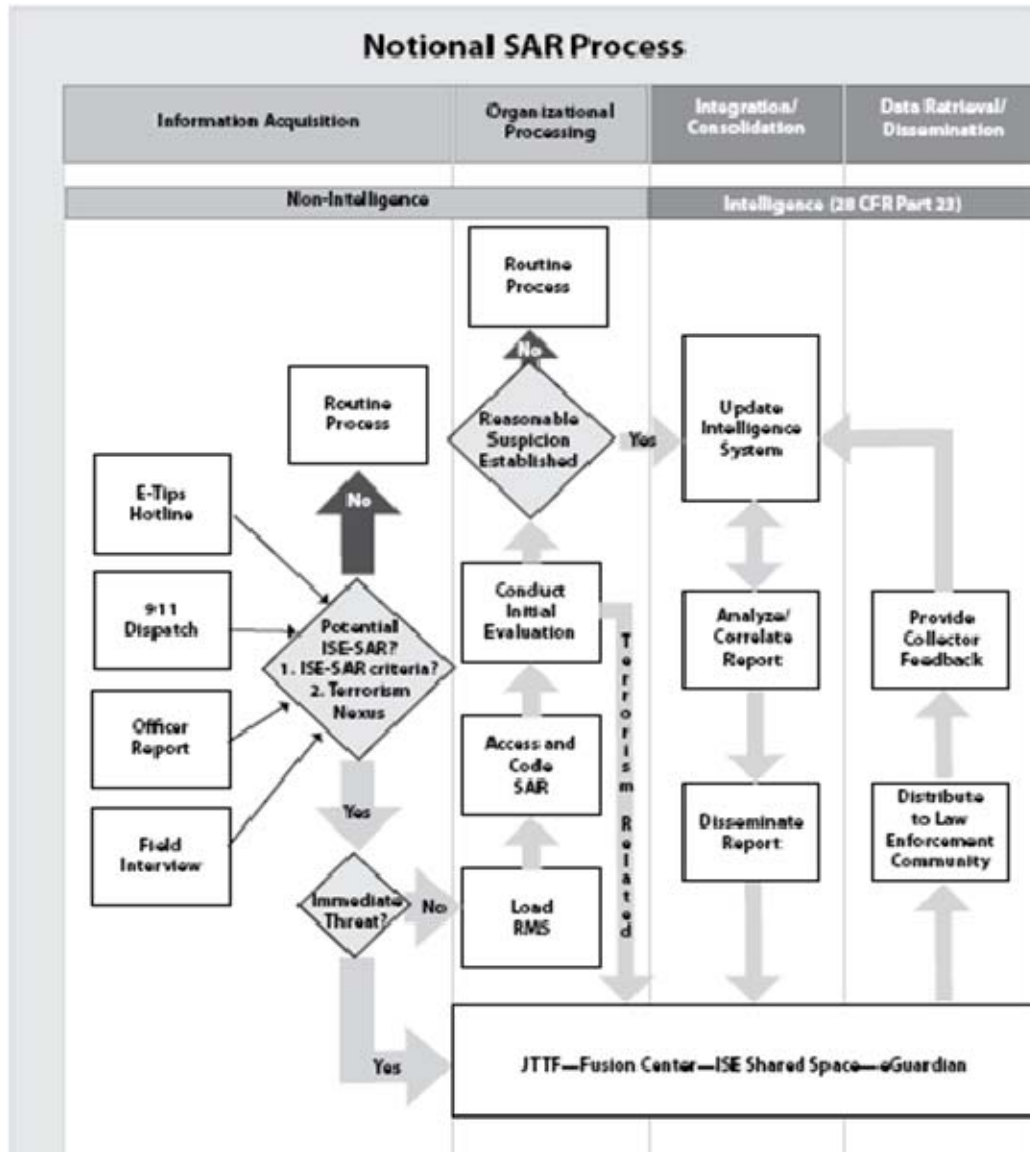


Figure 4. Notional SAR Process (From BJA, 2008)

In pursuing the implementation of this policy there are numerous issues that need to be considered, including the following:

1. Administrative

Incorporating SAR into the mission of state, local and tribal law enforcement agencies will require the development of directives, training, and continual oversight in institutionalizing this practice. Among the administrative decisions to be made will be whether or not to take an all crimes approach to reporting and how the information collected will be passed on from the agency or regional fusion center to the Joint Terrorism Task Force in an expedient manner.

2. Legal Criteria

In order to ensure that participating agencies are upholding constitutionally protected rights, a review and evaluation of departmental policies must be considered prior to proceeding with the collection and sharing of information regarding terrorism or crime related activity. As transparency is also an important factor in assuring public acceptance, policies should also be communicated to elected officials as well as the public. A determination also needs to be made to discern when 28 Code of Federal Regulations Part 23, apply.

3. Technology

As the impetus for this program is to facilitate the sharing of information both vertically and horizontally, it is imperative that the technical applications used have the ability to ensure standardized interoperability, while at the same time allowing the organization to customize SAR applications to meet individual agency needs. The technical application chosen should also be user friendly and be compatible with other systems that are currently employed.

4. Potential Courses of Action / Recommendation Metropolitan

a. Status Quo

The first course of action would be to maintain the status quo, which entails the path of least resistance as no change would be enacted. Time and resource

constraints that would be imposed as a result of the aforementioned criteria would be a non-issue. The vulnerabilities of failing to act, however, would leave agencies susceptible to acts of terrorism as critical information could likely be overlooked, go unreported, or fail to be passed on to the relevant node for action. This course of action would also result in making the same mistakes that have resulted in past catastrophe.

b. Agencies and Regions Build their own System

Agencies and regions also have the option of building their own in-house system for SAR. The argument in favor of this solution would be that minimal costs would be incurred and solutions would likely be compatible with existing systems. On the contrary, this would not ensure compliance with common national standards, which are needed if agencies are to overcome pre-existing obstacles that have led to previous intelligence failures. Likewise, even systems that could be applied to specific geographical regions are not effectual if organizations are failing to comprehensively collect and share data with all of the state, local, tribal and federal partners.

c. Use Accepted Technology for Analyzing Data

A third option is to use a commonly accepted technology that has the capacity to expediently and accurately analyze the collected data and transfer intelligence to the appropriate unit for action. The technologies being explored and currently being utilized are adaptable to customization while conforming to national standards. This will promote interagency as well as intra-agency efficiency, and also provides for the use of electronic reporting to be built into an array of field reports, which will speed up the collection and sharing process. The challenge with this option is that there is still disagreement as to which platform best serves this purpose, who owns the data and what hidden costs exist. This third option represents the most viable alternative and although SAR implementation is in its infancy, the participating agencies commencing this effort will be at the forefront in taking this initiative forward through the following proposed action.

Based upon the alternatives available, this last recommendation appears to be the most viable for meeting the needs of state, local and tribal agencies, while adhering to federal standards. Negotiations between the federal agencies and the major agencies representing law enforcement are likely to discern the appropriate preference that will meet the collaborative needs of all interests.

5. The Institutionalism of a Counterterrorism Outlook for the Law Enforcement Community and Beyond

The majority of Americans are keenly aware of the malicious intent of terrorist organizations to inflict harm to U.S. citizens both at home and abroad. Yet, very few people maintain a sense of urgency in developing or participating in strategies to minimize the consequences—including psychological consequences of terrorism through preventive efforts. Terrorism, unlike most other forms of crime or trauma, has a specific purpose in seeking to exact pervasive psychological fear and pain. The potential for an asymmetric attack using weapons such as chemical, biological, radiological or nuclear creates an even deeper sense of vulnerability with an enhanced fear of the unknown. In a 2004 Harris Interactive poll, the majority of survey participants in both the United States and Britain indicated little worry about a terrorist attack, with less than 10 percent of Americans worrying “a lot”—just three years after the tragedy of 9/11 (Taylor, 2004). One clear difference in the poll was that the Americans had much more confidence in the ability of the government to reduce the likelihood of a terrorist attack.

Just as many organizations assign complex tasks and decisions to teams as opposed to a sole person at the top of a hierarchy, team performance—including effective information sharing—are vital to counterterrorism efforts. In a recent research report (Mesmer-Magnus & DeChurch, 2009), a meta-analysis of information and team performance revealed that information sharing can be enhanced by: structuring team discussions, framing team’s tasks as intellectual and promoting a cooperative team climate. While teams typically possess a functional advantage over individuals, the study gleaned that teams fail to share information when “they most need to do so.” Figure 5 illustrates the relevance of openness and uniqueness in effectively dealing with complex

problems or tasks. Uniqueness in this context refers to the diversity of the experts involved, which allows for a wide range of views to develop a quality solution.

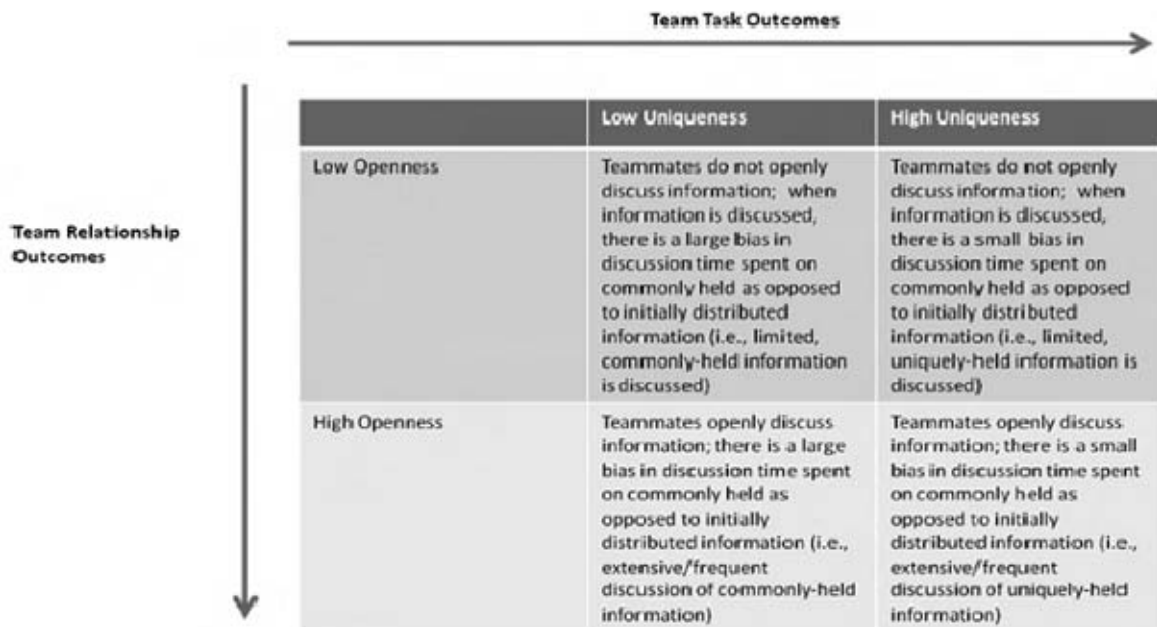


Figure 2. Two-dimensional typology of team information sharing and team outcomes.

Figure 5. Two-Dimensional Typology to Team Information Sharing and Team Outcomes (From Mesmer-Magnus & DeChurch, 2009)

The relevance of this material pertains to the need for a collaborative team effort to provide for an effectual information sharing process. With so many Americans having low levels of concern about a terrorist attack, this creates an ancillary challenge of encouraging the public to be proactive partners in efforts to preempt acts of crime and terror through participating in information sharing networks. The question to be considered, therefore, is how to get the public involved as enthusiastic partners in this mission.

Upon reviewing research pertaining to the inaction of persons or groups in emergency settings, stories such as the parable of the 38 witnesses, which involved the 1964 murder of Kitty Genovese, come to mind. In this particular story that received widespread public attention, it was reported that 38 witnesses had observed Ms. Genovese being attacked and stabbed, without intervening or making an effort to contact

the police. While much of this story has since been proven to be exaggerated, it does raise questions about the reasons that individuals or groups would fail to intervene in a similar scenario. Furthermore, if there are reasons that inhibit the involvement in emergency scenarios, then what is the likelihood that ordinary citizens will take steps to report suspicious activity or potentially criminal behavior rather than being just passive bystanders? The quote attributed to Edmund Burke, which reads “The only thing necessary for the triumph of evil is for good men to do nothing,” (Burke, n.d.) reinforces the need for citizens to take some kind of action—even if it involves notifying authorities through a phone call.

Although there can be a multitude of reasons that people may not step forward to get involved in a situation (e.g., they feel someone else is more qualified to help), one phenomenon that offers to explain this is known as the “bystander effect.” This occurrence addresses emergency situations where individuals are less likely to intervene when there are others present and argues that the more people in attendance, the less likely that someone will step forward to assist. In a release published by the Canada Safety Council, (2004) the council addresses this type of citizen complacency and provides an overview of why people fail to get involved and also simple tips such as how to quickly place an effective 911 call from a mobile telephone.

Certainly, there are many acts of heroism and vast accounts of people who report emergencies or seemingly more trivial events on a daily basis with no recognition or desire to be recognized. Instead of focusing on the negative aspects of inaction, developing new insights into the positive deeds of those who choose to be engaged and get involved with both emergency and even lesser scenarios is receiving more attention. In his book *The Lucifer Effect*, Dr. Phillip Zimbardo (2007) addresses the dynamics of seemingly ordinary people, who transcend their roles as passive observers to do extraordinary deeds. He describes this phenomenon as “the banality of heroism,” which is seemingly accompanied by a certain sense of humility in viewing individual actions as the norm rather than a heroic feat (Zimbardo, 2007) At a lecture in Philadelphia in June, 2009, Zimbardo expanded on this by proposing that people are more likely to do good and think positively about the future when they can imagine themselves acting a heroic

manner. He also advocates the importance of teaching this mental rehearsal, which will prepare individuals to take appropriate moral action in the event that the need arises. If this philosophy can become ingrained throughout society, the diffusion of personal responsibility due to the presence of others could be replaced by an intrinsic call to take action.

In the realm of homeland security, this type of heroic action does not necessarily have to mean that people are required to run into burning buildings to save babies. If societal norms advocated civic virtue and established behaviors focused on the positive, more people might be willing to take basic steps such as reporting a crime or suspicious activity in stead of disregarding an atypical situation that may require intercession. Aristotle once said that “ We are what we repeatedly do. Excellence, then, is not an act, but a habit” (Present Outlook, 2009) This statement applies as much to doing good and becoming a principle based citizen playing a functional role in society, as it does to eating healthy or any given habit.

While developing habitually moral principles may appear to be a very personal endeavor, Zimbardo (2007) proposes, “Government, education, and social institutions can be re-designed to facilitate critical thinking and responsible conduct.” Among the highlights he offers for achieving this type of thinking and conduct include the following ideas:

1. Teaching children to disobey *unjust* authority
2. Rewarding social modeling of moral behavior
3. Promoting critical thinking that challenges false ideologies and bad means to good ends
4. Encouraging respect for human diversity and appreciating human variability
5. Not allowing stereotyping and dehumanization of other people
6. Changing social conditions that make people feel anonymous
7. Encouraging admission of mistakes, accepting error in judgments – to reduce justification for continuing wrong, immoral behavior

8. Promoting personal responsibility and accountability of one's actions
9. Supporting independence over group conformity
10. Reducing poverty, inequities, and entitlements of the privileged
11. Never sacrificing freedom for promised security
12. Discouraging even the smallest of transgressions, cheating, gossiping, lying, teasing or bullying. (Zimbardo, 2007)

Ascertaining a sense of empathy for others may allow individuals to be more cognizant of others and lead them to act in a more compassionate manner. Likewise, with more people committing to personal accountability, there may be a greater likelihood that they will take action in even non-emergency situations in which they can contribute to the overall good of society. With the mounting availability of communication devices and social networking applications, participation in both local and global efforts is essentially at the fingertips of many Americans. If government at all levels is able to establish and maintain the trust of those that it serves, there is an escalating probability that greater numbers of citizens will take proactive measures to become involved in keeping their communities safe.

C. TECHNOLOGY STUDY

1. Evaluation of the FBI's eGuardian Program

Through the FBI's eGuardian, which was developed and released in the summer of 2008, a number of positive features were noted. Among those that were most appealing were:

- Ability to access eGuardian through Law Enforcement Online (LEO); as LEO is easy to access, it provides a secure environment to access eGuardian, which consequently allows officers to access unclassified information from eGuardian.
- eGuardian was advertised as a comprehensive tool with alert, warning and reporting capabilities, which would be flexible to meet the needs of the individual participating agencies.

- eGuardian appeared easy to use and allowed the ability to attach a variety of file types (e.g., images and documents).

While eGuardian promised to provide free and effortless access, there are lingering concerns about the ownership of information with this system and the ability to share information with other state, local and tribal law enforcement agencies. From a security perspective, the FBI's system seems to be viable and knowing the security levels required to access eGuardian through Law Enforcement Online, there is no reason to believe that there are any gaps to be exploited. The greatest potential benefit of proceeding with the eGuardian option is the threat tracking system that would allow agencies to pull unclassified information from eGuardian.

As this system commenced with a phased law enforcement rollout in December of 2008, additional testing and review is currently underway. A number of Virginia police departments and the Northern Virginia Regional Intelligence Center have signed on to conduct work flow testing. This work flow review will scrutinize the systems in place and will provide an opportunity for agencies to gauge the progress and practicality of this system.

2. Evaluation of the Program Manager–Information Sharing Environment Program

The second alternative studied involved the implementation of the SAR functional standard that was recommended by the Major Cities Chiefs Association. This Information Sharing Environment–Suspicious Activity Report (ISE-SAR) pilot program seeks to examine the functionality of the ISE-SAR criteria guidance and the sharing of this information between fusion centers, JTTFs, the federal government and the major city law enforcement agencies. The purpose of this project is to evaluate SAR development and its potential to evolve into an enduring information sharing capability. Coincidentally, the FBI is also a project partner and sponsor for this initiative. Among the other sponsors are:

- U.S. Department of Justice, Bureau of Justice Assistance
- U.S. Department of Homeland Security

- Program Manager, Information Sharing Environment
- Major Cities Chiefs Association
- International Association of Chiefs of Police (IACP)
- Department of Defense (DoD) Antiterrorism/ Force Protection
- DOJ's Global Justice Information Sharing Initiative, Criminal Intelligence Coordinating Council (CICC)

With the DOJ/BJA supporting the PM-ISE, who serves as the program manager, the potential benefits of participating in this project are as follows:

- This program leverages shared space and will extract suspicious activity data from existing systems (rather than creating a new system) and share it with other law enforcement agencies in the ISE.
- Agencies will store and own their data and will make the determination as to which information to share and the frequency of data to the shared space.
- DOJ and the PM-ISE will work with participating agencies to establish a privacy policy and training program that are consistent with organizational needs.
- The PM-ISE will purchase the shared space servers and provide a project team to work with participating IT staffs to design the technology processes that will facilitate this transfer of identified SAR data.

While both plans offer a number of benefits that address present deficiencies, the ISE-SAR plan appears to have greater support among the state and local law enforcement community. The hands on approach in providing assistance with program implementation, including legal assistance in crafting privacy policy guidelines and working through technology hurdles, was also a critical factor in steering this decision. Figure 6 provides an overview of some of the principal factors involved in evaluating these programs to include an internal solution (MPD) that some agencies may seek to explore.

Evaluation Criteria for Technology			
Type of Technology	eGuardian	MPD Solution	PM—ISE
Criteria			
Secure	Yes	Yes	Yes
Cost	Minimal	Minimal (time)	Minimal
User friendly	Claims to be	Undeveloped	Claims to be
Accessibility	Yes	Unlikely (poor)	Yes
Flexibility to meet agency needs	Yes	Yes	Yes
Ownership of Information	MPD—until entered in eGuardian	MPD	MPD
Access to unclassified data from Guardian	Yes	No	No
Ability to attach various files	Yes	Yes	Yes
Alert, warning and reporting capability	Yes	Limited	Yes
Implementation guidance	Limited	None	Very strong
Partnerships/Sponsors	Limited	Limited (NCR)	Very strong
Training	Limited	Limited knowledge	Hands on; very strong

Figure 6. Evaluation Criteria

Regardless of the strategy chosen, successfully implementing this technology requires a collaborative effort and strong leadership at the executive level. With chiefs, sheriff's and agency leaders serving as champions of the chosen program, all subordinates must have clearly delineated roles and responsibilities in bringing this initiative to fruition. While the executive support is critical, the key component is collaboration at all levels. As officers will be the primary reporters of information, it is essential that they be included in the planning process and that they are comfortable working with the end product. This technology must ultimately be user friendly and must be accompanied by a feedback component. If this initiative is too cumbersome and lacks follow up from either a detective or intelligence analyst, most officers are likely to avoid reporting suspicious activities through this mechanism.

D. BEYOND TECHNOLOGY: IMPLEMENTATION ISSUES AND POTENTIAL REMEDIES TO ADDRESS THEM

1. Policy Guidelines

Agencies must institute policies/directives, which outline background, procedures and individual responsibilities. This should include a determination of where privacy policy, specifically 28 CFR Part 23, is applicable. In order to adhere to national standards, organizations should also adhere to standardized codes and reporting formats. Auditing reports and systems should also be directed by policy in order to ensure that the agency is in compliance with privacy guidelines and that the appropriate screening and coding is being adhered to.

2. Training

In order for SAR to be institutionalized and become fully effective, agency members and other key stakeholders must be adequately trained to recognize suspicious behavior and know how to report their observations. Recommendations for training will likely include the incorporation of training into the recruit officer curriculum and into annual in-service training for the remainder of the department. With many law enforcement agencies transitioning to distance learning, this effort will likely proceed through that venue, with the officers/officials taking an on-line test at the end of the lesson. Beyond police department personnel, it is also important that the public, government officials and the private sector are included in this training and education. This effort will also provide transparency and answer outstanding questions about the program.

3. Technology

In implementing the PM-ISE version of SAR, participating agencies will be hosting servers and necessary equipment that will allow for internet based access by authorized users. Among the challenges is to make sure that privacy requirements are met and guarantee that no other departmental systems are adversely impacted. As part of the

memorandum of agreement (process, project teams should be dedicated to work with departmental IT staff to toil through any potential obstacles. Additionally, agencies may consider including SARs into all relevant types of field reports to flag pertinent information, or incorporate this into existing electronic field reporting systems. This will improve the rapidity of getting the information into the hands of the designated person.

As this pilot implementation progresses, there will likely be further challenges, which will need to be addressed as they arise. With a number of major cities across the United States taking on the same project, open lines of communication will allow agencies to collectively work through impediments and successfully execute this critical information sharing initiative. Federal guidance will be vital throughout this process to ensure that standardization is maintained and that state and local governments are provided with the resources and technical expertise to guide them through this process. With homegrown terrorism emerging as a future threat, the nation's state, local and tribal police officers must take a more active role in seeking to identify terrorists that are presumably living amongst us. While fusion centers have provided one avenue to facilitate the sharing of information, effectively leveraging technology to "create the dots" is imperative in using police resources to their utmost potential.

E. CASE STUDY: THE LOS ANGELES POLICE DEPARTMENT SAR IMPLEMENTATION

The Los Angeles Police Department (LAPD) implemented its suspicious activity reporting program in early 2008, becoming the first United States city to create a national standard for terrorism-related modus operandi codes. Since that time, it has experienced a number of success stories that have come about with increased awareness and subsequent reporting. Commander Joan McNamara of the LAPD provided a number of success stories pertaining to both potentially terrorist and criminal activity.

In developing this effort, the LAPD's Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) sought to improve the manner in which it collects, maintains, analyzes, tracks and shares information and incidents which have a potential nexus to terrorism. These efforts were intended to institutionalize a counter-terrorism

philosophy throughout the department and standardize internal procedures while providing a potential national model for similar standardization. Initial requirements for establishing a SAR included:

- Providing an intake or collection method for information that is not currently collected.
- Involving front line officers in supporting the institutionalization of counter-terrorism efforts department-wide.
- Establishing the requirement to complete the report when personnel become aware of suspicious activity or information that indicates possible terrorism related activity or affiliations.
- Utilizing the current Department Investigation Report which all officers are familiar with.
- Involving minor adjustment to the current Investigation Report to allow for immediate recognition of a SAR related report.
- Establishing the first of its kind terrorism related Modus Operandi (MO) codes to capture suspicious activity or incidents believed to be related to terrorism.
- Providing near real-time information capture for queries within the CCAD system in order to:
 - Assist in identifying patterns which may indicate potential targets, heightened activity of a specific nature within a given time frame, a specific area or involving a specific person or place, and the identification of trends in comparison to national or international occurrences.
 - Support the successful analysis and synthesis of information and the production of actionable intelligence.
 - Supply year to date analysis of activity to provide statistical support for determining the allocation of personnel, focus areas for training and the concentration of investigative, enforcement or protective and preventative efforts.
 - Provide for an associated ability to geographically map occurrences.

As community outreach is an important piece of program implementation, the LAPD developed an outreach model to engage, train and share information with community members, private stakeholders and employees and administrators at public and private infrastructure facilities. These efforts included information delivery through community meetings and organizations, along with postings to the department Web-site. Departmental training is also a critical factor, and as such, officers were trained in identifying activities that initially do not appear to indicate criminal behavior but where a wider perspective may reveal potential domestic or foreign terrorist related activity. The Counter-Terrorism and Criminal Intelligence branch also developed training materials and programs that were introduced through training venues such as: Web-based training (e-learning), the Terrorism Liaison Officer (TLO) program, inclusion in the roll call training calendars and in service training. The example provided below details the efficacy of this initiative in sharing information:

In December 2008, a Van Nuys Narcotics Detective contacted detectives from the Los Angeles Police Department's Counter-Terrorism unit pertaining to the arrest of a suspect with information about sales of illegal assault weapons, identity theft and narcotics to supply Asian and Armenian gangs. As a result of this information, the LAPD completed a suspicious activity report.

Counter-terrorism detectives subsequently joined forces with the Federal Bureau of Alcohol, Tobacco and Firearms and conducted an extensive follow-up investigation, which resulted in several illegal weapons purchases. The purchases were then used to track the supplier's weapons and to attempt other purchases of illegal assault weapons and explosives. In January 2009, three illegal weapons purchases netted one 9mm semi-auto pistol, one .44 revolver, five Mac-10 assault pistols (one fully automatic) and several extended high capacity magazines and suppressors.

The joint investigation led to the service of a search warrant and ultimately to the arrest of three suspects. Recovered in the searches were 21 weapons, including 10 assault rifles with numerous high capacity magazines, 280 rounds of .223 tracer ammunition and an inert hand grenade. This case illustrates how the diligence of one detective combined

with the appropriate sharing of information can have a dramatic impact on public safety. (J. McNamara, personal communication, July, 2009).

F. SAR AND INFORMATION SHARING DURING THE 56TH PRESIDENTIAL INAUGURAL

For years, non-federal law enforcement agencies have been seeking access to greater intelligence pertaining to localized threats. In the post-September 11 environment, improved interaction and formalized relationships have been among the many improvements in the domestic information sharing realm between the federal government and its state, local and tribal partners. Along with this dramatic increase in the exchange of information, comes a secondary issue. Specifically, now that state, local and tribal law enforcement has acquired this sought after information, how are they getting this information analyzed quickly and disseminating an intelligence product promptly to patrol officers in the field?

In the Washington, D.C., Metropolitan area, these relationships were put to the test on January 20, 2009, when Barack H. Obama was sworn in as the 44th president of the United States. As the nation's first African-American president, this inauguration had greater significance than any Investigation Report inaugural in recent history. Beyond the inauguration, a week of events including service activities, a concert and national prayer service, required substantial planning and resources from the law enforcement community and beyond.

As the transition of power is paramount in a thriving democratic society, it was important for this event to be accessible to the public, while at the same time providing a safe and secure environment for the many spectators and dignitaries in attendance. Furthermore, providing for the security of the first African-American president and sharing threat information with partner agencies and officers at all levels to achieve this task was critical.

The 2009 inauguration subsequently lived up to anticipated expectations, as it was the largest single-day event in the history of the nation's capital. An estimated 1.8 million

people were present on the National Mall and along the inaugural parade route for the swearing-in ceremony, which posed challenges for a myriad of agencies and the city's infrastructure.

As the Department of Homeland Security designated the 2009 Presidential Inauguration a National Special Security Event (NSSE), the United States Secret Service assumed the lead responsibility for the coordination of the operational security plan. A number of sub-committees, including an intelligence sub-committee, were established to provide for synchronized efforts between the participating agencies. In addition to the agencies within the National Capitol Region, the Metropolitan Police Department augmented its staffing with an additional 4,000 officers from 99 police departments from around the country. This aggregation of resources required that these personnel be kept abreast of actionable intelligence and maintain a heightened level of awareness.

The Metropolitan Police Department implemented its suspicious activity reporting program just prior to this event seeking to expand the volume of information available and address any potential threats. During the inaugural period, the MPD mapped SAR data to capture real-time incidents, suspicious packages and events as part of the collection plan on the current threat.

While there were numerous SARs submitted during this time period, two examples listed below portray the types of activity being reported:

- The first example involved a call for a suspicious person believed to be taking photos at the railroad tracks. As the president and vice president were traveling to the District via train, this type of behavior could be viewed as preoperational surveillance. Subsequently, this information was dispatched as a priority call and units responded to the area to investigate. A SAR submission allowed MPD to capture the information on the event and share this with law enforcement partners.
- A second case involved a suspicious male at a local Starbucks. The male was wearing a backpack and acting in a manner which drew attention to his behavior. This tip was of note, as it came from the private sector, where outreach was conducted prior to the inauguration on how to report suspicious behaviors, and again officers were called upon to investigate and collect information on the activity. This example emphasizes the role

that the private sector plays in both understanding what constitutes suspicious behavior and having a mechanism to report it.

While there were many tools used to enhance situational awareness and facilitate the sharing of information with the numerous agencies and more specifically law enforcement agencies dedicated to this event, the following apparatus played a pivotal role and again illustrate the role of technology:

- CCTV: Cameras were used for multiple purposes. Command centers were able to share information pertaining to any disorder and crowd movements due and communicate directly to relevant field personnel.
- Situational Alert Management System (SAMS): SAMS was used to track the movement of the 4,000 plus police officers from the DC Metropolitan Police Department and the 99 assisting agencies. The system tracked personnel movements, provided a running resume on all decisions and allowed for monitoring of real-time crime information.
- Classified systems and bulletins: A series of threats illustrated the limitations in using classified information in crafting a product to disseminate intelligence to critical personnel responsible for protecting the city. While command personnel with adequate clearance were privy to detailed information, there were delays in sanitizing the information to provide to officers in the field via teletypes and other electronic formats.
- Use of fusion centers as a force multiplier: Regional and national fusion centers were used to supplement the Washington Regional Threat and Analysis Center by coordinating systems and information from various sources. This coordination included incoming traffic highway enforcement in the states of Maryland and Virginia as a deterrent to a terrorist threat. The allied agencies also rode Amtrak and Marc trains as a visible deterrent.
- Text messaging: Due to the magnitude of the crowd, there were times when basic phone service was limited. The use of text messaging was a valuable tool in supplementing the existing communication options.
- Shotspotter: this acoustically based gunshot detection system was used as a crime-fighting tool to distinguish gunshots from non-gunshots (e.g., fireworks) to save both time and resources.
- Joint Operations Command Center (JOCC): Over 23 allied agencies were assigned to the Metropolitan Police Department's JOCC in order to facilitate communications to relevant agencies along the parade route and throughout the city and region. The allied agencies were provided access

to all technologies to ensure situational awareness and provide for officer safety. As 15 separate command posts were operational in the region, coordinated information sharing and command and control were vital to the success of the event.

Even with the many technological applications to support the various information sharing initiatives, the key element needed between the agencies was trust; beyond the technologies, trust remains the critical factor in providing for a successful collaborative partnership. Previous coordination with federal partners in the National Capitol Region during times of crisis exemplified the strengths of the relationships and allowed the key partners to work together through an extremely complex range of issues. The technologies discussed throughout this chapter address the research questions: *What types of technology can be leveraged to enhance this process, ensure privacy and provide for the security of classified information, as well as how SAR can be implemented and customized to meet agency needs as well as those of the information sharing environment.* The fact that there are numerous options available, which leverage existing systems while allowing flexibility for technology and respecting individual rights, is a positive indicator that the existing architecture can provide for secure, seamless sharing of information.


THIS PAGE INTENTIONALLY LEFT BLANK

V. REALIZING THE GOALS OF THE NATIONAL STRATEGY FOR INFORMATION SHARING

A. STRATEGY FOR ACHIEVING THE VISION

1. Value Innovation for Enhancing the Collection and Dissemination of Domestic Information/Intelligence

The vision for enhancing the collection and dissemination of domestic information/intelligence is to transform state, local and tribal police officers nationwide into active collectors of information and leverage technology to enable them to both share the requisite information and receive actionable intelligence in return. The Figures 7 and 8 illustrate the goals to be achieved using the Blue Ocean Strategy as a guide.



<p>Eliminate:</p> <ul style="list-style-type: none"> ✓Lack of access to information ✓Organizational/inter-agency silos ✓Information that fails to be analyzed ✓Intelligence failures (Inability of LE to connect the dots) 	<p>Raise:</p> <ul style="list-style-type: none"> ✓Situational awareness of state, local, and tribal police officers ✓Amount of information being collected ✓Volume of intelligence being shared horizontally, vertically and inter-agency ✓Level of involvement beyond the police to other government entities, the private sector, and community at large
<p>Reduce:</p> <ul style="list-style-type: none"> ✓Privacy/Civil liberties concerns ✓Intelligence distribution challenges ✓Information input limitations ✓Time frames in which information is collected, analyzed and distributed 	<p>Create:</p> <ul style="list-style-type: none"> ✓Intelligence-led policing environment ✓A focused preventive LE community ✓An intelligence capacity for all LE agencies regardless of size

Figure 7. Value Innovation (From Kim & Mauborgne, 2005)

ER²C Grid: Status of Domestic LE information collection and Intelligence Sharing

<p>Eliminate</p> <p>Lack of access to information Organizational/inter-agency silos Information that fails to be analyzed Intelligence failures (Inability of LE to connect the dots)</p>	<p>Raise</p> <p>Situational awareness of state, local, and tribal police officers Amount of information being collected Volume of intelligence being shared horizontally, vertically and inter-agency Level of involvement beyond the police to other government entities, the private sector, and community at large</p>	<p>Red Ocean Strategy = Current LE practices for collection/dissemination of Domestic information/Intelligence</p> <p>Blue Ocean Strategy = Smart practices for Large-Scale Strategic Change</p> <p>Application of Blue Ocean Strategy Principals:</p> <ol style="list-style-type: none"> 1. Reconstruct Market Boundaries - Expand pool of stakeholders 2. Focus on the Big Picture - Greater IS capacity 3. Reach Beyond Existing Demand- Officers as first "Preventers" 4. Get Strategic Sequence Right - Effective Change Mgmt Strategy 5. Overcome Organizational Hurdles - Strategic Leadership 6. Build Execution Into Strategy - IT support and Institutionalization
<p>Reduce</p> <p>Privacy/Civil liberties concerns Intelligence distribution challenges Information input limitations Time frames in which information is collected, analyzed and distributed</p>	<p>Create</p> <p>Intelligence-led policing environment A focused preventive LE community An intelligence capacity for all LE agencies regardless of size</p>	

Strategy Canvas: Domestic LE collection and dissemination of information/intelligence

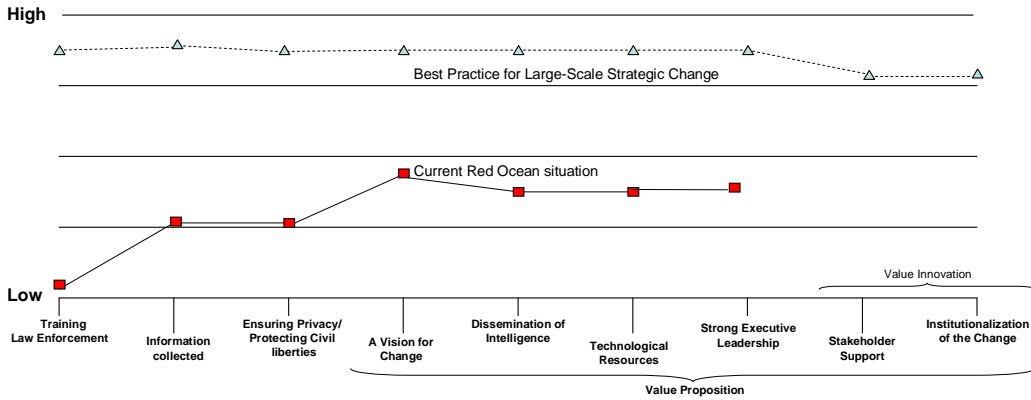


Figure 8. Strategy Canvass, Blue Ocean Strategy (From Kim & Mauborgne, 2005)

2. Blue Ocean Strategy for Enhancing the Collection of Information and Dissemination of Intelligence

In order to affect the successful implementation of suspicious activity reporting throughout the American law enforcement community, it is important to know who the relevant stakeholders are and what role they play in implementing and institutionalizing this system. The power versus interest grid divides these stakeholders into four groups. The “players” are the most critical group as they have the greatest power and interest in the success of this program. As SAR requires the standardization of reporting throughout the country, it is imperative to have the support of the agencies that represent LE throughout the nation. This includes organizations such as the International Association of Chiefs of Police (IACP), Major Cities Chiefs Association, National Sheriff’s Association and other major groups. Executive-level commitment within individual agencies is also paramount. Without this individual executive support, agencies will likely fail to assure successful execution. As the federal government also plays a

significant role in the intelligence community and the SAR process, key federal partners also have high interest/power in this process. Fusion center executives play a major operational role in this implementation and have a vested interest in seeing this prosper. Selected IT representatives are also included as technology is vital for implementation.

The second group, known as “subjects” have a high level of interest in this process, but do not have the same level of power as the players. Police officers, public/private sector partners, intelligence analysts and the homeland security community at large would fall into this category. Civil libertarians may not be proponents of this enhanced collection process, however, they do have a high level of interest in ensuring that privacy and civil liberties are not violated.

The “context setters” are primarily politicians at all levels of government. While they have great power to enable this process, the majority of setters have little direct interest in getting into the weeds involved in execution.

The community at large and those public/private sector partners with no perceived stake in this process or significant concern about their particular sector are classified in the “crowd” category. They have both a low level of power to impact this process and a similar level of interest.

While the players can be seen as the most critical group in bringing this process to fruition, it is important to know who the relevant persons are within each category that have a role in seeing this through. Failure to include stakeholders in the process will likely result in the failure of this initiative. The figure below represents the key personnel in this effort and classifies them into various categories based upon their positions.

Power v. Interest Grid for the Implementation of the SAR program

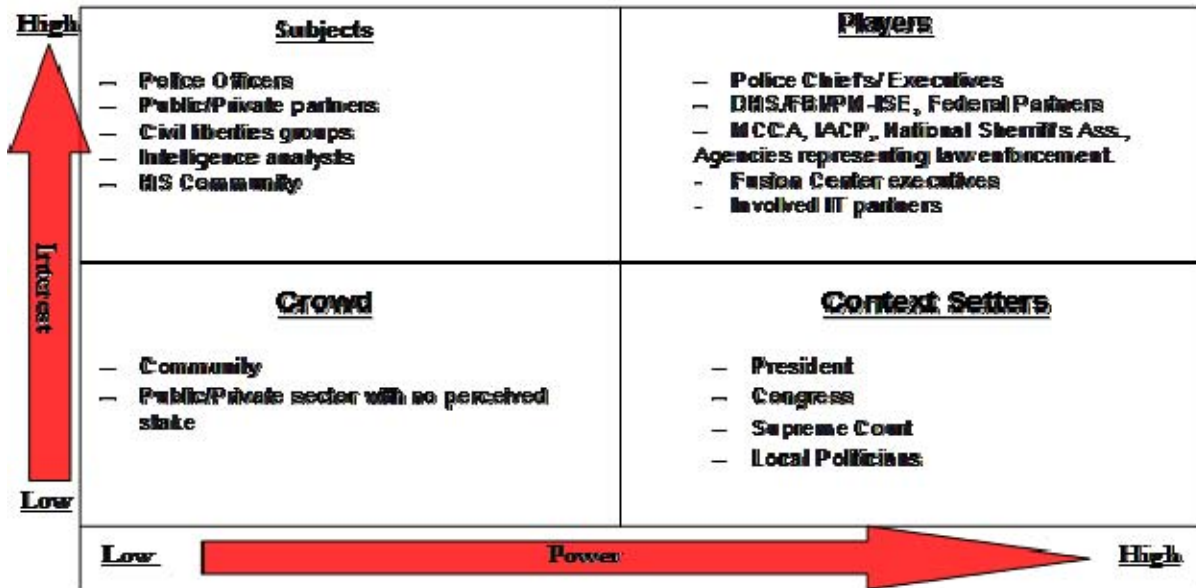


Figure 9. Power Versus Interest Grid (From Kim & Mauborgne, 2005)

B. POLICY RECOMMENDATIONS AND CONCLUSION

1. Strategy for Bringing Innovation to Fruition

a. Value Innovation

The value innovation being applied to the efforts for enhancing the collection and dissemination of domestic information/intelligence relies on a reconstructionist view of strategy. This strategy focuses on endogenous creativity to work beyond the existing market structure. Rather than relying on traditional forms of intelligence collection and dissemination, which greatly limits both the number of collectors and recipients, the new paradigm to transform state, local and tribal police officers nationwide into active collectors of information and requires moving beyond the

inclusion of more intelligence specialists. This strategy calls for a non-zero sum game, which expands beyond law enforcement and generates a new level of demand for both collectors and recipients of information/intelligence.

b. Planning

Using the outline identified in the book *Blue Ocean Strategy* (Kim & Mauborgne, 2005) as a guide, the major differences between Bryson's (2004) strategic planning principles and those identified by Brafrman and Beckstrom in the *Starfish and the Spider* (2006) predominantly pertain to hierarchy and leadership. Bryson (2004) emphasizes the importance of strong leadership and strategic actors to institute strategic change, while starfish communities emphasize the absence of leadership, structure and formal organization. While there are significant differences between these two approaches, there are also a number of similarities that would be viable to the strategic planning process.

c. Organizational Structure

The applied process to implement the value innovation discussed in this thesis employs a hybrid organizational structure. While there is still centralized leadership, hierarchy and consolidated bureaucracy, there is a decentralized network of collectors and consumers. This network greatly expands the flow of information coming into the system and empowers the many participants to add value to the overarching mission of keeping the country safe.

d. Leadership

Implementing a vigorous suspicious activity reporting program requires a strong commitment by the leadership of the agency in both sponsoring and championing the strategic process. At the same time, this process calls for a network effect where every additional provider of information adds value to the larger network and enriches the information. Facilitating the process and fostering collecting leadership are important similarities incorporated in both models.

Just as the starfish strategy acknowledges that knowledge is spread throughout an organization and that the best knowledge often lies at the fringe, both strategic processes recognize the value of understanding the people involved (including oneself) and the need to encourage people to take risks and explore unconventional solutions to existing challenges. Trust is a critical component of the process as risk assumes that people will be stepping out of their comfort zones and possibly making mistakes. Understanding the desire for people to make a contribution to the mission, creative thinking should be rewarded and multiple sources of insight should be encouraged.

Another common aspect of both approaches pertains to the need for a staunch advocate, who has a conviction to seeing the process through. While a process sponsor would be a chief of police or a top-level official with positional power to direct resources and guide the process, the champion—or catalyst—can come from any level in the organization. This person is tasked with managing the daily processes of the strategic plan and pulling the team members together when focus is lost. Key traits of this individual would include: strong interpersonal skills, emotional intelligence and the ability to foster both trust and inspiration.

As part of a hybrid organization, both chiefs (bosses) and catalysts are critical to the strategic planning process. With the catalyst working in an unstructured environment, they have the ability to expand the network of involvement and achieve the mission that is envisioned by the agency director. While operating at different levels, strong leadership in both of these positions is critical to success.

Combining various parts of the diverse strategies would be the best way to describe the construction of this strategic planning process. In seeking to establish a new paradigm in information sharing, executive leadership must become well versed and thoroughly knowledgeable about the task at hand and be both committed and passionate about instituting this strategic change. In doing so, executive leaders realize the criticality of collecting, analyzing and sharing suspicious activity in preventing both crime and terrorism.

e. Collaborative Advantage

As this comprehensive information sharing initiative entails expanding the network of collectors and consumers, a common national methodology is essential to provide for both standardization and consistency. Technology is also a critical component as it allows for access to information and imparts the ability to quickly and accurately analyze the data provided. The theory of collaborative advantage also applies to this strategy, as it requires the synergistic efforts of literally thousands of agencies at all levels of government. Leadership, commitment, determination and trust are once again ubiquitous amongst all of these strategic options.

2. Interagency Strategic Planning Process for the Implementation of Suspicious Activity Reporting (Synopsis)

- After gaining a thorough understanding of the task at hand and the importance of expanding the current information sharing environment, executive leadership understands the power of networking and communicates this vision throughout the organization.
- While sponsoring the SAR process, the executive also designates an advocate, who can serve as the catalyst and facilitate (or coordinate the facilitation of) the strategic planning process.
- In fostering collective leadership, meaningful processes are established to provide for the inclusion of vast and innovative ideas from throughout the organization. Employees are encouraged to take risks and trust is instilled in the agencies values.
- Management and catalysts measure, monitor and manage the process and work collaboratively to implement policy decisions.
- Processes are continually tweaked to improve quality of efforts and expand catalysts throughout the organization. As a result, the program will ultimately be institutionalized into the agency's culture and will be more easily expanded across agency boundaries.

C. LIMITATIONS OF RESEARCH AND RECOMMENDATIONS FOR FUTURE RESEARCH ISSUES

The proliferation of technology will continue to expand the possibilities for enhancing and expediting information sharing both within and beyond the law enforcement community. While fusion centers continue to hold great promise for maximizing the efficacy of collected information and the subsequent analysis to meet a range of agency missions, these centers are still developing baseline capabilities to provide for consistency and standardized approaches. While many centers commenced operations with a focus on counter-terrorism intelligence, many have grown to take on an “all hazards,” “all crimes,” or some sort of integrated variation of these approaches. The National Strategy for Information Sharing (White House, 2007) calls for the development of baseline operational standards. The development of these standards will be imperative for supporting future operational capabilities to include SAR analysis and risk assessments.

On July 22, 2009, the Department of Homeland Security issued a press release with the heading “Secretary Napolitano Releases Report on Department’s Progress Fulfilling 9/11 Commission Recommendations.” In reference to collaboration and information sharing, the release highlighted the following statement:

To improve collaboration and information sharing, DHS has established new law enforcement agreements across all levels of government—including two agreements between DHS and the Department of Justice signed since June to combat arms and drug trafficking—and forged international agreements with Canada, Germany, Greece, Italy, Mexico, Portugal and Spain since January to share information to combat serious crime and collaborate on science and technology. DHS has also worked with federal, state, local and tribal law enforcement to designate 72 state and local Fusion Centers across the country to centralize intelligence gathering and share information within their jurisdictions and with the federal government—and provided more than \$340 million to support these centers since 2004. (DHS, 2009)

This statement illustrates the reliance that the Department of Homeland Security has on fusion centers in advancing the flow of both information and intelligence in the future. Privacy policies may inhibit research efforts that would preclude agencies from

providing information that can be used to measure the spectrum of accomplishments or failures of these centers. However, through surveys, interviews, case studies and other research methods, there are numerous additional metrics that can be effectively utilized for evaluation purposes. Future research opportunities pertaining to fusion centers as well as collaborative efforts to improve collaboration and information sharing at all levels of government are abundant. Efforts to share information with the majority of the nation's smaller state, tribal and local law enforcement agencies that comprise approximately 75 percent of this population is of particular precedent as many of the current efforts are focused on the larger and predominantly urban departments.

Beyond law enforcement reliance on public and private partners, reliance on the community at large is an integral facet to a comprehensive information sharing effort. A well developed community-based intelligence collection model is essential to the overall goal of reducing crime and preventing terrorism. Just as efforts are being made to engage private stakeholders, employees and administrators at public and private infrastructure facilities, future efforts to better engage, train and share information with the community at large must be explored. Inquiries into the use of, relevance and practicality of social networking sites such as "twitter" and "facebook," provide great opportunities to explore how evolving technologies factor into the means for which information is currently being disseminated and opportunities for the government to capitalize on these contemporary phenomenon. Concurrently, this also poses the dilemma of researching any specific technologies as innovative products continue to be devised at a rapid pace.

One of the greatest impediments to the timely dissemination of intelligence has been the classification or over classification of intelligence products. Even with the vast improvements in the flow of information between the federal government and its tribal, state and local counterparts, sanitizing intelligence for dissemination to patrol officers, first responders and other key stakeholders without clearances can prove daunting. Greater efforts must be made to expedite and standardize the clearance process and actionable intelligence needs to be just that—passed on quickly in order to be acted on. Studies into expediting the clearance process and simplifying the classification system will allow future efforts to be more inclusive with an expanding pool of partners. As

information and intelligence can only be effective when acted upon, it is vital that better methods of communicating with both collectors and consumers be identified, evaluated and utilized. While restrictions on research may be imposed on these empirical inquiries due to the real-life context of these modern occurrences and the ambiguous boundaries between the experience and the context, future case studies may offer a valid means to provide answers to common questions of a similar nature.

D. CONCLUSION

Just as the National Commission on Terrorist Attacks (2004) cited a “failure of imagination” in failing to prevent the attacks of September 11, 2001, the prospects to use our imaginations in embracing and pursuing new opportunities for collaborating and sharing information hold infinite possibility. Leadership and imagination in looking at old problems in new ways and accepting responsibility to initiate change in a period of increasing complexity is paramount in keeping the homeland safe and guaranteeing the safety of future generations.

The research and arguments made in this thesis delineate the course of action for establishing a national capacity to better “collect and connect the dots” through the use of technology, acceptance and implementation of the suspicious activity reporting initiative and through a commitment to partnerships and collaboration at all levels to ensure that agencies have complete access to relevant information impacting their jurisdictions. Over the past eight years, elaborate plans have been created and visions articulated on methods for improving the information sharing environment. While state, local and tribal law enforcement and other partners are taking on a greater role, federal guidance is essential in providing for consistent funding, training, and the facilitation of technology for the collection and sharing of data and intelligence.

Identified policies and practices provided describe methods that are currently being used or that are proposed for use as well as guidance for implementation. While the appropriate technologies for achieving the prescribed information sharing goals are still being worked out, there is a commitment on the federal level to making the selected tool work. The greater challenge lies in promoting intelligence-led policing to smaller

agencies, which currently have no intelligence capacity. Leadership at all levels of law enforcement is needed to build a blueprint for this outreach plan that leverages existing systems, while being flexible for technology that provides for seamless sharing of information. Only when everyone shares this commitment to partnerships, using technology and standardization, will our country realize this potential to overcome these persistent impediments that have hindered information sharing.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

- Aitoro, J. (2009). *DHS Secretary promises more information sharing*. Retrieved May 25, 2009, from http://www.nextgov.com/nextgov/ng_20090225_3153.php
- Alpert, P. & Dunham, G. (1999). *Critical issues in policing*. Prospect Heights, IL: Waveleand Press, Inc.
- Aronson, E., Akert, R. D., & Wilson, T. D. (2006). *Social psychology* (6th ed.). Upper Saddle River, NJ: Pearson Prentice Hall.
- Arquilla, J. & Ronfeldt, D. (2002). *Networks and netwars: The future of terror, crime and militancy*. Santa Monica, CA: Rand.
- Bain, B. (2009, March 12). Napolitano backs fusion centers. *Federal Computer Week*. Retrieved June 9, 2009, from <http://www.fcw.com/Articles/2009/03/12/Napolitano-fusion-center.aspx>
- Brafman, O. & Beckstrom, A. (2006). *The starfish and the spider*. New York: Penguin Group.
- Bratton, W. (1999). *Turnaround*. New York: Random House, Inc.
- Bryson, J.M. (2004) *Strategic planning for public and non-profit organizations* (3rd ed.). Jossey-Bass. San Francisco: CA.
- Bureau of Justice. (2005). *Intelligence-led policing: The new intelligence architecture*. Washington, DC: Bureau of Justice Assistance.
- Bureau of Justice Assistance. (2006). *Fusion center guidelines: Developing and sharing information in a new era*. Washington, DC: author.
- Bureau of Justice Statistics. (2009). *Law enforcement statistics*. Retrieved March 3, 2009, from <http://www.ojp.usdoj.gov/bjs/lawenf.htm>
- Canada Safety Council (2004). *Don't just stand there—Do something*. Retrieved June 29, 2009, from <http://www.safety-council.org/info/community/bystander.html>
- Carter, D. (2004). *Law enforcement intelligence: A guide for state, local and tribal law enforcement agencies*. Washington DC: Department of Justice, Office of Community Oriented Policing Services.

- Carter, D. (2007). *Implementation of intelligence-led policing in state, local and tribal law enforcement agencies: Considerations and processes*. Washington, DC: Department of Justice Office of Community Oriented Policing Services.
- Chan Kim, W. & Mauborgne, R. (2005). *Blue ocean strategy: how to create uncontested market space and make competition irrelevant*. Boston, MA: Harvard Business School Publishing Corporation.
- Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism. (2008). *Testimony of William Bratton*. Retrieved July 20, 2009, from http://www.preventwmd.gov/9_10_08_william_bratton_testimony/ on June 8, 2009.
- Commission on the Roles and Capabilities of the U.S. Intelligence Community. (1996). "Executive Summary" in *Preparing for the 21st century: An appraisal of U.S. intelligence*. Washington, DC: Government Printing Office.
- Covey, S.M.R. (2006). *The speed of trust: The one thing that changes everything*. New York: Free Press.
- DeChurch, L.A. & Mesmer-Magnus, J.R. (2009). Information sharing and team performance: A meta-analysis. *Journal of Applied Psychology*, (94)2, 535–546. Retrieved June 20, 2009 from <http://www.apa.org/journals/releases/apl942535.pdf>
- Department of Homeland Security. (2003). *Homeland security presidential directive-8: National preparedness*. Washington, DC: author.
- Department of Homeland Security. (2007). *The National Strategy for homeland security*. Washington, DC: author.
- Department of Homeland Security. (2009). *DHS directive system, directive number: 252-11, revision #00: Office for State and Local Law Enforcement*. Washington, DC: author.
- Department of Justice. (2003). *National criminal information sharing plan*. Retrieved March 5, 2009, from http://www.it.ojp.gov/documents/NCISP_Plan.pdf
- Department of Justice. (2008). "Executive summary" in *National Criminal Information Sharing Plan*. Washington, DC: author (original published in 2003).
- Government of the District of Columbia. (2005). *District response plan*. Internal document, Government of the District of Columbia, Washington, DC: author.
- Edmund Burke. (n.d.). Webster's on-line dictionary. Retrieved September 16, 2009, from <http://www.websters-online-dictionary.org/Ed/Edmund+Burke.html>

- Federal Bureau of Investigation. (2004). *Protecting America against attack: A closer look at the FBI's Joint Terrorism Task Forces* [headline archives]. Retrieved March 8, 2009, from <http://www.fbi.gov/page2/dec04/jttf120114.htm>
- Federal Bureau of Investigation. (2006). *Crime in the United States, 2006*. Retrieved July 20, 2009, from http://www.fbi.gov/ucr/cius2006/data/table_08.html
- Federal Bureau of Investigation. *Intelligence directorate: The intelligence cycle*. Retrieved June 3, 2009, from http://www.fbi.gov/intelligence/di_cycle.htm
- Government Accountability Office. (2004). *Combating Terrorism: Evaluation of Selected Characteristics in National Strategies Related to Terrorism* (GAO-04-408T). Retrieved March 10, 2009, from: www.gao.gov/cgi/bin/getrpt?GAO-04-408T.
- Gerencser, M., Kelly, M., Napolitano, F. & Van Lee, R. (2009). *Megacommunities: How leaders of government, business and non-profits can tackle today's global challenges together*. New York: Palgrave MacMillan.
- Goldstein, H. (1996). *Community oriented policing: Towards best practice*. Queensland Australia: Griffith University, Centre for Crime Policy and Public Safety.
- Henry, V. *Compstat management in the NYPD: Reducing crime and improving quality of life in New York City*. Retrieved July 20, 2009, from http://www.unafei.or.jp/english/pdf/PDF_rms/no68/07_Dr.%20Henry-1_p100-116.pdf
- Home Office. *About the police*. Retrieved March 9, 2009, from <http://www.homeoffice.gov.uk/police/about/?view=Standard>
- Howitt, A. & Pangi, R. (2003). Intergovernmental challenges of combating terrorism. In *Countering terrorism: Dimensions of preparedness*. Cambridge, MA: MIT Press.
- Information Commissioner's Office. *Framework code for practice of sharing personal*. Retrieved March 10, 2009, from [informationhttp://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf)
- Information Sharing Environment. *Nationwide suspicious activity reporting initiative*. Retrieved March 9, 2009, from <http://www.ise.gov/pages/sar-initiative.html>
- Intelligence Reform and Terrorism Prevention Act of 2004, U.S.C., Section 1016.

- Jennings, T. (2009, June 5). Fusion centers key to efforts to combat drug violence officials say. *The New Mexico Independent*. Retrieved on June 8, 2009 from: <http://newmexicoindependent.com/28966/fusion-centers-key-to-fed-efforts-at-combating-drug-violence>
- Johnson, L. & Wirtz, J. (2008) *Intelligence and national security: The secret world of spies*. New York: Oxford University Press.
- Kaplan, E. (2007). *Fusion centers*. Retrieved May 2, 2009, from <http://www.cfr.org/publication/12689/>
- Kelling, G. & Wilson, Q. (1982, March). Broken windows. *The Atlantic*. Retrieved on July 5, 2009, from <http://www.theatlantic.com/doc/198203/broken-windows>
- Law Dog Files. The police are the public and the public are the police. (2008, April 6). Retrieved July 16, 2009, from <http://thelawdogfiles.blogspot.com/2008/04/police-are-public-and-public-are-police.html>
- Lowenthal, M. (2006). *Intelligence: From secrets to policy*. Washington, DC: CQ Press.
- Major City Chiefs Association Homeland Security Committee. (2008). *Twelve tenets to prevent crime and terrorism*. Columbia, MD: author.
- Major Cities Chiefs Association. (2008). *Suspicious activity report: Support and implementation project*. Columbia, MD: author.
- Present Outlook. (2009, January 17). Make excellence a habit. Retrieved July 12, 2009, from <http://presentoutlook.com/excellence/>
- Manhattan Institute Center for Policing Terrorism. (2006). *Practical guide to intelligence-led policing*. Retrieved July 20, 2009, from <http://www.cpt-mi.org/pdf/NJPoliceGuide.pdf>
- Maple, J. (1999). *The Crime Fighter*. New York: Doubleday
- Marcus, L., Dorn, B., & Henderson, J. (2005). *Meta-leadership and national emergency preparedness*. Boston, MA: John F. Kennedy School of Government.
- Metropolitan Police. *Metropolitan police home page*. Retrieved March 8, 2009, from http://www.met.police.uk/so/counter_terrorism.htm
- Metropolitan Police Department. (2008). Office of Human Resource Management Report. Internal document, Metropolitan Police Department, Washington, DC.

- Napolitano, J. (2009). *Confirmation hearing statement*. Retrieved on May 8, 2009, from http://www.cfr.org/publication/18283/janet_napolitanos_confirmation_hearing_statement.html
- Metropolitan Washington Council of Government. (2007). Appendix F in National Capitol Region Hazard Identification and Risk Assessment. (FOUO). Internal document Metropolitan Washington Council of Government.
- National Commission on Terrorist Attacks upon the United States. (2004). *The 9/11 commission report: Final report of the National Commission on Terrorist Attacks Upon the United States*. New York: W.W. Norton.
- National Policing Improvement Agency. *Impact*. Retrieved March 8, 2009, from <http://www.npia.police.uk/en/8489.htm>
- Navy Criminal Investigative Service. (2008). *NCIS Technical Overview—News*. Retrieved June 27, 2008, from <http://www.ncis.navy.mil/ncis/linx/technical.html>
- The New York Academy of Sciences. (2009, June 19) Zimbardo opens first world congress on positive psychology. *Member News*. Retrieved June 30, 2009 from <http://www.nyas.org/MemberCenter/MemberNews.aspx?cid=52aa1e94-9fda-4def-b37a-4fa3b256e15f>
- Office of the Director of National Intelligence. (2009). *National intelligence—A consumer's guide*. Retrieved June 8, 2009, from http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf
- Office of the Director of National Intelligence. (2005). *The National intelligence strategy of the United States of America: Transformation through integration and innovation*. Washington, DC: author.
- Phillips, Donald T. (1997). *The founding fathers on leadership: Classic teamwork in changing times*. New York: Business Plus.
- Randol, M. A. (2006). *Homeland security intelligence: Perceptions, statutory definitions and approaches*. Washington, DC: Congressional Research Service.
- Ratcliffe, J.H. (2008) *Intelligence-Led Policing*. Cullompton, United Kingdom: Willan Publishing.
- Senate Select Committee on Intelligence: Hearing on the state of intelligence reform, testimony of Cathy L. Lanier*. (2007). Retrieved on May 8, 2009, from http://www.fas.org/irp/congress/2007_hr/012507lanier.pdf

- Senate Select Committee on Intelligence: Hearing on the state of intelligence reform, testimony of Charles E. Allen.* (2007). Retrieved on May 8, 2009, from http://www.fas.org/irp/congress/2007_hr/012507allen.pdf
- Sims, J. & Gerber, B. (2005) *Transforming U.S. intelligence*. Washington, DC: Georgetown University Press.
- Snowden, D., and Boone, M. (2007) *A leader's framework for decision making*. Cambridge, MA: Harvard Business Review.
- Taylor, H. (2004, February). Similar levels of fear of terrorism in U.S.A. and Great Britain [Harris Interactive poll]. Retrieved June 22, 2009, from http://www.harrisinteractive.com/harris_poll/index.asp?PID=437
- Treverton, G. (2005) *The next steps in reshaping intelligence*. Santa Monica, CA. Rand Corporation.
- UK Intelligence Community. *Joint terrorism analysis center (JTAC)*. Retrieved March 9, 2009, from <http://www.intelligence.gov.uk/agencies/jtac.aspx>
- Wenger, A. & Zimmerman, D. (2007). *How states fight terrorism*. London: Lynne Rienner Publishers, Inc.
- White House. (2007). *National strategy for information sharing: Successes and challenges in improving terrorism-related information sharing*. Washington, DC: author.
- White House. (2009). *Homeland security and counterterrorism*. Retrieved July 21, 2009 from: http://www.whitehouse.gov/issues/homeland_security/
- Yin, R. K. (2008). *Case study research: Design and methods*. 4th ed. Thousand Oaks, CA: Sage Publications, Ltd.
- Zegart, A. (2007). *Spying blind: The CIA, the FBI, and the origins of 9/11*. Princeton, NJ: Princeton University Press.
- Zimbardo, P. (2007). *The Lucifer effect*. New York: Random House, Inc.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
Ft. Belvoir, VA
2. Dudley Knox Library
Naval Postgraduate School
Monterey, CA
3. Cathy L. Lanier
Chief of Police, Metropolitan Police Department
Washington, DC
4. Tom Frazier
Executive Director, Major Cities Chiefs
Columbia, MD