NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A MODEL FUSION CENTER TO ENHANCE INFORMATION SHARING

by

Walter E. Smith

December 2011

Thesis Co- Advisors: Nadav Morag
Patrick Miller

Approved for public release; distribution unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

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

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** December 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE Developing a Model Fusion Center to Enhance Information Sharing	**5. FUNDING NUMBERS**
6. AUTHOR (S) Walter E. Smith	
7. PERFORMING ORGANIZATION NAME (S) AND ADDRESS (ES) Naval Postgraduate School Monterey, CA 93943-5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number _____N/A_____.

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

13. ABSTRACT (maximum 200 words)

Fusion Centers are in a unique position to provide the necessary collaborative space to bring the federal intelligence community together with state, local and tribal initiatives to support homeland security efforts at the grass roots level. Fusion Centers are described as a collaborative effort of two or more agencies to share, or more importantly, fuse information or data from multiple sources. Although, fusion centers have developed at different intervals, the U.S. Department of Homeland Security has provided guiding documents to support fusion center maturation. This research examines these documents and proposed strategies incorporated into four proficient fusion centers in the Northeast Region of the United States to identify best or smart practices, success stories and areas for improvement.

There has been a plethora of literature written concerning fusion centers since the tragedies of September 11, 2001. These categories of the literature include: official documents, guidelines and lessons learned for intelligence input, civil liberties safeguards and protections and literature dealing with the intelligence cycle and information sharing. The focus of this thesis is to examine correlation between the implementation of the current United States Department of Homeland Security and U.S. Department of Justice suggested Fusion Center Guidelines, and the employment of these guidelines in the successful development of a model fusion center.

14. SUBJECT TERMS Fusion Center, Fusion Center Guidelines, Success Stories, Civil Liberties Safeguards, U.S. Department of Justice, Fusion Center Maturation, Intelligence Cycle	**15. NUMBER OF PAGES** 115
	16. PRICE CODE

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

NSN 7540-01-280-5500 Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEVELOPING A MODEL FUSION CENTER TO ENHANCE INFORMATION SHARING

Walter E. Smith
Captain, Philadelphia Police Department, Philadelphia, Pennsylvania
B.A., Eastern University, Saint David's Pennsylvania, 2006

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
December 2011

Author: Walter E Smith

Approved by: Nadav Morag
Thesis Co-Advisor

Patrick Miller
Thesis Co-Advisor

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Fusion Centers are in a unique position to provide the necessary collaborative space to bring the federal intelligence community together with state, local and tribal initiatives to support homeland security efforts at the grass roots level. Fusion Centers are described as a collaborative effort of two or more agencies to share, or more importantly, fuse information or data from multiple sources. Although, fusion centers have developed at different intervals, the U.S. Department of Homeland Security has provided guiding documents to support fusion center maturation. This research examines these documents and proposed strategies incorporated into four proficient fusion centers in the Northeast Region of the United States to identify best or smart practices, success stories and areas for improvement.

There has been a plethora of literature written concerning fusion centers since the tragedies of September 11, 2001. These categories of the literature include: official documents, guidelines and lessons learned for intelligence input, civil liberties safeguards and protections and literature dealing with the intelligence cycle and information sharing. The focus of this thesis is to examine correlation between the implementation of the current United States Department of Homeland Security and U.S. Department of Justice suggested Fusion Center Guidelines, and the employment of these guidelines in the successful development of a model fusion center.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
ACS	Automated Case System
AMSC	Area Maritime Security Committee
AOR	Area of Responsibility
ATAC	Anti-Terrorism Advisory Council
ATF	Alcohol Tobacco and Firearms
BCOT	Building Communities of Trust
BICE	Bureau of Immigration and Customs Enforcement
BLC	Baseline Capabilities
CFR	Code of Federal Regulation
CI/KR	Critical Infrastructure/Key Resources
COC	Critical Operational Capability
CTTWG	Counter Terrorism Training Coordination Work Group
DIAC	Colorado Information and Analysis Center
CRS	Congressional Service Report
DEA	Drug Enforcement Administration
DHS	Department of Homeland Security
DIAC	Delaware Information and Analysis Center
DoD	Department of Defense
DOJ	Department of Justice
DNI	Director of National Intelligence
DSP	Delaware State Police

DVIC	Delaware Valley Intelligence Center
DVRWG	Delaware valley Regional Work Group
EOC	Emergency Operations Center
FAMS	Federal Air Marshalls
FCG	Fusion Center Guidelines
FFC	Florida Fusion Center
GIWG	Global Intelligence Working Group
HITA	High Intensity Drug Trafficking Area
HSA	Homeland Security Advisor
HSIN	Homeland Security Information Sharing Network
HSSLIC	Homeland Security State and Local Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act
IACP	International Association of Chiefs of Police
ICE	Immigration Customs Enforcement
IO	Intelligence Officer
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ISEPGC	Information Sharing Environment Privacy Guidance Council
JIEM	Justice Information Exchange Model
JRIC	Joint Regional Intelligence Center
JTTF	Joint Terrorism Task Force
LEO	Law Enforcement Online
MCAC	Maryland Coordinating and Analysis Center
MCCA	Major Cities Chiefs Association
MOA	Memorandum of Agreement

MOU	Memorandum of Understanding
NCISP	National Criminal Intelligence Sharing Plan
NCTC	National Counter Terrorism Center
NCRIC	Northern California regional Intelligence Center
NDA	Non-Disclosure Agreement
NDEX	National Data Exchange
NIEM	National Information Exchange Model
NJOHPS	New Jersey Office of Home Land Security and Preparedness
NJOEM	New Jersey Office of Emergency Management
NJSP	New Jersey State Police
NOC	National Operations Center
ODNI	Office of the Director of National Intelligence
PACIC	Pennsylvania Criminal Intelligence Center
PARTSWG	Philadelphia Area Regional transit Security Work Group
PMISE	Program Manager Information Sharing Environment
RFI	Request for Information
RFS	Request for Service
RISS	Regional Information Sharing System
ROIC	Regional Operations Intelligence Center
SAR	Suspicious Activity Report
SBU	Sensitive but Unclassified
SEPARTF	Southeastern Pennsylvania Regional Terrorism Task force
SIPRNET	Secret Internet Protocol Router
SLT	State Local Tribal
SLTWG	State Local Tribal Working Group

SOP	Standard Operating Procedure
TLO	Terrorism Liaison Officer
TSC	Terrorism Screening Center
XML	Extensive Markup Language

ACKNOWLEDGMENTS

There are 86,400 seconds in a day, how often do we take one of those seconds to say thank you?

My faith in God, the support of my family, as well as my fellow classmates, has made this journey not only possible, but also empowering. I would like to thank my family for their sacrifice, understanding and patience, as well as the enduring love they have given to me everyday, but particularly over the last 18months. I am truly blessed to have you in my life.

My sincere thanks to the Philadelphia Police Department, and in particular Police Commissioner Charles H. Ramsey, for his continued support and guidance in allowing me to grow and mature in the field of Homeland Security.

I am grateful to the Naval Postgraduate School and the U.S. Department of Homeland Security Center for Homeland Defense and Security for providing me with an opportunity to experience a level of education that was truly astounding.

I would also like to acknowledge and thank the extraordinary cadre of NPS instructors, staff, and my two thesis advisors, Nadav and Pat, for helping to make this experience so rewarding.

Finally, to the men and women on the front lines of the New Jersey Regional Operations Intelligence Center, the Delaware Information and Analysis Center, the Pennsylvania Criminal Intelligence Center and the Maryland Coordinating and Analysis Center, I am truly grateful for your support and extremely proud of your accomplishments in providing safety and security to our communities. It is an honor to know you, and I look forward to working with you and learning from you in the future.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> Give me six hours to chop down a tree and I will spend the first four sharpening the axe
>
> Abraham Lincoln

Proficiency and perfection are critical components in today's fusion center environment. Tasked with the ability to share information and create collaboration between federal, state, local and tribal partners while managing an all crimes and all hazards perspective, in addition to preventing terrorism, will require a finely honed instrument.

The value proposition for fusion centers is that by integrating various streams of information and intelligence, including that flowing from the federal, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people, economic infrastructure, and communities can be developed and translated into protective action. The ultimate goal of fusion is to prevent manmade (terrorist) attacks and to respond to natural disasters and manmade threats quickly and efficiently should they occur. As recipients of federal government-provided national intelligence, another goal of fusion centers is to model how events inimical to U.S. interests overseas may be manifested in their communities, and align protective resources accordingly. There are several risks to the fusion center concept, including potential privacy and civil liberties violations, and the possible inability of fusion centers to demonstrate utility in the absence of future terrorist attacks (Rollins, 2007, p.1)

In the aftermath of September 11, 2001, it became clearly evident that an attack on U.S. soil was not only possible; it was also highly probable. In addition:

> In the spring of 2002, law enforcement executives and intelligence experts attending the International Association of Chiefs of Police (IACP) Criminal Intelligence Sharing Summit recognized that local, state, tribal, and federal law enforcement agencies and the organizations that represent

> them must work towards common goals, gathering information and producing intelligence within their agency and sharing that intelligence with other law enforcement and public safety agencies.
>
> (National Criminal Intelligence Sharing Plan, 2003, p. 1)

The development of fusion centers provides significant evidence of America's willingness to address current and future threats and enhance information exchange by "Building Communities of Trust" (BCOT) based on common safety and security concerns and in doing so protect the civil rights and civil liberties of individuals by upholding the Constitution of the United States as our core foundation based on sound principles and values. "The Building Communities of Trust (BCOT) initiative focuses on developing relationships of trust between law enforcement, fusion centers, and the communities they serve, particularly immigrant and minority communities, so that the challenges of crime control and prevention of terrorism can be addressed" (Wasserman, 2010, p. 3)

On March 11, 2009, United States Department of Homeland Security Secretary Napolitano related in her remarks to the National Fusion Center conference in Kansas City, Missouri," I believe that fusion centers will be the centerpiece of state, local, federal intelligence-sharing for the future and that the Department of Homeland Security will be working and aiming its programs to underlie fusion centers." **(**Napolitano, 2009**)**

Fusion centers serve not only as physical space for multi-agency collaboration and information sharing; they also present an opportunity for change to increase protection through prevention; however, formal adoption of this strategic initiative may require a unified acceptance across the Intelligence Community. "In their January 2005 survey, the National Governors Association Center for Best Practices revealed that states ranked the development of state fusion centers as one of their highest priorities." (Fusion Center Guidelines, p. 1)

A. ARGUMENT FOR THE DEVELOPMENT OF A MODEL FUSION CENTER

Fusion centers have been described as a grass roots effort to identify threats at the state and local levels of government in an effort to support the federal intelligence community in preventing crime and terrorism. These efforts have become more inclusive to also address natural disasters in an all hazards approach. The integration of multidiscipline agencies such as fire, public health, and emergency management, as well as the private sector, has opened lines of communications and increased collaboration in an effort to indentify the preincident indicators of terrorism and include such programs as Suspicious Activity Reporting (SAR's).

Fusion Centers are identified by the United States Department of Justice 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. Fusion Centers are intended to support information exchange at the federal, state and local levels of government and to enhance the overall security of the Homeland. State and local/regional fusion centers gather information in their area of responsibility (AOR) and attempt to create syntheses of information combined with federal intelligence to see the big picture or to conduct predictive analysis to prevent another terrorist attack. Fusion Centers have be defined as a mechanism to detect and prevent all threat, all crime and all hazard incidents; however, there is no requirement that these centers contain all of these capabilities, and each center differs based on their individual responsibilities as well as direction provided by state and local governments. In addition, fusion centers add increased value to the overall intelligence community.

This introductory section describes the fusion center value proposition and provides a greater understanding of the necessity of fusion centers; identifies primary and regional fusion centers, defines the intelligence cycle and intelligence systems to share information, as well as reporting current success stories of fusion center operations. This section is presented to gain a greater understanding of fusion center concepts.

1. The Fusion Center Value Proposition

Fusion Centers add value to the intelligence community faced with both international and domestic threats.

- Conceptually, the argument that fusion centers represent a vital part of our nation's homeland security relies on at least four presumptions: Intelligence, and the intelligence process, plays a vital role in preventing terrorist attacks.
- It is essential to fuse a broader range of data, including nontraditional source data, to create a more comprehensive threat picture. State, local, and tribal law enforcement and public sector agencies are in a unique position to make observations and collect information that may be central to the type of threat assessment referenced above.
- Having fusion activities take place at the subfederal level can benefit state and local communities and possibly have national benefits as well.

2. DHS's Value Proposition

The Department of Homeland Security (DHS) has stated that the value of fusion centers to both DHS and state and local authorities include a number of common and distinct functions. The following four areas were assessed by DHS as being common benefits fusion centers and would yield to DHS and state and local authorities:

- Clearly defined information-gathering requirements.
- Improved intelligence analysis and production capabilities.
- Improved information/intelligence sharing and dissemination.
- Improved prevention, protection, response, and recovery capabilities.

DHS also outlined areas of how it and state and local authorities would benefit uniquely from participation in the fusion centers. Unique benefits to DHS include:

- Improved information flow from state and local entities to DHS.

- Improved situational awareness.
- Improved access to local officials.
- Consultation on state and local issues.
- Access to nontraditional information sources.

According to DHS, the unique benefit of fusion centers to state and local authorities includes:

- Improved information flow from DHS to states and localities.
- Increased on-site intelligence and DHS law enforcement expertise and capabilities.
- Clearly defined DHS entry point.
- Insight into federal priorities.
- Participation in dialogue concerning threats" (Rollins, 2007 p. 3).

To increase interconnectivity, as well as ensuring information sharing capability across the Fusion Center Network, the U.S Department of Homeland Security has supported the establishment of a myriad of state and Regional Fusion Centers across the United States. These centers described below are designated as primary and recognized fusion centers.

3. Primary and Recognized Fusion Centers

There are currently 72 fusion centers throughout the country, 50 State Centers and 22 Regional Centers. Fusion Centers are owned and operated by state and local governments. The primary designation refers to the state centers designated by the state's Governor, while recognize centers refer to regional centers.

> Primary fusion centers serve as the focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information and have additional responsibilities related to the coordination of critical operational capabilities across the statewide fusion process with other recognized fusion centers or major urban area fusion centers.
>
> (U.S Department of Homeland Security, 2011 p. 1)

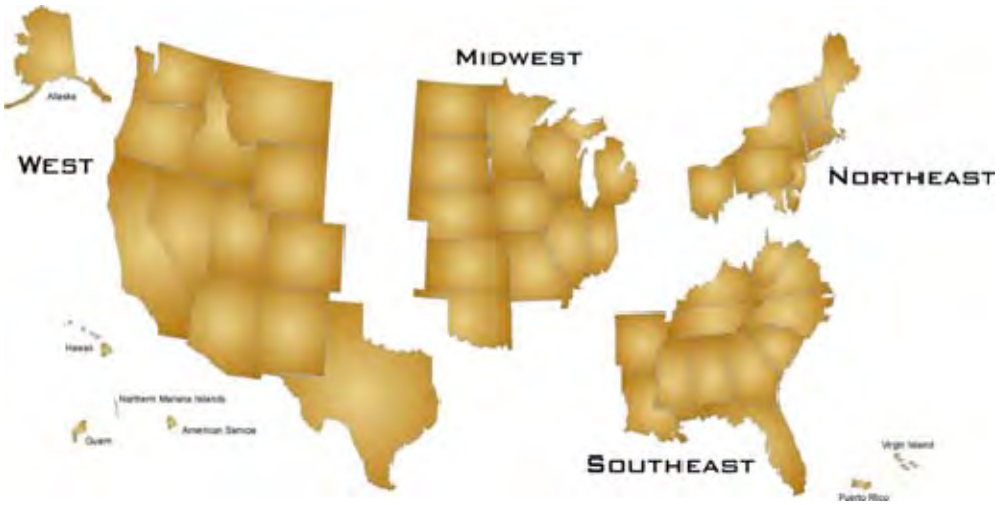

Figure 1. National Integrated Network of Fusion Centers (From Porter, Office of the Director of National Intelligence, 2011, p. 42)

72 designated fusion centers

50 Primary states Centers

22 Major Urban Areas Centers

Fusion Centers are tasked with gathering information from a multitude of sources; however, this information adds little value without a systematic process or approach. Connecting the dots can only be achieved, by first identifying the dots. Below is a review of the systems currently being utilized to support federal, state and local information sharing, which includes the intelligence cycle.

4. Importance of Intelligence and Intelligence Sharing

"Failure to connect the dots" were the words used to describe the events that led to the attacks on September11, 2011. However, the question remains, could we have made a difference if we had seen the big picture? Today's world is becoming smaller, with the speed of travel and the use of the Internet for rapid communications; a distant enemy separated by time and geography is no longer the case. The lines between domestic and international activities are becoming blurred. Terrorists, as well as criminals, seek benefits through transnational operations looking for the path of least

resistance. Decentralized networks of criminal and terrorist organizations are becoming the norm as groups, such as Al-Qaeda, spread across the Middle East and Africa. Terrorist activities can occur anywhere and at anytime. It is said it takes a network to defeat a network. “Decentralized organizations can be so resilient that it’s hard to affect their internal structure. The best opponent for a starfish organization is often another starfish.” (Brafman, 2006, p. 155) Fusion Centers utilizing a decentralize structure are perfectly positioned to collect, analyzes and disseminate real time information to support federal, state, local and tribal governments in their terrorism and crime prevention efforts.

Figure 2. The Intelligence Process (From U.S. Department of Homeland Security and U.S. Department of Justice, 2006, p. 19)

The importance of intelligence sharing is furthered emphasized in a CRS report to Congress titled Fusion Centers Issues and Options for Congress.

To briefly expand upon the four presumptions, which are often cited in arguments, that fusion centers are valuable to homeland security, it is important to first focus on the role of intelligence in homeland security, especially with regard to prevention efforts. At the First Annual National Fusion Center Conference, Secretary Chertoff reiterated to the hundreds of state and local conference participants that he views intelligence as an early warning system that allows public safety officials to get a jump

on the adversary. The 9/11 Commission states, "Not only does good intelligence win wars, but the best intelligence enables us to prevent them from happening altogether." All major post-9/11 government reorganizations, legislation, and programs have emphasized the importance of intelligence in preventing, mitigating, and responding to future terrorist attacks. This includes the creation of the Department of Homeland Security, specifically the Department's Office of Intelligence and Analysis, the passage of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2005 P.L. 108–458), intelligence sharing provisions of the USA PATRIOT Act (P.L. 107–56), as well as the creation of the Intelligence Sharing Environment (ISE), among numerous other developments. Another presumption that is often cited is that to prevent attacks intelligence needs to include a broad range of data, including that from nontraditional sources—state and local homeland security-related personnel and the private sector. The Commission found that the September 11 attack plots: fell into the void between foreign and domestic threats. The foreign intelligence agencies were watching overseas, alert to foreign threats to U.S. interests there. The domestic agencies were waiting for evidence of a domestic threat from sleeper cells within the United States. As such, the 9/11 Commission concluded there was a necessity for fusing domestic and foreign intelligence. Fusing foreign intelligence with a wide spectrum of domestic information is the stated primary purpose of most fusion centers. Locally gathered information collected from a broad array of law enforcement, public health and safety, as well as private sector sources, is fused with intelligence collected and produced by the security resources" (Rollins, 2007, p. 5).

Intelligence collection and intelligence sharing continues to be a key component echoed in the 2010 National Security Strategy.

> Intelligence: Our country's safety and prosperity depend on the quality of the intelligence we collect and the analysis we produce, our ability to evaluate and share this information in a timely manner, and our ability to counter intelligence threats. This is as true for the strategic intelligence that informs executive decisions as it is for intelligence support to homeland security, state, local, and tribal governments, our troops, and critical national missions. We are working to better integrate the Intelligence Community, while also enhancing the capabilities of our Intelligence Community members. We are strengthening our partnerships with foreign intelligence services and sustaining strong ties with our close

allies and we continue to invest in the men and women of the Intelligence Community.

(National Security Strategy, 2010, p. 15)

5. Intelligence Systems to Share Information

There are many systems at the federal level of government available to share information across the fusion center network. These systems are primarily utilized to share information at both the classified and unclassified levels. Although, fusion centers utilize internal information sharing systems, networks and systems to which state and local fusion centers have access at the federal level provide a mechanism to engage the intelligence community.

Table 1. Federal Intelligence Sharing Systems

Networks and Systems to Which state and local Fusion Centers May Have Access System or network	**Owner**	**Sensitivity level**	**Brief summary of selected functions**	**Types of information shared**
Homeland Security Information Network (HSIN)	DHS	Sensitive but unclassified	• _Supports secure communications and collaboration across the law enforcement community.	• _DHS' primary system for sharing terrorism and related information. • _Supplies suspicious incident and pre-incident information, 24x7 situational awareness, and analyses of terrorist threats, tactics, and weapons.
Federal Protective Service (FPS) Secure Portal System	DHS	Sensitive but unclassified	• _Secret-level classified communications network system with which government agencies are able to share information and collaborate in order to detect, deter, and mitigate threats to the homeland at the Secret level. • _Provides state and local governments with their own area to post and manage collateral-level information for access by	• _Manages information to help ensure the safety and security of federal buildings, protection officers, and visitors.

Networks and Systems to Which state and local Fusion Centers May Have Access System or network	Owner	Sensitivity level	Brief summary of selected functions	Types of information shared
			their federal law enforcement and intelligence community partners.	
Homeland Secure Data Network (HSDN)	DHS	Secret	• _Serves as a global area network used for communicating Secret information. • _Operated, maintained, and access controlled by the FBI.	• _Transmits homeland security data in support of activities including intelligence, investigations, and inspections that are classified at the Secret level.
Federal Bureau of Investigation Network (FBINET)	FBI	Secret	• _Serves as a real-time on-line controlled- access communications and information-sharing data repository. • _Supports an Internet-accessible focal point for electronic sensitive but unclassified communication and information sharing with federal, state, local, and tribal law enforcement agencies.	• _Communicates Secret information, including investigative case files and intelligence pertaining to national security.
Law Enforcement Online (LEO)	DOJ	Sensitive but unclassified		• _Contains information about, among other things, antiterrorism, intelligence, law enforcement, and criminal justice.

(From GAO-08-35, Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers, 2007, p. 13

Table 2. Federal Intelligence Sharing Systems, Cont'd

System or network Owner Sensitivity level Brief summary of selected functions Types of information shared	Owner	Sensitivity level	Brief summary of selected functions	Types of information shared
Regional Information Sharing Systems Automated Trusted Information Exchange (RISS ATIX)	State and local officials of the RISS program with funding through a DOJ grant	Sensitive but unclassified	• _Offers services similar to RISSNET to agencies beyond the law enforcement community, including executives and officials from governmental and nongovernmental agencies and organizations that have public safety responsibilities. • _Partitioned into 39 communities of interest such as critical infrastructure, emergency management, public health, and government officials. Services offered through its Web pages are tailored for each community of interest and contain community-specific news articles, links, and contact information.	• _Users can post timely threat information, documents, images, and information related to terrorism and homeland security, as well as receive DHS information, advisories, and warnings.

(GAO-08-35, Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers, 2007, p. 14)

In developing a model fusion center, it is also important to establish a barometer for success and to gain an understanding of what constitutes a successful fusion center. Described below are examples of successful fusion center initiatives.

6. The Success of Fusion Centers

There have been several incidents where fusion centers across the country have supported various crime and terrorism prevention initiatives. These efforts, although sometimes remaining unnoticed, have contributed to the overall safety and security of our communities and our country.

Every day, state and major urban area fusion centers receive, analyze, disseminate, and gather homeland security information in order to protect our local communities. Fusion centers enable DHS and other federal partners to connect with state, local and tribal law enforcement and homeland security partners to collaborate on terrorism, crime and other homeland security issues. For instance, at the end of June, the Colorado Information and Analysis Center (CIAC) played an instrumental role in the arrest of an individual suspected of placing two bombs at a local bookstore. In June 2011, the Lakewood Police Department was notified about an incident at a bookstore at a Colorado mall. Due to the nature of the crime, the Lakewood Police Department notified the FBI of the incident who then activated the local joint Terrorism Task Force (JTTF). The JTTF is led by the FBI and comprised of local, state and federal law enforcement agencies. After the JTTF collected preliminary information, it was sent to the fusion center and distributed nationwide and to Terrorism Liaison Officers (TLO) requesting information that might relate to the incident. Later that same day, the suspect crashed his vehicle on a highway in Clear Creek County, CO. A Colorado state Trooper, who is also a TLO, investigated the crash and took the suspect into custody on charges related to menacing and driving under the influence of alcohol. Less than 24 hours later, the Colorado fusion center released additional information about a possible suspect in the bookstore incident, including information about the suspect's vehicle. When the trooper received this information he suspected that the driver he had arrested was the suspect in the bookstore mall bombing. He contacted the fusion center to provide this information,

which in turn, notified the JTTF. The suspect was later charged with crimes related to threatening public safety related to the placing of the bombs in the bookstore. This event shows the important role of information sharing and fusion centers in our nation's homeland security effort. Hometown security is essential to homeland security. DHS support of fusion centers, like the one in Colorado, empowers local officials to better protect their communities and the nation from evolving security threats.

In addition, fusion centers continue to serve as hubs for information sharing to defeat potential terrorist related incidents**.** "On August 4, 2007, the Department of Homeland Security deployed IO assigned to the Florida Fusion Center (FFC) received a call from the Florida Homeland Security Adviser (HSA) regarding an on-going traffic stop of two University of South Florida students in Goose Creek, South Carolina. The HSA did not have specifics other than it involved a bomb squad and a Florida registered vehicle. The Department of Homeland Security National Operation's Center (NOC) had no visibility of the traffic stop but began to query North Carolina and South Carolina. The Department deployed Intelligence Officers (IO) and received further information regarding the incident from an FFC representative with specific information he received from a colleague at Operation SeaHawk in South Carolina. The FFC was able to provide the tag number of the vehicle and conducted full database checks on the vehicle's history and owner information. All of the results were provided to the NOC, South Carolina, and Tampa-JTTF within minutes for their situational awareness. The FFC was able to provide full database checks on the subjects to South Carolina and Tampa-JTTFs. An indictment was unsealed August 31, 2007, against the two students, Ahmed Abdellatif Sherif Mohamed and Youssef Samir Megahed, both Egyptian nationals, charging them with transporting explosives in interstate commerce without permits. Mohamed was also charged with distributing information about building and using an explosive device. Mohamed pled guilty to providing material support to terrorists on June 18, 2008, and was sentenced to 15 years in prison December 18, 2008. Megahed was acquitted of explosives charges in April 2009. Immigration and Customs Enforcement later took custody of him and launched removal proceedings against him. An immigration judge declined to find Megahed removable and granted his Motion to Terminate on October 9,

2009. The department decided not to appeal the judge's order. If it were not for the fusion centers and an Operation SeaHawk representative, Florida and the Department would not have gained situational awareness regarding the incident. Florida was able to provide relevant information regarding the subjects and associates to South Carolina law enforcement officials and the JTTF within minutes to aid in their investigation"(U.S. department of Homeland Security, 2011, p. 1).

B. PROBLEM STATEMENT

Fusion Centers are identified by the United States Department of Justice 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. Fusion Centers are intended to support information exchange at the federal, state and local levels of government and to enhance the overall security of the Homeland. State and local/regional fusion centers gather information in their area of responsibility (AOR) and attempt to create syntheses of information combined with federal intelligence to see the big picture or to conduct predictive analysis to prevent another terrorist attack. Today, there are currently 72 fusion centers throughout the county comprised of 50 state and 22 local or regional centers. These centers created in 2004 and 2005 were initially developed with few guidelines or formalized structures, which limited their ability to effectively communicate or share information with other federal, state and local partners. This lack of interoperability resulted in information "silos," as centers intended to share information were inefficient in meeting their intended purpose. (U.S. Department of Homeland Security, U.S Department of Justice, Justice, 2005, p. 1). The U.S. Department of Homeland Security (DHS) and U.S. Department of Justice (DOJ) Global Justice Information Sharing Initiative's (Global) has since produced many strategic documents to serve as templates or guidelines to support the structured development of fusion centers as well as to address all threats, all crime and all hazard issues.

It is uncertain, at this time, if these strategies are effective or require change in an effort to develop a model fusion center. Fusion centers developed without guidance or

formalize structure may become fractionalized limiting their ability to serve their intended customers or stakeholders, as well as the overall fusion center network.

In addition, Fusion Center Directors in conjunction with the federal government have identified "Four Critical Operational Capabilities" (COCs) necessary for successful fusion center operations (U.S. Department of Homeland Security, U.S Department of Justice, 2010, p. 5). These capabilities, including the ability to receive classified and unclassified information across various networks or systems, the ability to assess local implications of threat information, the ability to further disseminate threat information with state, local and private sector partners, and the ability to gather locally-generated information, aggregate, analyze and share this information with federal partners will require fusion centers to develop short-term gap mitigation strategies. Furthermore, fusion centers will be required to gather information lawfully to ensure the protection of privacy, civil rights and civil liberties of individuals, which may be overlooked as information is gathered and exchanged between fusion centers. (Privacy, Civil Rights, and Civil Liberties Compliance Verification for the Intelligence Enterprise, 2010, p. 1).

In summary, the current mix of fusion center models results in a wide variance in levels of capabilities, and they are not all well prepared to deal with classified materials both in terms of access and in terms of dissemination to others or with privacy/civil rights issues. The establishment of a National Homeland Security Fusion Center Doctrine may be necessary to support standardization among the plethora of fusion centers throughout the country. The adage: 'if you seen one fusion center you've seen one fusion center' constitutes a sense of inferiority or lack of uniformity that may or may not be an accurate depiction of overall fusion center's efficiency and effectiveness.

C. RESEARCH QUESTIONS

What will a model of an optimal fusion center, one that addresses the critical operational capabilities, as well as protecting Civil Liberties and Civil Rights of the general public during Suspicious Activity Reporting, need to look like?

Is a National Homeland Security Fusion Center Doctrine necessary to ensure efficiency and effectiveness across the Fusion Center Network?

What are the necessary core components for fusion centers to ensure success and how will fusion centers achieve operational relevance?

Are there standard performance measures to support Fusion Center Operations?

D. SIGNIFICANCE OF RESEARCH

There has been a plethora of literature written concerning fusion centers since the tragedies of September 11, 2001. These categories of the literature include: official documents, guidelines and lesson-learned for intelligence input, civil liberties safeguards and protections and literature dealing with the intelligence cycle and information sharing. This thesis will attempt to identify the correlation between the implementation of the current United States Department of Homeland Security, the U.S. Department of Justice suggested Fusion Center Guidelines, and the employment of these guidelines in the successful development of a model fusion center, including the identification of best or smart practices, lessons learned and future requirements or gaps requiring additional exploration.

Future research efforts will include observations and analysis of four fusion center's daily operations, as well as a review of fusion center documents and operating procedures. The information acquired during this process will serve the immediate consumers, Fusion Center Directors, as well as the public and private sector organizations identified as fusion center product recipients. In addition, this thesis will serve as a barometer to support Homeland Security practitioners and leaders nationally by identifying future strategies to enhance fusion center development.

In addition to identifying the key components that constitutes a model fusion center, this research also provides an opportunity for the author to gather information for a future practical application of lessons learned. The information acquired during this thesis will be utilize to support the development of a future fusion center located in the Delaware Valley region, whose mission will be to support four state fusion centers located in the states of New Jersey, Delaware, Pennsylvania and Maryland from a regional area of operations. Below is a description of the proposed fusion center located in the Delaware Valley region.

1. Proposed Delaware Valley Intelligence Center (DVIC)

On behalf of the Delaware Valley Emergency Management and Homeland Security Coordination Council (DVEM&HSCC), the Southeastern Pennsylvania Terrorism Task Force (SEPA RTF), the New Jersey Office of Homeland Security and Preparedness (NJ OHSP), the Philadelphia Area Regional Transit Security Work Group (PARTSWG), and the Philadelphia Police Department have proposed to consolidate regional planning efforts and develop a multi-county, four-state, regional intelligence fusion center.

The Delaware Valley Intelligence Center (DVIC) will be an information and intelligence collection, analysis and dissemination facility whose mission will be to support and enhance public safety in the twelve-county, four-state Delaware Valley Region, including Southeastern Pennsylvania, Southern New Jersey, Northern Delaware, and Northeast Maryland. The Center will support and enhance the activities of the numerous investigative and operational bodies currently functioning in these states by enabling them to be more effective and focused in their public safety missions. In addition, the DVRWG has engaged in partnerships with the U.S. Coast Guard's Area Maritime Security Committee (AMSC) for the Ports of Philadelphia, Pennsylvania, Camden, New Jersey, and Wilmington, Delaware.

a. Goals

The goals of the Delaware Valley Intelligence Center are to support Homeland Security and crime prevention efforts in the Delaware Valley Region. The Center will:

- Engage in an all-source, all-crimes, all-hazards approach to information sharing in ground, maritime, aviation, and cyberspace environments;
- Collect, analyze, disseminate real-time intelligence information to the appropriate operational and executive elements;
- Enhance regional coordination and assist in deconfliction efforts;

- Provide the basis for intelligence–led policing and homeland security functionality; and
- Facilitate public/private sector information sharing and coordination.

b. Objectives

The objectives of the Delaware Valley Intelligence Center are to:

- Allow local and state public and private agencies, as well as the federal sector, to better forecast and identify emerging crime and hazard trends;
- Support multi-disciplinary, risk-based problem-solving approaches to proactively address terrorism, crime, and hazard threats;
- Support a community-focused public safety strategy;
- Provide a continuous flow of intelligence and information to assist public safety field operations; and
- Enhance the delivery of emergency and nonemergency services to the public.

c. Proposed Outcomes

The proposed Delaware Valley Intelligence Center (DVIC) will provide the mechanism for regional information sharing, collection, analysis, and dissemination to strategically and tactically support preparedness and response. federal, state, and local public agencies, as well as private businesses have given their support for the fusion center. Core staff of the SEPA RTF has developed a DVIC Charter that provides governance for fusion center operations and administration. A Managing Board, an Executive Advisory Committee and several work groups have been created and SEPA RTF representatives have initiated searches for a facility, training resources, and other assets required for fusion center implementation.

To date, commitments from state-run fusion centers in Pennsylvania, New Jersey, Delaware, and Maryland have been acquired; Memoranda of Agreement (MOA) have been researched to address legal issues among the multi-state county partners. Significant multi-agency organizations, such as the Area Maritime Security Committee

(AMSC) for the U.S. Coast Guard, Sector Delaware Bay, and the Philadelphia Area Regional Transit Security Work Group (PARTSWG) have agreed to partner in planning and funding acquisitions.

The City of Philadelphia has determined that colocating certain city operational functions in the same facility as the DVIC will result in economies of scale and potential advantages in operational coordination. The current concept is to locate the Homeland Security and Criminal Intelligence components of the Philadelphia Police Department within the DVIC envelope. As a separate, but contiguous entity, the present intent is to locate the City's Emergency Operations Center (EOC) at the same facility. The current design concept is that there will be common spaces for meetings; conferences and training that will be shared by the DVIC and the EOC.

Since funding to begin implementation of the DVIC already exists, the current project plan would be to move forward with the DVIC first, and then expand the project to include the EOC as funding sources are identified. After incorporation of EOC implementation into the project, the city may add other related functions that would benefit from being in proximity to the DVIC and EOC.

In an effort to build a model fusion center , this research examines best or smart practices and key components within four state fusion centers, guiding documents for Fusion Center development, the role of leadership, collaboration, protection of civil liberties and civil rights, fusion center critical operating capabilities success stories, as well as the path forward for future fusion centers.

E. HYPOTHESES OR TENTATIVE SOLUTIONS

Developing a model fusion center to enhance information sharing will require the implementation of standards, or the development of a National Homeland Security Fusion Center Doctrine established across the fusion center network to increase effectiveness and efficiency. These standards include: 1) the development of a mission statement to establish fusion center goals and objectives, 2) ensuring adherence with the National Criminal Intelligence Sharing Plan, 3) creating a governance structure that is representative of law enforcement, public safety, and the private sector to enhance

information sharing among all stakeholders at the federal, state, local and private sector levels. 4) Instituting the establishment of appropriate security for facilities, data and personnel through the utilization of existing and emerging technologies, 5) providing training to enhance and ensure fusion center leadership and privacy/civil rights protections, while adopting a philosophy of intelligence-led policing to connect the dots to increase crime and terrorism prevention, 6) build collaborative relationships across all disciplines to address all threat, all crime and all hazards, 7) explore database interoperability to streamline operations and provide the best overall operational picture, and 8) institute Suspicious Activity Reporting to identify prewarning indicators of potential terrorist related activity. It is the assumption of this research that although early fusion centers have developed without formal guidance; the implementation of standard practices and procedures will augment the performance of fusion centers, protect individual privacy, and streamline operations to enhance terrorism and crime prevention.

II. LITERATURE REVIEW

There have been numerous documents written concerning fusion centers, which identify their importance and their potential pitfalls. The categories of the literature include: official documents, guidelines and lesson-learned for intelligence input, civil liberties safeguards and literature dealing with the intelligence cycle and information sharing.

A. OFFICIAL DOCUMENTS RELATING TO FUSION CENTERS

The first category of literature reviewed looks at official documents that discuss the role of fusion centers including, documents written by federal, state and local government committees, government sponsored organizations, including congressional service research reports, as well as guidelines for successful fusion center development. These documents, including such publications as the Council on Foreign Relations, CRS Report on fusion centers describe the value of fusion centers as a mechanism of sharing information to prevent terrorism. The CRS report provides a general understanding of the fusion center concept, the potential drawback of fusion centers, including immaturity issues and the dangers of potential privacy violations, as well as the suggested path forward in fusion center development. The report is general in nature but provides recommendations, including the creation of a national fusion center network to enhance information exchange (Masse, T., O'Neil, S., & Rollin, J, CRS Report: Fusion Center 2007, p. 1).

The CRS report falls short in identifying the means by which to achieve these suggested goals and the measures necessary to minimize the risk to the general public as collection of information may negatively impact civil liberties. The CRS report stresses:

> The value proposition for fusion centers is that by integrating various streams of information and intelligence, including that flowing from the federal government, state, local, and tribal governments, as well as the private sector, a more accurate picture of risks to people, economic infrastructure, and communities can be developed and translated into

> protective action. The ultimate goal of fusion is to prevent manmade (terrorist) attacks and to respond to natural disasters and manmade threats quickly and efficiently should they occur.
>
> (Masse, T., O'Neil, S., & Rollin, J, CRS Report: Fusion Center 2007, p. 1)

The testimony of former Director Robert Riegle, state and Local Program Office, Office of Intelligence and Analysis regarding the Future of Fusion Centers and Potential Promise and Danger is a dissertation of the testimony provided by former Director Riegle before the Committee on Homeland Security, Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment.

This testimony provides the described vision of fusion centers, their necessity and the federal support that will be required for sustainment. The format is easy to follow as it flows from the vision to the necessary components required for future fusion center development. The testimony provided by Mr. Riegle is concise and covers such areas as incorporating diverse multiple disciplines as fusion center partners and provides a template for the future (Riegle, R. 2009 The Future of Fusion Center and Potential Promise and Danger, 2010, p. 1).

Fusion centers (Kaplan, E. 2007, CRS report: Fusion Centers) provides an overview of how fusion centers work, the federal support necessary in pushing information to state and local partners, the value of intelligence-led policing, addressing the all hazard approach, avoiding information overload and protecting civil liberties of individuals who are not suspected of a crime in violation of the Federal Privacy Act of 1974. Kaplan further relates "Experts say putting this information at the fingertips of local law enforcement—who are likelier than federal authorities to come across aspiring terrorists on U.S. soil—transforms police officers from first responders into "first preventers." (Kaplan, E. 2007, CRS report: Fusion Centers)

The Department of Homeland Security, Office of Inspector General's report :DHS' Role in state and local fusion centers is evolving" depicts the importance of information sharing since the terrorist attacks of September 11, 2001, the establishment of fusion centers, creating fusion center guidance and information sharing requirements,

developing a strategy for information sharing within fusion centers, and DHS' role to support fusion center coordination and timely information dissemination. This document further emphasizes the importance of the federal government's willingness to partner with state and local fusion centers and provides guidance and support through the Office of Intelligence and Analysis.

These documents, consisting of Congressional Service Reports, statements of former Director Robert Riegle, state and Local Program Office, Office of Intelligence and Analysis and the Department of Homeland Security, Office of Inspector General report, " DHS' Role in state and local fusion centers provide a brief overview of the importance of fusion centers and their contribution to terrorism prevention. All authors concur that the importance of fusion centers lies in their ability to share information across a broad spectrum of stakeholders. The CRS report and the testimony of former Director Riegle argue that fusion centers are an area for consideration to enhance information sharing. Each document identifies the roles fusion centers play in support of the federal government in terrorism prevention. In addition, each document warns of the necessity of ensuring the protection of civil liberties of the general public.

These reports provided a well-rounded overview of the importance of fusion centers, their development and a description of the roles fusion centers play at the state and local levels to support the overall intelligence community. The information was comprehensive and inspired further research in this area.

B. LITERATURE ON GUIDELINES AND LESSONS-LEARNED FOR INTELLIGENCE INPUT

The second category of literature reviewed provides guidelines and lessons-learned for intelligence input, tasking and dissemination, and information-sharing to stay at the forefront of the fusion center phenomenon. Documents, such as the U.S. Department of Justice (DOJ), U.S. Department of Homeland Security (DHS), and DOJ's Global Justice Information Sharing Initiative, provide best practices or smart practices for the development of a model fusion center to enhance information sharing.

The Fusion Center Guidelines, "*Developing and Sharing Information in a New Era"* provide guidelines for the establishment of fusion centers at the local, state and federal levels. It serves as a roadmap for successful fusion center development and implementation. The Fusion Center Guidelines is insightful in its methodology while remaining specific to the structuring of fusion centers. Recognizing that in 2004 and 2005 many fusion centers were developed with little or no guidance, the Fusion Center Guidelines provide a clear depiction of the fusion process, the role of leadership, fusion center concepts and functions, information flow, and a phased approach integrating law enforcement, public safety and the private sector into a cohesive collaborative environment. It further identifies the necessary requirements and collaborations needed to meet the fusion center's missions and goals and ensure consistency across the country. (Department of Justice, Fusion Center Guidelines 2006, p. 3).

The Fusion Center Baseline Capabilities for state and major urban area fusion centers is a supplemental document to the Fusion Center Guidelines and further identifies the baseline level of capability and standards necessary for fusion centers to perform basic functions. It identifies structures, processes and tools to support the fusion center function of gathering, processing, analysis and dissemination of information. The Fusion Center Baseline Capabilities document provides guidance to ensure fusion centers are established and operated consistently across the country. The Baseline Capabilities document is divided into two sections, Fusion Process Capabilities and Management and Administrative Capabilities.

In addition, the critical operational capabilities for state and major urban area fusion centers, Short-Term Gap Mitigation Strategy Guidebook takes a look at where fusion centers currently are in development. Staying with the idea of standardization, this document identifies current gaps in fusion center development and provides templates to meet fusion center critical operational capabilities. All three documents reviewed appear to reveal a need for consistency or standardized structure among fusion centers, or the creation of a model fusion center.

The literature on fusion center guidelines was comprehensive and provided a roadmap for fusion center development based on standard or best practices to formalize

fusion centers across the fusion center network. Furthermore, a review of testimony provided by Michael C. Mines, Deputy Assistant Director, Directorate of Intelligence, Federal Bureau of Investigation before the House Committee on Homeland Security describes the criticality of fusion centers from an FBI perspective, and the commitment of the Federal Bureau of Investigation to stem the threat of terrorism through collaborative efforts at the federal, state, local and tribal levels of government. This testimony provides valuable insight into the role of the Federal Bureau of Investigation's increasing partnerships with fusion centers throughout the country and the strengthening of the FBI Joint Terrorism Task Forces, the primary investigative agency tasked with terrorism investigation and prevention through information sharing. "Currently, the FBI participates in 36 fusion centers, which is realized through our 56 field intelligence groups (FIGs) that serve as the primary link between the FBI and the fusion center network. To date, a total of 256 FIG personnel are assigned to the 36 fusion centers throughout the United States. Of these, 68 are special agents, 123 are intelligence analysts, and 65 are personnel assigned to other work roles (e.g., language analysts, financial analysts, and investigative support specialists" (Mines, 2007, p.1).

C. LITERATURE ON CIVIL LIBERTIES SAFEGUARDS

The third category of literature reviewed examines civil liberties safeguards, including First Amendment protections, as well as review of civilian committees, such as the American Civil Liberties Union (ACLU) focused on privacy, civil rights and civil liberties protections that bring a watchful eye to fusion center development.

The establishment of privacy and civil rights protection within fusion center development is critical to the mission and future sustainment of fusion centers. A document written by the ACLU entitled "What's Wrong with Fusion Centers" depicts the concern for the collection of information by fusion centers in an era when technology, government powers, and a zest for the war on terrorism is predominant among the fusion center culture.

The document warns of intrusion of the privacy of the general public. It questions and argues the need for fusion centers and emphasizes that information collected about

the American public must be collected lawfully and with utmost care. Specifically, the ACLU emphasizes the need for oversight, as it relates to collaboration between fusion centers, the private sector and the military as these partnerships offer data-mining opportunities that are not traditional law enforcement sources of information. The ACLU document provides oversight and has a ground truth effect in ensuring that the protection of individual privacy is considered with each law enforcement encounter and transaction. The literature also serves as a warning for fusion centers that violate the law and stresses the need for fusion center transparency through independent oversight to remove the perception of excessive secrecy in fusion center operations.

D. LITERATURE ON THE INTELLIGENCE CYCLE AND INFORMATION SHARING ENVIRONMENT

The fourth category of literature reviewed focuses on the intelligence cycle and the information-sharing environment, including the types of systems and mechanisms used by fusion centers to support everyday operations.

Fusion centers appear to be in an excellent position to support law enforcement intelligence missions in post- 9/11 eras as strategies, such as Intelligence Led Policing come to the forefront of modern day policing efforts (David L Carter, 2004, p. 1). A review of the United States Department of Homeland Security Office of Intelligence and Analysis describes fusion centers as;

> The logical touch-points for the Department to access local information and expertise as well as provide them with timely, relevant information and intelligence derived from all-source analysis. The result is a new intelligence discipline and tradecraft that gives us a new, more complete understanding of the threat. The Department provides personnel and tools to the fusion centers to enable the National Fusion Center Network.
>
> (Office of Intelligence and Analysis, 2010, p. 2)

Both documents identify strategies for fusion centers to reach their goals of crime and terrorism prevention. The documents described above provided a step-by-step methodology for the institution of intelligence led policing, describing crime-fighting and terrorism prevention strategies. The information was succinct and complete as Carter

argues that new crime fighting strategies, such as intelligence-led policing will enhance fusion center efficiency and effectiveness in enabling the centers to better identify and forecast criminal behavior.

A review of intelligence sharing systems, currently being utilized by state and local fusion centers, included a 2009 press release written by the United States Department of Homeland Security titled "DHS Announces New Information-Sharing Tool to Help Fusion Centers Combat Terrorism." In 2009, the United States Department of Homeland Security, in conjunction with the U.S. Department of Defense, announced a major initiative to allow fusion centers to share classified terrorism-related information residing in DoD's classified network known as the Secret Internet Protocol Router (SIPRNET) (Department of Homeland Security SIPERNET, 2009). This document, written as a press release, provides a quick overview of this initiative while identifying a vehicle by which DHS can disseminate information to the widespread fusion center community in a timely manner. The document was written to inspire collaboration and commitment of federal resources to support state and local terrorism prevention strategies. In addition, this document argues that information contained in classified DoD databases can, without much heavy lifting, be used by state and local agencies in an effort to fight terrorism.

In addition, a review of the "*Findings and Recommendations of the Suspicious Activity Report (SAR)"* (U.S. Department of Justice 2008, p. 2) list six major findings, including the importance of leading from the top, ensuring privacy protections through formalized privacy policies, utilizing the intelligence cycle to process SAR data, standardized formatting for information sharing, the necessity for providing education to law enforcement tasked with collecting SAR data, and the education of the community regarding the SAR's process, as well as the use of technology to develop information networks.

> The recognized need to advance the sharing of terrorism-related law enforcement information was clearly articulated in the Intelligence Reform and Terrorism Prevention Act of 2004 and in several national-level documents, such as the *National Strategy for Information Sharing* (NSIS), issued to reinforce, prioritize, and unify our nation's efforts to advance the

> sharing of terrorism-related information among federal, state, and local government entities; the private sector; and foreign partners. The primary purpose of this initiative is to identify those behaviors that are reasonably indicative of preoperational planning related to terrorism or other criminal activity and coordinate the sharing of information with the appropriate fusion center and the FBI's Joint Terrorism Task Forces.
>
> (U.S. Department of Justice, 2010, p. 1)

E. SUPPLEMENTARY LITERATURE

Supplementary literature reviewed, such as the Federal Bureau of Investigation's e-guardian system, allows information sharing between fusion centers and the Federal Bureau of Investigation and appears to be as an excellent collaboration tool (Federal Bureau of Investigation, e-guardian system, 2008 p. 1). This document provides an overview of the FBI intelligence collection and dissemination system and was written as an informational bulletin to inspire state and local fusion centers to share information with the FBI. This document, written as an instructive tool, did not focus on the necessity of the integration of other intelligence collection systems such as the Homeland Security Information Sharing Network (HSIN). This DHS information sharing strategy is designed as secure web-based portal to share information across what DHS describes as the community of interest (United States Department of Homeland Security's Information Network, 2008).

A further literature review of additional intelligence collection systems, such as LEO, Law Enforcement Online (Federal Bureau of Investigation, law enforcement online, 1995 p. 1), the United States Department of Homeland Security Shared Space currently being utilized to support the National Suspicious Activity Reporting (SARS Reporting, 2009), and RISS (Regional Information Sharing System, 2007), all describe information collection and sharing strategies from various intelligence agency view points; however, none of these documents, LEO, SARS, or RISS specifically address how or if these systems were collaborative, and if there was any endeavor underway to coordinate these systems into a common portal of information sharing.

The above documents were written as guidelines for imputing information into various intelligence databases. The information presented in these documents was instructional in nature and argued the importance of information sharing across federal, state and local agencies.

A review of the 9/11 Commission Report supports this argument "A breakdown in information sharing was a major factor contributing to the failure to prevent the attacks of September 11, 2001, according to the National Commission on Terrorist Attacks Upon the United States" (9/11 Commission Report, 2002). This document argues that the information was present to prevent a terrorist attack, but the identified failure to share information was evident and the results of this information sharing failure are obvious. The 9/11 Commission Report is a detailed document that depicts the tragedies of September 11, 2001, and the miss steps that led to the attack.

The 9/11 Commission Report provides an insider's view of the historical events. A review of documents, such as the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 (Intelligence Reform Act, 2004), requires that the President prescribe and implement procedures under which federal agencies can share relevant and appropriate homeland security information with other federal agencies and with appropriate state and local personnel, such as law enforcement agencies and first responders (GAO-08-35 Homeland Security Report, 2007, p. 1). These documents, written as Acts, provide a statuary plan passed by congress to support information sharing. These documents also provide guidance and direction at the federal level to extend support to the state and local fusion centers. Written as federal documents, they argue for the need of the establishment of the United States Department of Homeland Security and the need for the collection, analysis, production, and dissemination of intelligence information.

Additionally, literature reviewed, such as "DHS wants Fire Service to Join Fusion Centers" (DHS wants Fire Service to Join Fusion Centers, 2010, p. 1), has identified a new fusion center development with the integration of Fire Services into fusion centers. The document argues that the incorporation of additional emergency services into fusion centers will foster better relationships and increase prevention through comprehensive

multi-discipline reporting. The document serves as an instructional article and provides guidance on Fire Service integration to support multidiscipline information sharing.

A review of the Federal Emergency Management Comprehensive Guide indicates in order for a fusion center to be comprehensive, they must also be focused on all hazards (FEMA, Comprehensive Preparedness Guide (CPG) 502, 2009, p. 1). This document describes the need for fusion center expansion to mitigate all threats. It provides guidance on ensuring public safety through all hazard mitigation. This document argues or suggests the necessity of adding one more step in the fusion center evolution covering new areas of responsibility.

Although, the above mentioned literature provides an overview of where fusion center are in development, it is important to provide a more general understanding of fusion centers. At this time, literature suggests that there is no formalized model that indicates how fusion centers should be structured. Authors have stated that the value added to the development of fusion centers is the comingling of various intelligence sources at the federal, state, and local levels of government, including the private sector to better-forecast possible harm as a result of terrorist, criminal and all hazards events. This assumption in the literature reviewed appears to be the core of fusion center acceptance (T. Massee, S. O'Neil, & J. Rollins, Fusion Center: Issues and Options for Congress, 2007, p. 1).

The above literature reviewed regarding the information sharing environment, provided the researcher with an mosaic image of various opinions, options and concerns regarding current fusion center development, including expanding missions, current silos of information, and possible repeated mistakes that could once again leave us vulnerable to another attack, without some sort of resolution based on structure and coordinated information sharing across all agencies.

F. CONCLUSION

In conclusion, a review of this preliminary literature provided a wealth of information, which was rich in identifying a broad spectrum of opinions and suggestions, while opening up possibilities for discovering further alternative solutions and options.

The literature was comprehensive and established a framework for future research and exploration. Gaps identified in the literature were failures or weaknesses to address individual fusion-center performance measures, or how fusion centers are evaluated, what constitutes a model fusion center, as the literature appears to be more suggestive and fewer directives in nature.

THIS PAGE INTENTIONALLY LEFT BLANK

III. METHODOLOGY

A. PROGRAM EVALUATION METHOD

1. Problem

In order to enhance multidiscipline information sharing at the federal, state and local levels of government, the United States Department of Homeland Security has identified state and local/regional fusion centers as primary points of collection, analysis, and distribution of real-time threat information over the Fusion Center Network. There are currently 72 fusion centers throughout the United States operating at different levels of capability. These centers, created in 2004 and 2005, were initially developed with little guidelines or formalized structure. The U.S. Department of Homeland Security and U.S. Department of Justice have since produced many documents to serve as templates or guidelines to support fusion centers and to develop a cohesive fusion center network. It is uncertain at this time if these strategies are effective or require change in an effort to develop a model fusion center to enhance information sharing.

In order to determine whether this intervention or standardization has the intended result, the Program Evaluation Method will be utilized. This methodology is being utilized because the phenomenon under study is not well-researched, observing actual behavior and conducting comprehensive reviews of literature, existing fusion center documents and guidelines can allow for a more effective study of the issue at hand in a deeper and fuller manner.

A formative evaluation will be conducted based on-site observations and a review of fusion center documents in four fusion centers located in the Northeastern United States. Formative evaluations take place in the natural context. Document reviews and observations in the field are the primary methods of collecting data. Little is done to initiate “control” over the program by design or by statistical manipulation. The case is bounded by the evaluator in terms of time, space, people, and context. Formative evaluations begin with the collection of data, although bias is always a problem in any

form of evaluation, formative evaluators are as neutral as possible before the outset of the evaluation. Conceptual data collection and data analytic methodologies emerge as the study progresses. A balanced portfolio of program strengths and weaknesses and suggestions for improvement are the usual deliverables in a formative evaluation. The purpose is to improve the program by identifying strengths and weaknesses of existing fusion centers, identify the importance or lack of importance of standardization, identify means of effective information sharing and collaboration to enhance the fusion center network and to identify or create synthesis in discovering the required steps or actions to build a model fusion center.

B. BOUNDARIES OF ANALYSIS

The boundaries of this qualitative analysis will focus on the collection of information based on-site observations and review of fusion center documents including, missions statements, standard operating procedures, best or smart practices, privacy policies, utilization of fusion center guidance documents, as well as other available documentation in four fusion centers located in the states of New Jersey, Delaware, Pennsylvania and Maryland. These four centers were chosen due to their geographical locations, size, and to gather a four state perspective on fusion center processes and procedures. They were also chosen to determine if the process of standardization through the implementation of the Department of Homeland Security's Fusion Center Guidelines is supporting daily fusion center operations, as well as strengthening the fusion center network.

In addition, the information acquired during this process will be utilize by the author's home agency, the Philadelphia Police Department, to support the development of a future fusion center located in the Delaware Valley Region, whose mission will be to support the above mentioned four state fusion centers from a regional area of operations.

C. ON-SITE OBSERVATIONS AND QUALITATIVE DATA ANALYSIS

Sampling strategies during fusion center site visits include on-site observations, and document review. The purpose for utilizing the types of data collected will include,

identifying the strengths and weakness of fusion center standardization, including the means of effective information sharing and collaboration to enhance the fusion center network. Identify or create synthesis in discovering the required steps or actions to build a model fusion center, as well as exploring the importance of leadership, relationship building and training to enhance effectiveness, while reducing liabilities. It is intended that the information captured during this evaluation will assist in the development of series of themes directed to identify the positive and negative assumptions of fusion center standardization, collaborative capacity, leadership, training, as well as a reduction in liability. An example argument for standardization may include confirmatory themes, such as standardization reduces confusion while improving operation consistency.

In addition, to support this analysis, the employment of a Force Field Analysis will be utilized to identify strengths and weaknesses, or the pros and cons of fusion center operations, as well as identifying the driving forces that are positive for change and the restraining forces that create obstacles for change within current fusion center operations and future fusion center development. By employing the Program Evaluation Method, it is possible to identify and capture real-world nuisances during on-site observations that would not have been possible utilizing alternative research methods such as a survey methodology. Based on the above-mentioned process and the identification of concurring themes, a detailed analysis will be produced to either support or refute assumptions regarding the requirement to develop a formalized fusion center doctrine, as well as identifying the necessary components required to build a model fusion center that will operate both efficiently and effectively in the prevention and management of all crime, all threat and all hazard information.

D. RESEARCH LIMITATIONS

Although, the research methodology employed in this thesis examines the current guidelines necessary for fusion center development, its scope is limited based on the evaluation of four chosen fusion centers and does not evaluate or take into account the operational capabilities of the remaining fusion centers, although also extremely capable they were not considered in this thesis.

In order to gain a better understanding of overall fusion center operations, this research begins by examining current fusion center guidance or core principles described as the Fusion Center Guidelines and Baseline Capabilities. These documents serve as fusion center doctrine and provide the necessary components or foundation to build a model fusion center**.**

IV. AN ANALYSIS OF THE FUSION PROCESS, HOW IS IT WORKING?

Chapter IV examines several core principles of fusion center development, including guiding documents such as ”Fusion Center Guidelines” and “Baseline Capabilities.” In addition, this chapter further explores the protection of civil rights and civil liberties critical to fusion center operations, including the establishment and benefits of a formalized privacy policy to support the collection process during suspicious activity reporting. The chapter concludes by providing an overview of the fusion center critical operational capabilities, the intelligence-led policing model used to connect the dots, and the components necessary to achieve an award winning fusion center, as well as analyzing the capabilities four fusion centers in the Northeastern United States in comparison with the identified Fusion Center Guidelines.

A. REVIEW OF FEDERAL GUIDANCE

1. Fusion Center Guidelines

The *Fusion Center Guidelines, Developing and Sharing Information in a New Era* provides guidelines for the establishment of fusion centers at the federal, state, local and tribal levels of government (U.S. Department of Homeland Security, U.S. Department of Justice, 2006 p 1). This document serves as a roadmap for successful fusion center development and implementation. Although, fusion centers have developed at various stages throughout the years, Fusion Center Guidelines propose guidance to support concurrent development, although these guidelines are not statutory in nature, they prove valuable in establishing core principals for fusion center development.

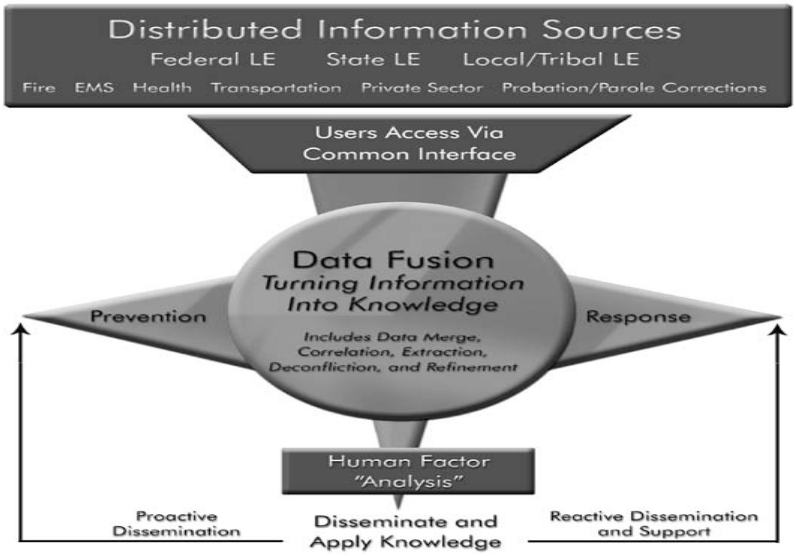

Figure 3. Fusion Process

The U.S. Department of Homeland Security and U.S. Department of Justice, as well as the Federal Bureau of Investigation along with the Global Information Sharing Initiative, have partnered to support fusion development.

> DHS and DOJ have collaborated to provide guidance and technical assistance to fusion centers, and along with the PM-ISE, have sponsored regional and national conferences, in part to determine the needs of fusion centers. For example, DHS and DOJ jointly issued their most recent Fusion Center Guidelines in August 2006 that outlines 18 recommended elements for establishing and operating fusion centers. The guidelines were intended as a way to ensure state and local fusion centers could be established and operated consistently and were developed to help fusion center administrators create policies, manage resources, and evaluate fusion center services.
>
> (GAO-08-35, 2007, p 36)

Divided into 18 critical components, the Fusion Center Guidelines begin with a clear concise definition or description of fusion centers, and then expand into the core competencies or recommendations to support Fusion development. Among other areas for consideration, these guidelines include adhering to the National Criminal Intelligence Sharing Plan, developing a clear and concise mission statement, establishing a representative governance structure, utilizing Memorandums of Understanding, creating a

collaborative environment, leveraging existing systems, as well as developing privacy and civil liberties policies and protections. Although the Fusion Center Guidelines provide a comprehensive list of suggested measures to support fusion center development, this thesis focuses on four core principles for evaluation based on their criticality to fusion center operations. The four areas listed below appear to be the basic building blocks or founding principles for fusion center development and operations, as well as ensuring the protection of individual rights and freedoms.

a. Guideline 2 Develop and Embrace a Mission Statement and Identify Goals

Mission Statements provide direction and establish goals and objectives that are based on clear and concise fusion center requirements.

> A mission statement is a written statement of the organization's purpose, such as enhancing public safety, sharing information, or resolving criminal investigations. It is important to have a mission statement because it focuses efforts and is the foundation of all the decisions that follow..
>
> (U.S. Department of Justice, U.S. Department of Homeland Security 2006, p. 23)

b. Guideline 4 Create a Collaborative Environment for Sharing of Intelligence and Information

Fusion centers provide collaborative space for multiagency integration; however, true collaboration begins with the willingness and acceptance of individuals to engage in accomplishing a common mission.

> To maximize intelligence sharing, all levels of law enforcement and public safety agencies and the private sector must communicate and collaborate. The objective is to leverage resources and expertise while improving the ability to detect, prevent, and apprehend terrorists and other criminals.
>
> (U.S. Department of Justice, U.S. Department of Homeland Security, 2006, p 29)

c. Guideline 6 Leverage the Databases, Systems, and Networks

Leveraging existing databases reduces cost and provides immediate communication. “Centers may want to evaluate the types of databases that participating agencies have available. Gaps should be identified and researched. Leveraging the databases and systems available via participating entities will help maximize information sharing.” (U.S. Department of Justice, U.S. Department of Homeland Security 2006, p. 33)

d. Guideline 8 Privacy and Civil Liberties Policy

“Develop, publish, and adhere to a privacy and civil liberties policy” (U.S. Department of Justice, U.S. Department of Homeland Security 2006, p.41).

Fusion centers focused on Terrorism and Crime prevention must ensure the protection of individual Civil Rights and Civil Liberties. Although, investigating terrorism can become clouded, investigations should be based on a criminal predicate and not on an individual’s race, religion, or national origin.

> The National Criminal Intelligence Sharing Plan (NCISP) stresses the need to ensure that constitutional rights, civil liberties, civil rights, and privacy are protected throughout the intelligence process. In order to balance law enforcement’s ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be in place.
>
> (U.S. Department of Homeland Security, U.S. Department of Justice, 2008, p. 65)

The Fusion Center Guidelines provide an overview of the core competencies necessary for fusion center development. These guidelines serve as the building blocks, and provide clear direction for building a model fusion center and are not intended as federal mandates, nor do they represent any statuary requirements.

B. BASELINE CAPABILITIES FOR STATE AND MAJOR URBAN AREA FUSION CENTERS

The Fusion Center Baseline Capabilities for state and major urban area fusion centers is a supplemental document to the Fusion Center Guidelines and further identifies the baseline level of capability and standards necessary for fusion centers to perform basic functions. It identifies structures, processes and tools to support the fusion center function of gathering, processing, analysis and dissemination of information. The Fusion Center Baseline Capabilities document provides guidance to ensure fusion centers are established and operated consistently across the country. The Baseline Capabilities document is divided into two sections, Fusion Process Capabilities and Management and Administrative Capabilities.

Figure 4. Fusion Process Capabilities

By achieving this baseline level of capability, a fusion center will have the necessary structures, processes, and tools in place to support the gathering, processing, analysis, and dissemination of terrorism, homeland security, and law enforcement information. This baseline level of capability will support specific operational capabilities, such as Suspicious Activity Reporting (SAR); Alerts, Warnings, and Notifications; Risk Assessments; and Situational Awareness Reporting. The development of baseline operational standards is called for in the National Strategy for Information Sharing (Strategy) and is a key step to reaching one of the Strategy's goals: "Establishing a National Integrated Network of State and Major Urban Area Fusion Centers." Defining these operational standards allows federal, state, local, and tribal officials to identify and plan for the resources needed—to include financial, technical assistance, and human support—to achieve the Strategy's goal.

(U.S. Department of Homeland Security, U.S. Department of Justice, 2008, p. 1)

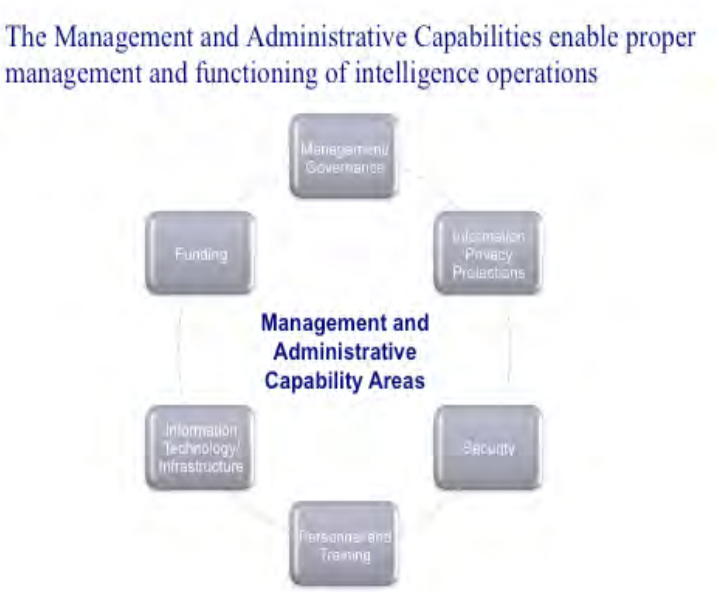

Figure 5. Management and Administrative Capabilities (From Director Steven Hewitt, Tennessee Fusion Center)

In addition, the Baseline Capabilities for state and major urban area fusion centers introduces the importance of ensuring the protection of civil liberties and civil rights of individuals, as well as incorporating fusion centers into the Information Sharing Environment.

> To support this requirement, the ISE PGC, which is made up of ISE Privacy Officials from the federal agencies participating in the ISE, formed a working group to examine the privacy issues relative to state, local, and tribal entities, including fusion centers, interfacing with the ISE. The PGC State/Local/Tribal Working Group (SLT WG) began with the existing guidance found in the Fusion Center Guidelines, specifically Guideline 8, "Develop, publish, and adhere to a privacy and civil liberties policy," and performed a gap analysis to identify where the guidance to the fusion centers did not include the requirements of the ISE Privacy Guidelines. While some of the concepts and requirements of the ISE Privacy Guidelines are referenced in Guideline 8, noteworthy gaps were identified, in part because protected information shared in the ISE is given enhanced privacy and civil liberties protection under the ISE Privacy Guidelines. In order to provide the most comprehensive guidance, the gap analysis compares Guideline 8, the ISE Privacy Guidelines, and 28 Code of Federal Regulations (CFR) Part 23, since all address privacy concerns and are relevant to the fusion centers.
>
> (U.S. Department of Homeland Security, U.S. Department of Justice, 2008, p. 6)

C. PROTECTING PRIVACY, CIVIL LIBERTIES, AND CIVIL RIGHTS

"Benjamin Franklin is said to have observed, "Those who would give up ESSENTIAL LIBERTY to purchase a little TEMPORARY SAFETY, deserve neither LIBERTY nor SAFETY" (U.S. Department Justice, Office of Justice Programs, Privacy and Civil Liberties, 2010, p. 1).

The establishment of privacy and civil rights protections within fusion center development is critical to the mission and future sustainment of fusion centers. A document written by the ACLU entitled "What's Wrong with Fusion Centers" depicts the concern for the collection of information by fusion centers in an era when technology, government powers and a zest for the war on terrorism is predominant among the fusion center culture. In addition, to ensure transparency, fusion centers may be subject to out-

side audits or independent oversight. Public trust is an essential element of fusion center operations. Fusion centers must avoid what is known as the "*One Way Mirror*."

> Even as fusion centers are positioned to learn more and more about the American public, authorities are moving to ensure that the public knows less and less about fusion centers. In particular, there appears to be an effort by the federal government to coerce states into exempting their fusion centers from state open government laws.
>
> (German, 2008, p. 7)

Protecting privacy and civil liberties, as well as ensuring public trust is paramount within fusion center operations.

> In accordance with Section 1016 of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), as amended, the ISE is a conceptual framework composed of the policies, procedures, and technologies linking the resources (people, systems, databases, and information) of state, local, and tribal (SLT) agencies; federal agencies; and the private sector to facilitate terrorism-related information sharing, access, and collaboration. Consistent with Presidential Guideline 5, the U.S. Attorney General, the U.S. Department of Justice (DOJ), and the Director of National Intelligence (DNI)—in coordination with the Program Manager for the ISE (PM-ISE) and the heads of federal departments and agencies that possess or use intelligence or other terrorism-related information—developed privacy guidelines for the ISE, titled Guidelines to Ensure That the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment (ISE Privacy Guidelines). The ISE Privacy Guidelines describe the means by which federal departments and agencies participating in the ISE will protect privacy and civil liberties in the development and operation of the ISE.
>
> (U.S. Department of Homeland Security and U.S. Department of Justice, 2010 p. 3)

Transparency and communication to the public and other stakeholders regarding the establishment of privacy policies is paramount to ensure public acceptance of fusion centers throughout the country. Fusion Centers must strike a balance between individual rights and freedoms while seeking potential clues of pre-indicators of terrorism. These clues potentially developed during such activities, such as Suspicious Activity Reporting

(SAR), must be collected lawfully recognizing the requirement to protect constitutional freedoms. Violation of privacy may occur through the use of Personally Identifiable Information (PII) when there is no nexus too criminal or terrorism related behavior.

1. Benefits of a Privacy Policy

There are many benefits of a well-established privacy policy, which serves as the corner stone of public protection. Public trust is fundamental in ensuring public acceptance and support of the Fusion Center Network. Public confidence is quickly lost during any indication of any unjust violation of individual freedoms. “A strong privacy policy is good public policy, because it is responsive to widely held public expectations about the collection and use of information about individuals and the fair and open operation of a democratic government. A well-developed privacy policy protects the center, external agencies that access and share information with the center, and their employees from liability under lawsuits and civil rights and civil liberties complaints; protects the public and promotes public trust in information sharing. A comprehensive policy that is properly enforced will also result in more effective and efficient use of public resources” (U.S. Department of Homeland Security and U.S. Department of Justice, 2010, p. 2)

D. SUSPICIOUS ACTIVITY REPORTING (SAR)

“Whether a plan for a terrorist attack is homegrown or originates overseas, important knowledge that may forewarn of a future attack may be derived from information gathered by state, local, and tribal government personnel in the course of routine law enforcement and other activities.”(National Strategy for Information Sharing, 2007, p. 1)

Fusion centers are tasked with the collection, analysis, and dissemination of information to support crime and terrorism prevention, although fusion centers receive information from various sources including, the public, and the private sector, as well as various public safety disciplines, law enforcement plays an essential role in public protection.

> Local law enforcement agencies are critical to efforts to protect our local communities from another terrorist attack. Fundamental to local efforts to detect and mitigate potential terrorist threats is ensuring that frontline personnel are trained to recognize and document behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Daily, there are more than 17,000 local law enforcement agencies in the United States that document information regarding suspicious behavior, including that related to terrorism. The ISE-SAR functional standard defines a Suspicious Activity Report (SAR) as "Official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.
>
> (U.S. Department of Justice, 2008, p. 5)

Although, Suspicious Activity Reporting (SAR) is essential in preventing terrorist related activity, all information must be collected lawfully, contain a criminal predicate, or other information specifically related to potential terrorist activity. Information collected in an unlawful manner undermines the entire fabric of the fusion center network. Proper information management can only be achieved through effective leadership and continual training. As fusion centers develop, they will be the responsible entity for analyzing these SAR reports from 18,000 law enforcement agencies, as well as information collected from the public and private sector.

E. CRITICAL OPERATIONAL CAPABILITIES (COCS)

As fusion centers mature, other areas for improvement emerge becoming necessary components for fusion center growth and sustainment. During the 2010 National Fusion Center Conference, Fusion Center Directors, in partnership with the federal government, distilled the Baseline Capabilities for state and major urban area fusion centers into National Network priorities, including four Critical Operational Capabilities (COCs).

- Receive: Ability to receive classified and unclassified information from federal partners.

- Analyze: Ability to assess local implications of that threat information through the use of a formal risk assessment process.
- Disseminate: Ability to further disseminate that threat information to other state, local, tribal, territorial and private sector entities within their jurisdiction.
- Gather: Ability to gather locally-generated information, aggregate it, analyze it, and share it with federal partners as appropriate.

Strengthening the ability of fusion centers to execute the COCs and ensure P/CRCL protections is critical to building an integrated National Network of Fusion Centers capable of sharing information with the federal government and SLTT partners during situations involving time-sensitive and emerging threats (U.S. Department of Homeland Security, National Network of Fusion Center Fact Sheet, 2010, p. 1).

F. INTELLIGENCE-LED POLICING

Fusion centers throughout the country appear to be moving toward an intelligence led-policing model to support crime and terrorism related investigations.

> The IACP National Law Enforcement Policy Center defines criminal intelligence as "information compiled, analyzed and/or disseminated in an effort to anticipate, prevent or monitor criminal activity." It may be "strategic" (provide general guidance on emerging patterns and trends) or "tactical" (focused on a specific criminal event). Information is not the same thing as "intelligence." Rather, intelligence is the combination of credible information with quality analysis. Intelligence-led policing defines intelligence by stressing that intelligence is "a guide to operations, rather than the reverse.
>
> (International Association of Chiefs of Police: Criminal Intelligence Sharing, 2007, p. 12).

G. AWARD WINNING FUSION CENTERS: WHAT IS REQUIRED?

As fusion centers mature, they are recognized for outstanding achievements in various areas of fusion center operations, such as fostering collaboration, providing

leadership, as well as meeting milestones that support the overall fusion center network. This recognition serves to motivate fusion center leaders to develop centers of excellence, but more importantly to enhance information sharing and cooperation at the federal, state, local and tribal levels of government. At the 2010 Nation Fusion Center Conference, several fusion centers were recognized for their outstanding achievements.

Award winners included:

- Fusion Center of the Year–The Colorado Information and Analysis Center (CIAC) was recognized for exemplifying every aspect of a robust and mature fusion center. CIAC leadership has been a strong advocate of fusion centers, organizing and supporting the national build-out of the network. They were specifically recognized for their recent support to the Najibullah Zazi terrorism investigation as well as their leadership during the 2008 National Democratic Convention.
- Fusion Center Federal Representative of the Year–FBI agent, Leslie Gardner, assigned to the Los Angeles Joint Regional Intelligence Center (JRIC), was nominated for her leadership in developing the JRIC into a nationally recognized model of cooperation and collaboration between agencies of all sizes and missions. She has been responsible for initiating policies, processes, and programs, which exceeded expectations and drove standards across the national network of fusion centers.
- State/Local Fusion Center Representative of the Year–Mike Sena, Deputy Director, Northern California Regional Intelligence Center (NCRIC), was recognized for his leadership and management of the NCRIC's growth and maturation. Under his leadership, the fusion center has expanded its all-crimes/all-hazards mission by providing superior customer service and expanding its partnerships across all levels of government.
- In addition, the 12 pilot sites for the Nationwide Suspicious Activity Reporting (SAR) Initiative were recognized for their support to the country's homeland security mission. These sites included police

departments in Boston, Chicago, Houston, Las Vegas, Los Angeles, Miami-Dade and Washington; Arizona Department of Public Safety (Arizona Counterterrorism Information Center), Florida Department of Law Enforcement, New York State Intelligence Center, Seattle Police Department/Washington State Fusion Center, and the Virginia Fusion Center.

The above information provides a sense of what constitutes a successful fusion center, although there are many other attributes required for success, it is valuable to understand the recognized matrix for success in the development of a model Fusion Center. Leadership, as noted above, whether individually or collectively, appears to be a driving force in the success of the recognized fusion centers. By understanding and recognizing achievements, developing fusion centers can set the bar to ensure motivation, a concept that is not written in any guidance and which often goes unrecognized as a driving force to reach identified milestones.

H. FUSION CENTER REVIEW OF ON-SITE OBSERVATIONS AND QUALITATIVE DATA ANALYSIS

As part of the Program Evaluation Method and Formative Analysis, as well as to gain a deeper understanding of fusion center operations, on-site observations were conducted in four fusion centers located in the Northeastern United States. Formative evaluations take place in the neutral context. Document reviews and observations in the field are the primary methods of collecting data. The purpose for utilizing the types of data collected will include, identifying the strengths and weakness of fusion centers in correlation with the four identified Fusion Center Guidelines, including establishing clear goals and direction through the incorporation of a mission statement, creation of a collaborative environment to share information, the ability to leverage existing databases for information exchange, and protecting privacy and civil liberties through established privacy policies.

It is intended that the information captured during this evaluation will assist in the development of series of themes directed to identify the positive and negative

assumptions of fusion center guidelines, and if they are being utilized efficiently and effectively in developing a fusion centers. An analysis of data collected and on-site observations will then be used to provide recommendations to identify smart or best practices in identifying the necessary components to develop a model fusion center.

In addition, to support this analysis, the employment of a Force Field Analysis will be utilized to identify strengths and weaknesses, or the pros and cons of fusion center operations, as well as identifying the driving forces that are positive for change and the restraining forces that create obstacles for change within current fusion center operations and future fusion center development. By employing the Program Evaluation Method, it is possible to identify and capture real-world nuisances during on-site observations that would not have been possible utilizing alternative research methods such as a survey methodology.

1. The New Jersey Regional Operations Intelligence Center (ROIC)

The New Jersey Regional Operations Intelligence Center (ROIC) pronounced Rock was established in 2006 within the agency of the New Jersey State Police. The ROIC is an all crimes, all hazards and all threats fusion center. The New Jersey ROIC consists of three main components:

- Watch Operations Unit
- Analysis Unit
- Strategic Outreach Unit

The ROIC is a 24-hour a day, seven day a week all-crimes, all-hazards, all-threats, watch command and analysis center. The New Jersey State Police is the executive agency of ROIC and administers the general personnel, policy, and management functions. The center's mission is to collect, analyze, and disseminate intelligence to participating law enforcement entities; evaluate intelligence for reliability and validity; provide intelligence support to tactical and strategic planning; evaluate intelligence in the Statewide Intelligence Management System; and disseminate terrorism-related activity and information to the FBI, among others.

The ROIC is also the home of the State Emergency Operations Center, the State Office of Emergency Management, and the State Police Emergency Management Section Offices. The ROIC has personnel assigned (including 13 analysts) from the FBI, DHS, ATF, ICE, FAMS, and the U.S. Coast Guard, in addition to personnel from the State Police, New Jersey Office of Homeland Security and Preparedness, and the Department of Transportation.

The ROIC is seeking representation from the departments of Corrections, Parole, Health and Senior Services; Environmental Protection; and Military and Veteran Affairs. The ROIC is overseen by a Governance Committee, chaired by the director of ROIC, which consists of representatives from state and federal entities and law enforcement associations who meet quarterly to discuss ROIC policies and other related matters. In addition, the ROIC is seeking to develop additional relationships with private sector organizations—such as the American Society of Industrial Security, the Princeton Area Security Group, the Bankers and Brokers Group, and the All Hazards Consortium—to further the mission of the intelligence analysis element of ROIC. The ROIC consists of three components: (1) an analysis component, responsible for collecting, analyzing, and disseminating intelligence information entered into the Statewide Intelligence Management System by local, county, state, and federal law enforcement; (2) the operations component, which will control the actions of State Police operational and support personnel and serve as a liaison to federal agencies, other state entities, and county or municipal agencies on operational matters; and (3) a call center component, which will provide the center with situational awareness intelligence about emergency situations. DHS and DOJ systems and networks to which the ROIC has access include LEO, HSIN, HSIN-Secret, and ACS, as well as SIPRNet.

The ROIC disseminates officer safety information, bulletins, and any other information deemed to be of value to the law enforcement or homeland security community. The State Police provide operational support to the law enforcement community on canine support for bomb and drug detection, bomb technicians, medevac

helicopter support, and Marine services (GAO-08-35, Federal Efforts Are Helping to Alleviate Some Challenges Encountered by state and Local Information Fusion Centers, 2007, pp. 87–88).

a. Watch Operations Unit

The Watch Operations Unit serves as the alert or warning section and operates on a 24/7 basis. The Watch Operations Unit "conducts rapid analysis of violent crime, terrorist activity, and emergent incidents (both natural and man-made) to provide real time situational awareness of both regional and statewide law enforcement activities. It organizes, coordinates, and initiates the deployment phase of all New Jersey State Police operational assets and utilizes both open and closed intelligence resources to provide tactical intelligence for the purpose of investigational support (Regional Operations Intelligence Center, 2006, p. 1).

b. Analysis Unit

The process of analysis is utilized in turning information into actionable intelligence and serves as the cornerstone of all fusion center operations and also supports the development of tactical and strategic decisions. Described as part of the fusion process, "the concept of fusion has emerged as a fundamental process to facilitate the sharing of homeland security-related and crime information and intelligence." (U.S Department of Homeland Security, Department of Justice, 2006, p. 2)

The Analysis Unit–

> Influences the decision making process, guides the allocation of federal, state and local resources, and aids in the investigative process through the use of supportive threat and crime analysis, examines and evaluates homeland security and counter terror threat streams specific to the state of New Jersey and surrounding regions, produces risk and threat assessments based upon the current threat environment in relation to regional infrastructure vulnerabilities, examines and interprets statistical data and trends to provide insight into the current criminal environment and produces timely intelligence in an effort to enhance the decision making process as it relates to preventing, detecting and suppressing criminal activity.
>
> (Regional Operations Intelligence Center, 2006, p. 2)

c. Strategic Outreach Unit

Effective communication and collaboration across federal, state, local, tribal and the private sector are paramount for the efficient and effective operations of fusion centers. “To maximize intelligence sharing, all levels of law enforcement and public safety agencies and the private sector must communicate and collaborate. The objective is to leverage resources and expertise, while improving the ability to detect, prevent, and apprehend terrorists and other criminals. Fostering a collaborative environment builds trust among participating entities, strengthens partnerships, and provides individual, as well as a collective ownership in missions and goals of the center” (Department of Justice, Fusion Center Guidelines 2006, p. 29).

New Jersey Regional Operations Intelligence Center through their Strategic Outreach Unit “promotes ongoing dialogue and timely communication between members of the law enforcement community and private sector, enhances private sector security through the sharing of threat and crime analysis, and increases the statewide intelligence network through inclusion of the private sector, thereby promoting enhanced threat detection and crime suppression” (Regional Operations Intelligence Center, 2006 p. 3). In addition to ensure operational efficiency and compliance, the New Jersey Regional Operations Center has instituted the Office of Baseline Capabilities. This new office ensures overall operational compliance in accordance with U.S. Department of Justice Fusion Center requirements, as well as providing oversight to support the institution of the Critical Operating Capabilities and formalized privacy policies.

d. New Jersey Office of Emergency Management

In addition, the New Jersey Office of Emergency Management (NJ OEM) is also located within the New Jersey Regional Operations Intelligence Center. Tasked with all hazard mitigation the NJ Office of Emergency Management supports the New Jersey Regional Operations Intelligence Center operations.

> The NJ OEM is the lead state agency responsible for preparedness, mitigation, response, and recovery efforts related to all natural and man-made disasters within the state of New Jersey, incorporates traditional and

> modern law enforcement techniques, practices, and procedures into the emergency management environment via an all hazards approach designed to protect life and preserve property.
>
> (Regional Operations Intelligence Center, 2006, p. 4)

e. Mission Statement

All efforts begin with the identification of the mission; a mission statement is the foundation for present and future actions and decisions. A mission statement serves as a navigational instrument providing clear and concise direction.

> A mission statement is a written statement of the organization's purpose, such as enhancing public safety, sharing information, or resolving criminal investigations. It is important to have a mission statement because it focuses efforts and is the foundation of all the decisions that follow. A mission statement can also inspire people in the organization and inform customers of the benefits and advantages of what the organization offers and is the first step in educating entities about the center and its services.
>
> (Department of Justice Fusion Center Guidelines, p. 23).

Understanding the mission is critical to fusion center operations; although missions may vary to serve individual operational needs, they must be interwoven through the roles of the center.

> The mission of the New Jersey Regional Operations Intelligence Center (NJ ROIC) is to interface with the New Jersey law enforcement community, and other law enforcement and homeland security agencies, by being a primary point of contact for collection, evaluation, analysis, and dissemination of intelligence data and criminal background information in a timely and effective manner in order to detect and/or prevent criminal or terrorist activity, and to solve crimes. This mission shall remain consistent with the National Criminal Intelligence Sharing Plan.
>
> (New Jersey Regional Operations Intelligence Center Privacy Policy, 2010, p. 1.)

Colonel Rick Funetes, New Jersey State Police Superintendent and NJOEM Director, related when interviewed by the New Jersey Office of Emergency Management that,

> In its short existence, the fusion center has allowed us to better execute decisions and plans based on the productive flow of information both internally and externally. This flow has allowed us to deploy resources in a timelier manner than in the past. As we all know, when protecting lives, time is always of the essence. Colonel Funetes describe four areas of concern including the need to effectively manage technology, ensure analytical growth, the need for the implementation of a call center and the necessity to increase catastrophic planning. In conclusion Colonel Funetes describe Good people as the cornerstone of the ROIC.
>
> (Office of Emergency Management, 2008, p. 1)

f. Privacy Policy

Developing a Model Fusion Center will require the development and implementation of a formal written privacy policy to ensure the protection of individual civil rights and civil liberties. Fusion Center Privacy Policies must also remain transparent to ensure public trust. It is also important to ensure that all fusion center personnel are aware of privacy requirements, as well as ensuring accountability as described below in brief overview the privacy policy instituted by the NJ ROIC.

"The purpose (goal) of the NJ ROIC Privacy Policy is to ensure protection of the privacy, civil rights, and civil liberties of individuals and organizations. The goal of establishing and maintaining the NJ ROIC is to further the following purposes:

- Be an active participant in the Information Sharing Environment.
- Increase public safety and security in the state of New Jersey, the region and to contribute to the security of the nation.
- Mitigate or minimize the threat and risk of injury to all members of the public safety and health care communities.

- Mitigate or minimize the threat and risk of damage to real or personal property.
- Protect the individual privacy rights, civil rights or other protected interests a person or persons may have.
- Protect the integrity of the criminal investigative, criminal intelligence, and justice system processes and information.
- Foster relationships with persons or groups of people in an effort to promote cooperation between law enforcement and the community, which it serves.
- Make the most effective use of public safety resources."

g. Policy Applicability and Legal Compliance

The NJ ROIC personnel, including enlisted personnel, sworn participating agency personnel, civilian New Jersey State Police (NJSP) and participating agency personnel will comply with the privacy policy of the NJ ROIC. This policy shall apply to any information that the NJ ROIC collects, receives, maintains, archives, accesses, or discloses among its personnel, other government agencies (including Regional Intelligence Sharing Systems [RISS] and Information Sharing Environment [ISE] agencies), and partner criminal justice and public safety agencies, as well as quasi-government entities, private contractors, and the general public. The NJ ROIC will provide a printed copy of this policy to all enlisted, civilian and partner agency personnel, as well as contractors who provide services and will require both a written acknowledgment of receipt of this policy and a written agreement to comply with this policy and all the provisions contained herein. All New Jersey Regional Operations Intelligence Center (NJ ROIC) personnel, sworn participating agency personnel, civilian and participating agency personnel who provide information technology services to the NJ ROIC, the New Jersey State Police or any participating agency, private contractors and other authorized partners or users will comply with all applicable state and federal laws concerning the protection of privacy, civil rights, and civil liberties.

The NJ ROIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including applicable state and federal privacy, civil rights, and

> civil liberty laws. It is the policy of the NJ ROIC to ensure that all personnel assigned to the NJ ROIC strictly adhere to any rule, regulation, guideline, or mandate, with regard to the use or dissemination of any information or intelligence. It is not the intention of the NJ ROIC administrators to create rules or regulations that exceed any pre-existing rules or regulations, but to expect compliance with those standards already in place. As the NJ ROIC is an entity within the New Jersey State Police, a Division within the Department of Law and Public Safety, all applicable policies of the Department will be adhered to by the NJ ROIC. Violations of this privacy policy by employees of the NJSP, enlisted and civilian, shall be disciplined in accordance with administrative procedures available to the Superintendent of the State Police. Outside agency personnel assigned to the NJ ROIC are subject to removal from assignment to the NJ ROIC by the Task Force Commander and shall be referred to their host agency for appropriate action. Participating agencies and individual users are subject to the enforcement procedures and sanctions provided in Accountability and Enforcement.
>
> (New Jersey Regional Operations Intelligence Center Privacy Policy, 2010, p. 1.)

h. Governance and Oversight

Effective governance provides stability within fusion centers and offers a sounding board for decision makers.

> Primary responsibility for the operation of the NJ ROIC, its justice systems, operations, coordination of personnel; the receiving, seeking retention, evaluation information quality, analysis, destruction, sharing or disclosure of information; and the enforcement of this policy is assigned to the Task Force Commander of the NJ ROIC. The NJ ROIC is guided by a center-designated and trained Privacy Officer who liaises with community privacy advocacy groups to ensure that privacy, civil rights, and civil liberties are protected within the provisions of this policy and within the center's information, collection, retention and dissemination processes, and procedures. The Operations Officer is designated as the Privacy Officer.
>
> (New Jersey Regional Operations Intelligence Center Privacy Policy, 2010, p. 3)

i. Information

The proper collection and management of information is critical to the sustainability of fusion centers. Information must be collected properly and within the confines of the law "The role of the NJ ROIC is linked closely with the Intelligence-Led Policing (ILP) initiative undertaken by the New Jersey State Police. Specifically, ILP is a collaborative philosophy based on improved intelligence operations to aid in understanding the changes in the operating environment to enable law enforcement to rapidly adjust to new circumstances. In its most efficient state, ILP requires police officers and investigators to become better data collectors and better consumers of intelligence related products.

The NJ ROIC will seek and retain information and/or intelligence that:

- Is based upon a criminal predicate or threat to public safety; or
- Is based upon reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or is planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, the state of New Jersey, the region, or the nation, and the information is relevant to the criminal (including terrorist) conduct or activity; or
- Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents; the resulting justice system response; the enforcement of sanctions, orders or sentences; or the prevention of crime; or
- Is useful in a crime analysis or in the administration of criminal justice and public safety; and the source of the information is reliable and verifiable or limitations on the quality of the information are identified; and the information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate (New Jersey Regional Operations Intelligence Center Privacy Policy, 2010, p. 4).

j. Tips and Leads and Suspicious Activity Reports

The utilization of Suspicious Activity Reports (SAR) by fusion centers provides a mechanism for information collection across many disciplines, as well as the private sector. The NJ ROIC will also retain and share suspect information that does not reach the level of reasonable suspicion such as tips and leads or suspicious activity reports (SAR).

k. Acquiring and Receiving Information

The Code of Federal Regulations 28, part 23 mandates federal statuary requirements for any agency receiving federal funding.

> Information-gathering (acquisition), and access and investigative techniques used by the NJ ROIC and information-originating agencies, will remain in compliance with and will adhere to applicable laws and guidance, including, but not limited to: 28 CFR Part 23 regarding criminal intelligence information. The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy). Criminal intelligence guidelines established under the U.S. Department of Justice's (DOJ) National Criminal Intelligence Sharing Plan (NCISP). Constitutional provisions; New Jersey statutes; Attorney General Guidelines; and administrative rules, as well as regulations and policies that apply to multi-jurisdictional criminal intelligence information data bases. Information-gathering and investigative techniques used by the NJ ROIC will, and those used by originating agencies should, be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.
>
> (National Fusion Center Association, 2010, p. 10)

l. Analysis

The New Jersey Regional Operations Center is a highly professional organization tasked with preventing crimes, terrorism and all hazards within the state of New Jersey. At the core of the centers, success is the leadership and dedication of the center personnel. A clear decisive mission statement provides direction and guidance and

sets the tone for overall fusion center operations. The New Jersey Regional Operations Center also provides a collaborative environment incorporating many federal, state and local agencies, while continuing to engage the private sector in critical infrastructure and key resource protection. Utilizing existing databases, as well as federal systems, such as HSIN and Leo, provide the ROIC with the capability to exchange information across a broad spectrum of partnerships. However, a multitude of disparate databases may impinge upon information sharing as federal agencies compete for fusion center information. In addition, the New Jersey Regional Operations Center has developed an extensive privacy policy to support the protection of Civil Rights and Civil Liberties during the performance of its duties.

Although there are many attributes that could be considered in the development of a model fusion center, the New Jersey Regional Operation's Center meets and exceeds the criteria identified in the four Fusion Center Guidelines chosen for this analysis. In addition, to ensure operational efficiency and compliance, the New Jersey Regional Operations Center has instituted the Office of Baseline Capabilities. This new office ensures overall operational compliance in accordance with U.S. Department of Justice Fusion Center requirements, as well as providing oversight to support the institution of the Critical Operating Capabilities and formalized privacy policies and can be considered as a best or smart practice for other fusion centers throughout the country.

2. The Delaware Information and Analysis Center (DIAC)

a. Overview

The Delaware Information and Analysis Center was established in the spring of 2005 within the Homeland Security Unit of the Delaware State Police, which also consists of the Counterterrorism Threat Squad, and the DPS Maritime Unit. The Delaware Information and Analysis Center is an all crimes and all hazard fusion center.

The Delaware Information and Analysis Center (DIAC), Delaware's Fusion Center, serves as a critical component of Delaware's Homeland Security, as well as Criminal Intelligence, Critical Infrastructure Protection and Statewide Law

Enforcement investigative support. The DIAC adheres to an All Crimes and All Hazards approach to Homeland Security at the state level. This approach necessitates that DIAC provide real-time information and intelligence to those decision makers with a need and right to know in the law enforcement sector. The DIAC has numerous full time components embedded within that include a six person analytical section, a Critical Infrastructure Protection Unit, and a statewide WMD coordinator. The DIAC's analytic section is composed of four full time civilian intelligence analysts and two Delaware National Guard analysts, as well as a Department of Homeland Security representative.

In addition, the Department of Public Health provided a representative who works part time at the DIAC. The Critical Infrastructure Unit is composed of two sworn troopers and a civilian critical infrastructure planner. These full time members of DIAC work in conjunction with each other to identify, prevent, secure and inform Delaware's Law Enforcement, private sector and public leaders of any and all threats to the security of Delaware. In addition to the above full time partners, DIAC works daily with Delaware's Joint Terrorism Task Force, the FBI, ATF, ICE, the Delaware National Guard, United States Coast Guard, Dover Air Force Base, the U.S. Attorney's Office, and The Department of Homeland Security to ensure that information is shared and exchanged regularly to better protect our state.

In 2009, DIAC played a critical role in several events in Delaware. The DIAC once again served as the intelligence lead in both NASCAR races held at Dover Downs providing a comprehensive threat assessment of the event. DIAC also served as an intelligence and information hub for President Obama's Whistle Stop Tour and Inauguration events held in Delaware. DIAC also played a key role in the successful Returns Day event attended by Vice President Joe Biden in Georgetown in January. DIAC analysts also assisted in numerous successful criminal arrests and prosecutions. Several were the result of detailed analysis and suspect workups done by the analysts. Others were the direct result of DIAC's Daily Roll Call bulletins that allowed officers to identify suspects in numerous unsolved incidents" (Sawyer, 2010, p. 1).

b. Mission Statement

To enhance the quality of life for all Delaware Citizens and visitors by providing professional, competent and compassionate law enforcement services

c. Information Sharing

The Delaware Intelligence and Analysis Center supports information sharing through its informational bulletins. “The DIAC is proactive in reaching out to partner agencies and dissemination intelligence in a fast, efficient manner, using a variety of products, which include, but are not limited to:

- Daily Roll- Call Bulletins (BOLOs, Requests for Information, Officer Safety)
- Subject Matter-Specific Bulletins (Daily Infrastructure)
- Threat Assessments
- On-Site Analytical Support
- Long-Term Analytical Products
- Networks and Databases

There are several databases being utilized by the Delaware Intelligence and Analysis Center:

- Post-9/11, several online networks and databases have been developed which have proved useful for the purpose of sharing intelligence and other information between law enforcement agencies. These include, but are not limited to: Statewide Intelligence System (Memex Patriarch)—a private sector-developed intelligence software product that serves as Delaware’s statewide intelligence database, providing a searchable database for both intelligence reports and suspicious activity reports (SARs);

- Law Enforcement Online (LEO)—A website accredited and approved by the FBI for sensitive but unclassified information. LEO is intended to be used to support investigative operations, send notifications and alerts, and provide an avenue for federal, state, and local personnel to remotely access other law enforcement and intelligence systems and resources;
- Homeland Security State & Local Intelligence Community of Interest (HS-SLIC)—An information sharing website for federal, state, and local intelligence agencies and fusion centers;
- Regional Information Sharing Systems (RISS)—a federally funded nationwide program consisting of six regional centers and a technical support center that provides flexible and locally based services to federal, state, local, and tribal law enforcement and criminal justice agencies nationwide, as well as Australia, Canada, the United Kingdom, and New Zealand. RISS maintains the RISS Secure Intranet (RISSNET), which allows for the sharing of information and intelligence between members; and
- Guardian/E-Guardian—A centralized nationwide database for SARs
- Law Enforcement National Data Exchange (N-DEx)—A website, operated by the FBI under the auspices of the Criminal Justice Information Services (CJIS), that brings together data from law enforcement agencies nationwide, including incident and case reports, booking and incarceration data, and parole/probation information. N-DEx then detects relationships between people, vehicles/property, locations, and/or crime characteristics. The site also assists in information sharing between law enforcement agencies, fusion centers, and multi-jurisdictional task forces by notifying the organizations

involved when links are found following a query on N-DEx. All law enforcement personnel and analysts who have attended N-DEx training have access to N-DEx."

d. The Counter-Terrorism Threat Squad

The Counter Terrorism Unit focuses Delaware efforts in the mission of Homeland Security.

> The squad was established in April of 2002 and continues their homeland security efforts, protecting the citizenry and key assets of Delaware. This unit works directly with the U.S. Attorney's "Anti-Terrorism Advisory Council" (ATAC), the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF), the Bureau of Alcohol, Tobacco, and Firearms, the United States Secret Service, the United States Coast Guard, the Bureau of Immigration and Customs Enforcement (ICE), the U.S. Postal Inspector, the Delaware National Guard, all U.S. military service investigative units, other state police agencies, and regional, county/municipal law enforcement agencies. The squad is charged with investigating terrorism and related activities within the state of Delaware and works with federal agents to develop criminal intelligence information and criminal prosecutions in this area. This unit also monitors the toll free tip line for leads and assigns these leads appropriately to various law enforcement jurisdictions.
>
> (Delaware State Police Intelligence Unit, 2011, p. 1)

e. DSP Maritime Unit

As part of the information collection efforts and in an effort to enhance Port Security in Sector Delaware Bay, as well as increase security of critical infrastructure, the Delaware State Police provide security, intelligence and outreach for the state's critical infrastructure along the waterways. This unit works in conjunction with the other maritime units in the area to provide coordinated response to the needs of the Maritime Community Delaware Information and Analysis Center Privacy Policy

The purpose of an established privacy policy is to ensure the protection of individual Civil Rights and Civil Liberties under the United States Constitution.

Statement of Purpose

This privacy policy will allow the Delaware Information and Analysis Center (DIAC) to establish how protected information is collected, used, and secured in order to apply this policy to daily operations. As a result, the privacy policy will clearly define the law, policy, and procedure that the DIAC, participating agencies, and authorized users need to comply with in order to appropriately protect privacy, civil rights, and civil liberties.

The goal of establishing and maintaining the DIAC is to further the following purposes:

(a) Increase public safety and improve national security;

(b) Minimize the threat and risk of injury to specific individuals;

(c) Minimize the threat and risk of physical or financial injury to law enforcement and others responsible for public protection, safety, or health;

(d) Minimize the threat and risk of damage to real or personal property;

(e) Protect individual privacy, civil rights, civil liberties, and other protected interests;

(f) Protect the integrity of the criminal investigatory, criminal intelligence, and justice system processes and information;

(g) Minimize reluctance of individuals or groups to use or cooperate with the justice system;

(h) Support the role of the justice system in society;

(i) Promote governmental legitimacy and accountability;

(j) Not unduly burden the ongoing business of the justice system; and

(k) Make the most effective use of public resources allocated to public safety agencies.

The DIAC is a participant in the Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI). The shared space is a networked data and information repository, which is under the control of the submitting agencies and provides for the sharing of terrorism-related SAR information to participants in the NSI.

Compliance with Law Regarding Privacy, Civil Rights, and Civil Liberties

All DIAC personnel, participating agency personnel, personnel providing information technology services to the DIAC, private contractors, and users will comply with this privacy policy and all applicable law protecting privacy, civil rights, and civil liberties in the collection, use, analysis, retention, destruction, sharing and disclosure of information to DIAC personnel, governmental agencies (including ISE participating centers and agencies), and participating justice and public safety agencies, as well as to private contractors, private entities, and the general public.

Accountability and Enforcement Information System Transparency

(a) This policy establishing protections of privacy, civil rights, and civil liberties will be made available to the public on request and posted online at www.dsp.delaware.gov/.

(b) The Director of the DIAC will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center (Delaware State Police, DIAC Privacy Policy, 2011, p. 3).

f. Analysis

Although not as large as the New Jersey Regional Operations Center, the Delaware Intelligence and Analysis Center performs its fusion center function serving many customers. Driven by a simple but effective mission statement focused on providing safety and security to the community, the DIAC ensures a collaborative environment incorporating such agencies as the Federal Bureau of Investigation, Public Health, state and local law enforcement and Emergency Management. To ensure information exchange, the Delaware Intelligence and Analysis Center utilizes a myriad of

the internal databases, such as Memex, as well as external systems including the Homeland Security State & Local Intelligence Community of Interest (HS-SLIC)—an information sharing website for federal, state, local intelligence agencies, fusion centers, and the Regional Information Sharing Systems (RISS). In addition, the DIAC Privacy Policy serves the center as a guiding document to protect civil liberties and civil rights of the public, while providing the DIAC with a mechanism to determine how protected information is collected and secured. Although Privacy Policies are an important mechanisms to support Civil Rights and Civil Liberties, they are individual in nature and are not standard in language or design. Although there is similarity in core principles, they serve the purpose of the individual fusion centers much like the early development of fusion centers and may require standardization to be effective.

3. The Pennsylvania Criminal Intelligence Center (PaCIC)

a. Overview

The Pennsylvania Criminal Intelligence Center was established to enhance law enforcement informational requirements. Today it continues to serve as an efficient mechanism to provide accurate and timely information.

> The Pennsylvania State Police, Bureau of Criminal Investigation, established the Pennsylvania Criminal Intelligence Center (PaCIC) July of 2003 in an effort to provide law enforcement agencies throughout the Commonwealth with one central point of contact for their information needs. Through the PaCIC, trained analysts provide state police members and federal, state, and municipal law enforcement officers with access to intelligence information, investigative data, and public source information 24 hours a day, seven days per week. Analysts also provide investigative support by analyzing complex information and collating it into intelligence summaries, organization charts, link analysis, time event analysis, and other manageable, professional products. The PaCIC is an attempt to provide law enforcement officers a central point of contact for information needed during traffic stops, investigative detentions, and other law enforcement encounters and investigations.
>
> (Pennsylvania State Police, 2003, p. 1)

b. Mission Statement

> The mission of the PaCIC is to support the decision-making process of Pennsylvania's law enforcement agencies through collating, analyzing, and disseminating intelligence and investigative information pertaining to criminal activity while ensuring the rights and privacy of citizens are not violated.
>
> (Pennsylvania State Police, 2011, p. 1)

c. Protection of Critical Infrastructure and Key Resources

The Pennsylvania Criminal Intelligence Center is part of the Pennsylvania State Police and has created many partnerships at the federal, state, local levels of government, as well as the private sector through its Critical Infrastructure and Key Resource (CI/KR) mission guided by Homeland Security Presidential Directive 7. By examining the designated 18 key critical sectors, the Pennsylvania Criminal Intelligence Center increases community safety through an active CI/KR protection program.

> Recently the need was recognized to increase information sharing between criminal justice agencies and the owners and operators of critical infrastructure and key resources throughout Pennsylvania with whom we share the fundamental responsibility of safeguarding our communities. Critical Infrastructure / Key Resources (CI/KR) are the assets, systems, and networks, whether physical or virtual, so vital to the U.S. that their incapacitation or destruction would have a debilitating effect on security, national economic security, public health or safety, or any combination thereof. A group of Intelligence Analysts at PaCIC are specifically tasked with monitoring potential threats to the various CI/KR sectors throughout Pennsylvania and keeping the owners and operators informed so they can better protect the Commonwealth's infrastructure, environment, and citizens from future threats.
>
> (Pennsylvania State Police, 2010, p. 1).

d. Staffing

Staffing of the Pennsylvania Criminal Intelligence Center includes members of the state and federal law enforcement community tasked with a mission of

crime and terrorism prevention. All hazard prevention outside of CI/KR protection is currently the responsibility of the Pennsylvania Emergency Management Agency (PEMA).

e. Information Sharing

In order to enhance security within Pennsylvania, the Pennsylvania Criminal Intelligence Center produces and distributes the PACIC Daily Report focused on state and local crime trends and patterns, as well the Pennsylvania Criminal Intelligence Center's Information Bulletins to assist critical infrastructure owners with current threat streams that could potentially impact various CI/KR sectors.

f. Privacy Policy

The purpose of the Pennsylvania Criminal Intelligence Center's Privacy Policy is to ensure the civil liberties and civil rights of citizens are not violated during any law enforcement action. The privacy policy ensures compliance with all federal, state and local laws pertaining to the collection, use and sharing of information.

In addition, the privacy policy ensures transparency and accountability for all personnel engage in information sharing within the Pennsylvania Criminal Intelligence Center. The policy supports the information sharing environment (ISE), as well as the collection of information during Suspicious Activity Reporting. In addition, the Pennsylvania State Police have instituted privacy policy training, as well as establishing a Privacy Committee to address public concerns regarding privacy issues (Pennsylvania State Police, 2010, p. 1).

g. Analysis

The Pennsylvania Criminal Intelligence Center's mission statement emphasizes and strong and clear message of support for the fusion process, while ensuring the protection of Civil Rights and Civil Liberties of the individual. This is further highlighted in the PaCIC Privacy Policy ensuring the civil rights of citizens are not violated as a result of law enforcement actions. Transparency and accountability are

key components of the PaCIC privacy policy echoing the sentiments of the American Civil Liberties Union described in Chapter I. A collaborative environment is maintained through the incorporation of the Federal Bureau of Investigation, as well as analysis assigned to support the private sector through Critical Infrastructure and Key Resource protections.

Similar to the Delaware Intelligence and Analysis Center, the Pennsylvania Criminal Intelligence Center also utilizes similar data systems such as Memex, to share information both internally and externally with other fusion centers in an effort to streamline information and reduce costs.

4. The Maryland Coordinating and Analysis Center (MCAC)

a. Overview

The Maryland Coordination and Analysis Center (MCAC) was established under the guidance of the Maryland ATAC Executive Committee in 2003. The Anti-Terrorism Advisory Committee consists of multiple agencies and disciplines including public health, law enforcement, transportation, fire and military personnel tasked with developing policies and procedures to support terrorism prevention in the state of Maryland. The MCAC is a 24 hour, 7 day a week operation focused on an all crimes and counterterrorism mission.

b. Mission Statement

The mission of the Maryland Coordination and Analysis Center is "to provide analytical support for federal, state and local agencies involved in law enforcement, fire, emergency medical service, emergency response, public health and welfare, public safety and homeland security in Maryland " (Maryland Coordination and Analysis Center, 2007, p. 1). The Maryland Coordination and Analysis Center works closely with the Federal Bureau of Investigation's Joint Terrorism Task Force (JTTF).

c. Staffing

The MCAC staffing consists of federal, state and local government partners tasked with the prevention of crime and terrorism within the state of Maryland, including the Department of Homeland Security, ATF, DEA, ICE, and the FBI. In addition, the Maryland Coordination and Analysis Center supports three regional centers in Southern Maryland, Eastern Shore, and Western Maryland (Maryland Coordination and Analysis Center, 2007, p. 1).

d. Watch Section

The Maryland Coordination and Analysis Watch Center serves as the core center for warnings and alerts. The Watch, receives tips and leads, and identifies suspicious activities. The Watch Section's core functions include:

- Receive and process suspicious activity Tips.
- Receive and process requests for information (RFI) and requests for Service (RFS).
- Monitor all available intelligence sources.
- Coordinate Maryland law enforcement resources.
- Disseminate and Communicate intelligence information.

Primary Watch Section Databases:

- Case Explorer (Nonterrorism TIPS tracking and intelligence database).
- SONAR—MCAC tracking database.
- Guardian—FBI terrorism tracking database.
- Automated Case System (ACS).
- Maryland Motor Vehicle Administration (Maryland Coordination and Analysis Center, 2007, p. 8).

In addition to enhance information dissemination, the Maryland Coordination and Analysis Center also utilizes federal HSIN, LEO and RISS information sharing systems. These systems support information collaboration across the intelligence community.

e. Information Sharing

The MCAC supports information sharing at the federal, state and local levels of government including the Maryland Joint Terrorism Task Force (JTTF), Terrorist Screening Centers (TSC), the National Counter-Terrorism Center (NCTC), the National Operations Center (NOC), Washington/Baltimore High Intensity Drug Trafficking Area (HITA) to name a few.

f. Privacy

The MCAC privacy policy ensures that all agencies, employees and users comply with all applicable laws and regulations protecting individual and organizations privacy rights, and civil liberties in the use, analysis, retention, destruction, sharing and disclosure of protected information.

g. Analysis

The Maryland Coordination and Analysis Center's Strategic Analysis Section identifies patterns or trends, is preventative in nature, assesses threats, produces bulletins, alerts and warnings as well as strategic assessments. The mission of the (SAS) is to "to provide strategic analysis to better focus the investigative activities being conducted by law enforcement agencies within the state and to better enable public health and safety agencies to perform their important protective functions" (Maryland Coordination and Analysis Center, 2007, p. 10).

The Maryland Coordinating and Analysis Center, is uniquely housed in federal space overseen by the U.S. Attorney's Advisory Council, which appears to provide direct connectivity with the Federal Bureau of Investigation Joint Terrorism Task Force, as well as other federal agencies, such as the Terrorist Screening Center (TSC), the

FBI Counter Terror Watch, and the National Counter-Terrorism Center (NCTC). The MCAC is a collaborative environment consisting of many federal, state and local law enforcement agencies, including the FBI, Maryland State Police and Baltimore City Police Department.

The Maryland Coordinating and Analysis and Coordinating Center utilizes a number of federal, state and local databases, including Interpol, Leo, HISN and RISS. In addition, the Maryland Coordination and Analysis Center supports three regional centers in Southern Maryland, Eastern Shore and Western Maryland. The MCAC's mission statement emphasizes analytical support to both traditional law enforcement and nonlaw enforcement agencies such as fire, public health and welfare and emergency response ensuring collaboration across a broad spectrum of emergency responders. Although, it is not possible at this time to integrate every fusion center into federal space, the Maryland Coordination and Analysis Center appears to be a model of federal, state and local cooperation, with enhanced data mining capabilities based on location.

THIS PAGE INTENTIONALLY LEFT BLANK

V. ANALYSIS/RECOMMENDATIONS

Chapter V provides a summary analysis of the current state of fusion centers. While a formalized Fusion Center Doctrine may not be the appropriate solution to support fusion center maturation, it describes how guidance is being effectively applied by the U.S. Department of Justice and U.S. Department of Homeland Security to enhance fusion center development, including institution of the four identified critical operating capabilities. Chapter V concludes with identifying the core competencies necessary to build a model fusion center, as well as areas for future consideration and research.

In order to enhance multidiscipline information sharing at the federal, state and local levels of government, the United States Department of Homeland Security has identified state and local/regional fusion centers as primary points of collection, analysis, and distribution of real-time threat information over the Fusion Center Network. There are currently 72 fusion centers throughout the United States operating at different levels of capability. These centers created in 2004 and 2005 were initially developed with little guidelines or formalized structure. The U.S. Department of Homeland Security and U.S. Department of Justice have since produced many documents to serve as templates or guidelines to support fusion center's development and to support a cohesive fusion center network.

No two fusion centers are alike, there is no formalized uniformity, although this research has shown that fusion centers contain core principles identified in the Fusion Center Guidelines and Baseline Capabilities, their missions are unique to the environment and their area of responsibility. Owned and operated by state and local governments, these centers are an extension of those individual states and local government's prevention strategies. Although this research has exhibited an unequivocal requirement for the development of fusion centers by many federal, state, local, tribal and Private

Sector entities to support crime and terrorism prevention, it has also demonstrated that the protection of civil rights and civil liberties are paramount as fusion centers move forward in their quest to prevent crime and terrorism.

Although the possibility of developing a formal fusion center doctrine, one that would enable all fusion centers to function consistently, was considered, formal doctrines are often rigid and leave little room for the necessary flexibility that is required to support individual state and local missions. In addition, a federal formal doctrine that is directive in nature may be seen as intrusive and may not take into account state and local requirements. “Given that fusion centers are entities established by states, localities and regions to serve their own criminal, emergency response, and terrorism prevention needs, and the sensitivities associated with federalism, there may not necessarily be a federal remedy to every fusion center-related issue” (Rollins, 2007, p. 56).

A review of the U.S Department of Homeland Security and U.S. Department of Justice Fusion Center Guidelines, Fusion Center Baseline Capabilities, Privacy and Civil Liberties and Civil Rights Protections, as well as the Critical Operational Capabilities during this research, conclude that these documents are both accepted by the fusion center community and are very capable of serving as templates for nonrestrictive guidance. They would provide the fusion centers with the necessary direction to be effective, while affording individual fusion centers the ability to establish their unique priorities based on their area of responsibilities.

In addition, these documents provide a comprehensive roadmap for success, and with the continual support from the U.S. Department of Homeland Security, these efforts have proven to be both effective and efficient. Further support for the implementation of fusion center guidelines was offered by several law enforcement agencies that are the core of Fusion Center Operations. “The Federal Fusion Center Guidelines (FCG) received support from several law enforcement organizations, including the Law Enforcement Intelligence Unit (LEIU) and Major Cities Chiefs Association (MCCA), which added further credibility to the fusion center movement”(Rollins, 2006, p. 40).

A review of the 2010 Baseline Capabilities assessment of Fusion Centers and Critical Operational Capabilities Gap Mitigation Strategy revealed that these guidelines are proven effective and promising in reaching stability and cohesiveness among the Fusion Center Community.

In September 2010, federal, state, and local officials completed the first nationwide, in depth assessment of fusion centers to evaluate fusion center capabilities and to establish strategic priorities for federal government support. The 2010 Baseline Capabilities Assessment (BCA) was conducted by the Office of the Program Manager for the Information Sharing Environment (PM-ISE), in coordination with Fusion Center Directors, the Department of Homeland Security (DHS), the Federal Bureau of Investigation (FBI), and other federal interagency partners.

The objectives of the BCA were to; Assess fusion centers' capabilities in an effort to understand the overall maturity of the National Network of Fusion Centers; Leverage the data gathered to enhance the efficiency and effectiveness of federal support of fusion centers' efforts to achieve and maintain baseline capabilities through investment planning and prioritized resource allocation; Establish strategic priorities and help identify gaps in capabilities at individual fusion centers and across the National Network; and aid fusion centers in reaching their full potential to serve as focal points within the state, local, tribal, and territorial (SLTT) environment for the receipt, analysis, gathering, and sharing of threat-related information.

The 2010 BCA on-site validation focused primarily on the four Critical Operational Capabilities (COCs), which reflected the National Network priorities identified jointly by Fusion Center Directors and the federal government during the 2010 National Fusion Center Conference:

- COC 1—Receive: Ability to receive classified and unclassified information from federal partners;
- COC 2—Analyze: Ability to assess local implications of threat information through the use of a formal risk assessment process;

- COC 3—Disseminate: Ability to further disseminate threat information to other SLTT and private sector entities within their jurisdiction; and
- COC 4—Gather: Ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners, as appropriate.

Beginning in January 2011, DHS launched an effort to evaluate both the results of the short-term COC gap mitigation efforts, and the effectiveness of federal resources provided to assist fusion centers in building their capabilities in the COCs and P/CRCL protections. Based on the results of this evaluation, fusion centers made progress from September 2010 to December 2010 in building their capabilities and addressing gaps identified during the BCA. Fusion centers reported significant progress in defining their business processes through the development of final, approved plans, policies, and/or standard operating procedures for each of the four COCs. The greatest increase in capabilities during the short-term COC gap mitigation efforts were related to COC 2: Analyze, and P/CRCL protections. Fusion centers overwhelmingly responded that they were provided a clear understanding of the intent and expected timeframe associated with the Short-Term Strategy, and that they were provided with adequate guidance to meet the short-term gap mitigation objectives" (U.S. Department of Homeland Security, 2010 Baseline Capabilities assessment of fusion centers, 2010, p. 1).

Employing a formative evaluation methodology provided a unique perspective based on-site observations in four fusion centers located in the Northeastern United States. These four centers in New Jersey, Delaware, Pennsylvania and Maryland were chosen due to their geographical locations. In addition, the information acquired during this process will be utilized by my agency, the Philadelphia Police Department, to support the development of a future fusion center located in the Delaware Valley Region, whose mission will be to support the above-mentioned four state fusion centers from a regional area of operations.

The purpose was to improve the program by identifying strengths and weaknesses of existing fusion centers, identify the importance or lack of importance of

standardization, identify means of effective information sharing and collaboration to enhance the fusion center network and to identify or create synthesis in discovering the required steps or actions to build a model fusion center.

By employing the Program Evaluation Method, it was possible to identify and capture real-world nuisances during on-site observations that would not have been possible utilizing alternative research methods such as a survey methodology. In addition, the employment of a Force Field Analysis provided a mechanism to identify the driving forces that are positive for the development of a model fusion center and areas that inhibit fusion center effectiveness.

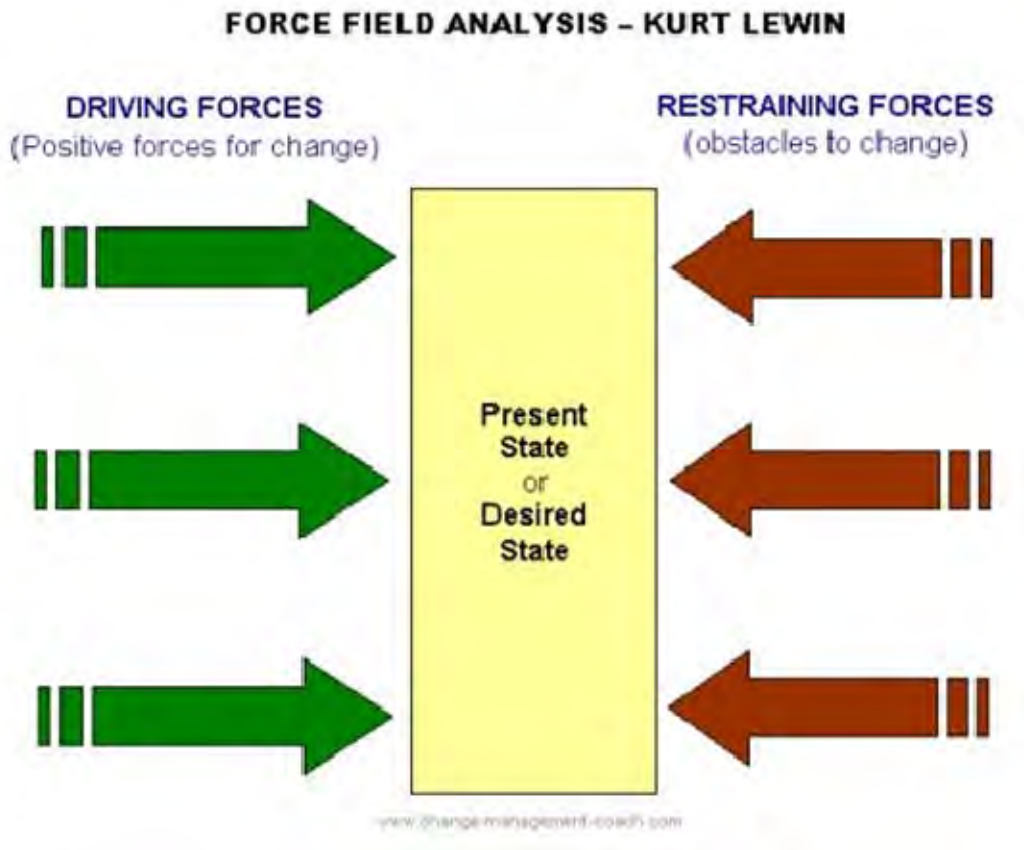

Figure 6. Force Field Analysis

Positive Forces (Driving Forces) identified during this analysis of the four chosen fusion centers revealed the following:

Strong Leadership appears to be a key component in the development of effective model fusion center. First identified in the Fusion Center Guidelines as a core principle. In developing our country's response to the threat of terrorism, law enforcement, public safety, and private sector, leaders have recognized the need to improve the sharing of information and intelligence across agency borders. Every official involved in information and intelligence sharing has a stake in this initiative. Leaders must move forward with a new paradigm on the exchange of information and intelligence; one that includes the integration of law enforcement, public safety, and the private sector (U.S. Department of Justice and U.S. Department of Homeland Security, 2006, p. iii). The importance of leadership was further collaborated during onsite fusion center visits, as well as being identified as a recognized criteria in award winning fusion centers. This quality further epitomizes the importance of leadership to ensure compliance, accountability and transparency in fusion center operations.

Developing a clear and concise Mission Statement.

> A mission statement is a written statement of the organization's purpose, such as enhancing public safety, sharing information, or resolving criminal investigations. It is important to have a mission statement because it focuses efforts and is the foundation of all the decisions that follow. A mission statement can also inspire people in the organization and inform customers of the benefits and advantages of what the organization offers and is the first step in educating entities about the center and its services.
>
> (U.S. Department of Justice and U.S. Department of Homeland Security, 2006, p. 23)

Building a model fusion center begins with establishing focus. The analysis of all four fusion centers indicated that their mission statement provided clear direction for current and future development.

Institution of a formal privacy policy to ensure protection of Civil Liberties and Civil Rights protections. Protecting Civil Rights and Civil Liberties is paramount within the development of a model fusion center.

> The National Criminal Intelligence Sharing Plan (NCISP) stresses the need to ensure that constitutional rights, civil liberties, civil rights, and

> privacy are protected throughout the intelligence process. In order to balance law enforcement's ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be in place.
>
> (U.S. Department of Justice and U.S. Department of Homeland Security, 2006, p. 41)

Establishing a collaborative environment for sharing of information—collaborative environments support information sharing across a wide spectrum of first responders. Collaboration was a key element observed in the four fusion centers visited during this analysis. Described as a collaborative justification under Fusion Center Guideline # 4, collaboration is a means used to:

> To maximize intelligence sharing, all levels of law enforcement and public safety agencies and the private sector must communicate and collaborate. The objective is to leverage resources and expertise while improving the ability to detect, prevent, and apprehend terrorists and other criminals.
>
> Fostering a collaborative environment builds trust among participating entities, strengthens partnerships, and provides _individual as well as a collective ownership in the mission and goals of the center.
>
> (U.S. Department of Justice and U.S. Department of Homeland Security, 2006, p. 29)
>
> Leverage the databases, systems, and networks. Leveraging existing databases reduces cost and provides immediate communication. "Centers may want to evaluate the types of databases that participating agencies have available. Gaps should be identified and researched. Leveraging the databases and systems available via participating entities will help maximize information sharing.
>
> (U.S. Department of Justice, U.S. Department of Homeland Security 2006, p. 33)

Fusion centers utilizing comparative databases will streamline information exchange, reduce costs and support fusion center operations. Building a model fusion center will require a general and specific understanding of the various databases at the

federal state and local levels to exchange information. Identifying correlating databases will support technological collaboration

Although, further study could identify additional similarities, these five positive driving forces were identified as key themes consistent with each fusion center during this research. In addition, these themes are consistent with the recommended Fusion Center Guidelines for developing and sharing information and intelligence in a new era.

Negative Forces (Restraining Forces) identified during this analysis of the four chosen fusion centers revealed the following:

No two fusion centers are alike, and there is no formalized uniformity. Although this research has shown fusion centers contain core principles identified in the Fusion Center Guidelines and Baseline Capabilities, their missions are unique to the environment, and their area of responsibility, as well as to the states and local governments they serve.

Although, Privacy Policies are important mechanisms to support Civil Rights and Civil Liberties, they are individual in nature and are not standard in language or design. Although,, there is similarity in core principles, they serve the purpose of the individual fusion centers, much like the lack of standardization first observed in the development of early of fusion centers and may require standardization to be effective.

Utilizing existing databases, as well as federal systems such as HSIN and Leo, provide fusion centers with the capability to exchange information across a broad spectrum of partnerships. However, a multitude of disparate databases may impinge upon information sharing at the federal state and local levels. In developing a model fusion center, it is necessary to weave through competing databases and support development of database interoperability.

No defined Performance Measure to indicate Fusion Center Value. Although this research has reviewed many documents and conducted onsite observations, there are currently no formalized performance measures or matrix to ensure fusion center performance. As budgets are cut across the spectrum of federal programs, fusion centers will be required to exhibit value added to the Intelligence Community. Although, success

stories are important, developing a model fusion center will require a more formalized mechanism or structure to ensure success.

A. RECOMMENDATIONS

Fusion centers across the country will continue to serve as a key component in the intelligence community. The recent terrorist attack in Times Square, New York have proven that an alert public, supported by a well-informed and coordinated law enforcement agency serving in a multijurisdictional environment, can prevent terrorist activity. Although, fusion centers serve as portals for collaboration, their true value lies in the relationships they create and the willingness of individuals to cross federal, state, local and tribal boundaries to keep communities safe. In addition, this research has shown that protecting privacy of individuals must remain constant in all fusion center applications. Although there is a myriad of suggestions or guidelines to support the development of a model fusion center, core components, such as a strong Mission Statement to establish direction of effort and leveraging existing databases that are comparative with other fusion center's databases, are effective strategies to reduce costs and support integration efforts.

It is also critical in today's economy to ensure proper staffing, continual funding, as well as promoting fusion center's awareness as key components to address crime and terrorism and identifying the path forward in creating a network of fusion centers of excellence. Although short-term gap mitigation proved successful, the true value of fusion centers is operating as a united force. One way to ensure future success of fusion centers is to develop Performance Measures to indicate fusion center value.

> To enhance the ability to demonstrate the results fusion centers are achieving in support of national information sharing goals and help prioritize how future resources should be allocated, the Secretary of Homeland Security should direct the State and Local Program Office, in partnership with fusion center officials, to define the steps it will take to design and implement a set of standard performance measures to show the results and value centers are adding to the Information Sharing Environment and commit to a target timeframe for completing them.

(GAO-10-972, 2010, p. 1)

In addition, fusion centers must be predictive in nature avoiding the Black Swan event, one that is highly improbable, with a devastating impact that we should have seen coming. By utilizing a risk based analysis, fusion centers will begin to better forecast merging threats, improve performance and enhance prevention. Utilizing business models, such as the "Cynefin Framework," Fusion centers can institute predictive analysis, better forecast potential problems, learn to survive, or at least exist in various complex, complicated, chaotic and simple environments (Snowden, 2003, p. 1).

B. CONCLUSION

In the aftermath of September, 11, 2001, it became clearly evident that the United States faced a new and dynamic enemy, one that valued imagination as a strategic advantage. This new enemy with external support adapted to operate internally within America. Failure of imagination (9/11 Commission) is the process of failing to recognize the recognizable. Today's enemy seeks new opportunities and places the American public at risk. Failure to share information across the wide spectrum of intelligence agencies at the federal, state, tribal and local levels of government may result in another high impact event.

Fusion Centers are in a unique position to provide the necessary collaborative space to bring the federal intelligence community together with state, local and tribal initiatives to support Homeland Security efforts at the grass roots level.

Proficiency and perfection are critical components in today's fusion center environment. Tasked with the ability to share information and create collaboration between federal, state, local and tribal partners, while managing an all crimes and all hazards perspective, in addition to preventing terrorism, will require a finely honed instrument. On March 11, 2009, United States Department of Homeland Security Secretary Napolitano related in her remarks to the National Fusion Center conference in Kansas City, Missouri, "I believe that fusion centers will be the centerpiece of state, local, federal intelligence-sharing for the future and that the Department of Homeland

Security will be working and aiming its programs to underlie fusion centers" **(**Napolitano, 2009**).**

Today, there are currently 72 fusion centers throughout the county comprised of 50 state and 22 local or regional centers. These centers created in 2004 and 2005 were initially developed with few guidelines or formalized structures, which limited their ability to effectively communicate or share information with other federal, state and local partners. However, an analysis of the four fusion centers conducted during this research indicates a positive change, as these centers appear to be steadily moving in a direction of cohesiveness and uniformity based on the guidance provided by existing documents and the support of the U.S. Department of Homeland Security and the U.S. Department of Justice.

In addition, this research has concluded that building a model fusion center will require adoption of identified core competencies including; Strong leadership, clear mission statements, goals and objectives, development of a formal privacy policy to ensure civil liberties and civil rights based on lawfulness and constitutional protections, standard operating procedures, consistent training, creation of a collaborative environment, adherence with the National Criminal Intelligence plan, governance, and common analytical tools, as well as ensuring products that meet customers requirements.

Although the possibility of developing a formal fusion center doctrine, one that would enable all fusion centers to function consistently, was considered, formal doctrines are often rigid and leave little room for the necessary flexibility that is required to support individual state and local missions. In addition, a federal formal doctrine that is directive in nature may be seen as intrusive and may not take into account state and local requirements. "Given that fusion centers are entities established by states, localities and regions to serve their own criminal, emergency response, and terrorism prevention needs, and the sensitivities associated with federalism, there may not necessarily be a federal remedy to every fusion center-related issue" (Rollins, 2007, p. 56).

In addition, although the development of core competencies ensures success of fusion centers, operational relevance will only be achieved through the development of fusion center's Performance Measures.

> To enhance the ability to demonstrate the results fusion centers are achieving in support of national information sharing goals and help prioritize how future resources should be allocated, the Secretary of Homeland Security should direct the State and Local Program Office, in partnership with fusion center officials, to define the steps it will take to design and implement a set of standard performance measures to show the results and value centers are adding to the Information Sharing Environment and commit to a target timeframe for completing them.
>
> (GAO-10-972, 2010, p. 1)

Turning information into actionable intelligence is the corner stone of fusion center operations; failure to connect the dots described in the 9/11 Commission report led to the devastating terrorist attacks on September 11, 2001. There are currently numerous databases at the federal, state and local levels of government that limit federate search capability. Although, there are improvements on the horizon, this appears to be more of a need for a cultural change than a need for a technology required solution.

Lastly, there are many positive initiatives that will support future fusion center operations that may require further research to ensure success. One area that appears promising is the unwavering support of the Federal Bureau of Investigation and their commitment, under the Deputy Assistant Director Harris, to provide analytical support from their field/regional intelligence group into enhance federal, state, tribal and local information sharing effectiveness on a state and regional level.

Another area for consideration is an inspiring commitment from the Major Cities Chief's Association to approve the establishment of a "National Criminal Intelligence Enterprise (NICE)."

> The objective is to establish the necessary architecture to better connect state and local intelligence efforts, develop a better understanding of

> regional threat domains, compliment the capabilities of the FBI and DHS, and fulfill the objective of state and local law enforcement to prevent crime and terrorism.
>
> (Major Cities Chief's Intelligence Commanders Group, 2011, p. 1)

This idea is further collaborated in a study conducted by George Washington University, Homeland Security Policy Institute entitled "Counterterrorism Intelligence: Law Enforcement Perspectives." In this study, it is suggested that law enforcement is both the first and last line in detecting threats of terrorism within our communities, however, the ability of American officials to support those law enforcement officers on the front line is an open question as the United States lacks understanding of the intelligence enterprise, which results in a limited ability to develop anticipatory knowledge regarding future attacks (Cilluffo, Clark, Downing 2011, p. 1). Both of these initiatives support the fusion center environment and appear to open new possibilities for future collection, analysis, and dissemination of critical information.

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

ACLU. (2010). *What's wrong with fusion centers*, November 14, 2010, Retrieved October 10, 2011 from www.ACLU.org

Brafman, O. & Beckstorm, R. (2006). The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations. Penguin group (USA) 2006.

Carter, D. (2004). Law Enforcement Intelligence, November 4, 2010. Retrieved September 9, 2011 from www.COPS.USDOJ.gov

CRS Report. (2010). *Fusion Center- Council on Foreign Relations*, November 5, 2010. Retrieved October 10, 2011 from www.cfr.org

Counterterrorism Intelligence Law Enforcement Perspectives. Retrieved November 11, 2011 from www.gwumc.edu/.../HSPI%20Research%20Brief%20-

Department of Homeland Security. (2009). *(SIPRNET*), November 6, 2010. Retrieved September 9, 2011 from http://www.dhs.gov/ynews/releases/pr_1252955298184.shtm

Delaware Information and Analysis Center. Retrieved November 11, 2011 from http:/dsp.delaware.gov

Delaware State Police Intelligence Unit. Retrieved November 29, 2011 from dsp.delaware.gov/Intelligence.shtml

Delaware State Police - Intelligence Unit. Retrieved November 11, 2011 from dsp.delaware.gov/intelligence%20unit.shtml

DHS. | *2010. Baseline Capabilities Assessment* of Fusion Centers. Retrieved November 2, 2011 from ...www.dhs.gov/files/programs/gc_1296491960442.shtm

FBI. (2008). *Connecting the Dots*. November 14, 2010. Retrieved November 22, 2011 from www.fbi.gov FBI — The *FBI and Fusion Centers*, *www.fbi.gov/news/testimony/the-fbi-and-fusion-center_sReterived*

FEMA. (2009). *Federal Emergency Management Agency*, November 6, 2010. Retrieved November 1, 2011 from www.fema.gov *Findings and Recommendations* of the *Suspicious* Activity Report, Retrieved November 22, 2100 from iwitnessvideo.info/files/mccarecommendation-06132008.pd

Firehouse News. (2010). *DHS wants Fire Service to Join Fusion Centers*, November 6, 2010. Retrieved November 3, 2011 from www.Firehouse.com

Fusion Center Guidelines. (2010). Retrieved September 4, 2011 from www.it.ojp.gov Homeland Security (2009) *About the Homeland Security Information Network*, November 4, 2010. Retrieved November 11, 2011 from www.DHS.gov

Homeland Security. (2010). *State and Local Fusion Centers*, Retrieved November 11, 2011 from www.DHS.gov *FUSION CENTER* UPDATE - *American Civil Liberties Union*. Retrieved November 20, 2011 from *www.aclu.org/files/pdfs/privacy/fusion_update_20080729.pdf*

Information Sharing Environment (ISE) - Suspicious Activity. Retrieved November 5, 2011 from nsi.ncirc.gov/documents/NSI_EE.pdf

Kaplan, E. (2007). CRS report: Fusion Centers, November 6, 2010. Retrieved November 22, 2011 from http://www.cfr.org/intelligence/fusion-centers/p12689

Law Enforcement Online. (1995). *LEO*, November 6, 2010. Retrieved November 23, 2011 from www.FBI.gov

Major Cities Chief's, National Criminal Intelligence Enterprise. 2011. Retrieved November 10, 2011 from *Maryland Coordination and Analysis Center* Overview www.thetrainingco.com/pdf/.../MCAC%20PRES%20-%20Eisenburg...

Masse, T., O'Neil, S., & Rollin, J. (2007). *CRS Report: Fusion Center*, November 6, 2010. Retrieved November 28, 2011 from www.CFR.org

Napolitani. (2009). *Eight Years After 9/11: Confronting the Terrorist Threat To The Homeland*, November 6, 2010. Retrieved November 26, 2011 from www.DHS.gov

New Jersey Regional Operations Intelligence Cen… Retrieved November 22, 2011 from *Www.Nfcausa.Org/.../Documentdownload.Aspx?Documentid=42...1*

Office of Intelligence and Analysis. (2010). November 3, 2010. Retrieved November 29, 2011 from www.FEMA.gov

PaCIC Privacy Policy. Retrieved November 22, 2011 from *www.pema.state.pa.us/portal/server.pt/.../pacic_privacy_prolicy*

Pennsylvania Criminal Intelligence Center - *Commonwealth Portal*. Retrieved November 22, 2011 from www.portal.state.pa.us/portal/server.pt?open=512...

Porter, R. Office of the Director of National Intelligence, 2011 Fusion Center presentation, Fusion Center Leadership program, Naval Postgraduate School, Monterey, CA.

Regional Information Sharing. (2007). *RISS*, November 6, 2010. Retrieved November 26, 2011 from, www.ncjrs.gov

Regional Operations Intelligence Center. 2006. Brochure, All Crimes, All Hazards, All Threats. November 20, 2011. New Jersey State Police

Riegle, R. (2009). *The Future of Fusion Center and Potential Promise and Danger*, November 6, 2010. Retrieved November 22, 2011 from www.DHS.gov

Snowden, D. J. - Cynefin *S*ense making Framework - PAEI ... Retrieved November 26, 2011 from www.*paei.wikidot.com/snowden-d-j-cynefin-sensemaking-framework*

U.S. Department of Homeland Security. (2010). *Advisory Council*, November 4, 2010. Retrieved November 2, 2011 from www.DHS.gov

U.S. Department of Justice. (2007). *Regional Information Sharing System*, November 6, 2010. Retrieved November 24, 2011 from www.ncjrs.gov

United States Government Accountability Office. (2007). *Preview of the US Department of Homeland Security Efforts into Information Sharing*, November 5, 2010. Retrieved October 3, 2011 from www.GAO.gov

United States Department of Justice. (2010). *Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI)*, November 3, 2010. Retrieved September 2, 2011 from www.NIEM.gov

United States Department of Justice. (2010.*) Critical Operational Capabilities for State and Major Urban Area Fusin Centers.* November 16, 2010, *Global Justice Information Sharing Initiative.* Retrieved October 12, 2011 from www.DHS.gov

U.S. Department of Homeland Security, Office of Inspector General Report. (2008). "DHS' Role in State and Local Fusion Centers is Evolving" United States Department of Homeland Security. Retrieved September 2, 2011 from http://www.dhs.gov/

Welcome to the ROIC - New Jersey Office of Emergency Management. Retrieved November 11, 2011 from .www.ready.nj.gov/media/pdf/102308_oembulletin.pdf

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Police Commissioner, Charles H. Ramsey
   Philadelphia Police Department
   Police Headquarters
   Philadelphia, Pennsylvania