NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

DEVELOPING A BLUEPRINT FOR SUCCESSFUL PRIVATE PARTNERSHIP PROGRAMS IN SMALL FUSION CENTERS: KEY PROGRAM COMPONENTS AND SMART PRACTICES

by

Kenneth Rueben

March 2013

Thesis Co-Advisors: Lauren Fernandez
Kathleen Kiernan

Approved for public release; distribution is 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** March 2013	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE DEVELOPING A BLUEPRINT FOR SUCCESSFUL PRIVATE PARTNERSHIP PROGRAMS IN SMALL FUSION CENTERS: KEY PROGRAM COMPONENTS AND SMART PRACTICES			**5. FUNDING NUMBERS**
6. AUTHOR(S) Kenneth Rueben			
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)

The *Baseline Capabilities for State and Major Urban Area Fusion Centers* required fusion centers to establish programs to interact with the private sector. These programs took the form of Public and Private Sector outreach programs. This requirement had a profound budgetary and operational impact on fusion centers, but agencies received very little guidance about how to plan, organize, and sustain these programs.

The goal of this thesis was to identify smart practices and create an operational blueprint that fusion centers and intelligence units could use to establish a successful private sector outreach program. Three nationally recognized programs were studied and evaluated by a panel of subject-matter experts. The group identified six fundamental components that executives should consider prior to establishing a program: determine if the host agency has the expertise to manage the program, assess the agency's culture to identify it's willingness to interact with the business community, establish sustainable funding mechanisms prior to implementing the program, use a hybrid approach to communication including websites and face-to-face meetings, fully understand the value of the private sector, and emphasize the importance of participation by agency leadership.

14. SUBJECT TERMS Fusion Centers, Capabilities, Public and Private Sector Outreach Programs, Fusion Center Leadership, Criminal Intelligence Programs, Law Enforcement Agency Culture, Law Enforcement Communication Methods, Establishing a Law Enforcement Program, Best practices, Smart Practices, Key Considerations, National HIDTA Program, Oregon Department of Justice			**15. NUMBER OF PAGES** 109
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UU

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 BLUEPRINT FOR SUCCESSFUL PRIVATE PARTNERSHIP PROGRAMS IN SMALL FUSION CENTERS: KEY PROGRAM COMPONENTS AND SMART PRACTICES

Kenneth Rueben
Special Agent in Charge, Oregon Department of Justice
B.S., City University of Seattle, 2001

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
March 2013**

Author: Kenneth Rueben

Approved by: Lauren Fernandez
Thesis Co-Advisor

Kathleen Kiernan
Thesis Co-Advisor

Daniel Moran
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The *Baseline Capabilities for State and Major Urban Area Fusion Centers* required fusion centers to establish programs to interact with the private sector. These programs took the form of Public and Private Sector outreach programs. This requirement had a profound budgetary and operational impact on fusion centers, but agencies received very little guidance about how to plan, organize, and sustain these programs.

The goal of this thesis was to identify smart practices and create an operational blueprint that fusion centers and intelligence units could use to establish a successful private sector outreach program. Three nationally recognized programs were studied and evaluated by a panel of subject-matter experts. The group identified six fundamental components that executives should consider prior to establishing a program: determine if the host agency has the expertise to manage the program, assess the agency's culture to identify it's willingness to interact with the business community, establish sustainable funding mechanisms prior to implementing the program, use a hybrid approach to communication including websites and face-to-face meetings, fully understand the value of the private sector, and emphasize the importance of participation by agency leadership.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....1
B. RESEARCH QUESTIONS....5
C. LITERATURE REVIEW....5
1. Introduction and Background....5
2. Findings and Claims....7
3. Government Publications....7
4. Reports for Congress....8
5. Journal Articles....9
D. RESEARCH METHOD....11
1. Data Sample....12
2. Data Collection....13
3. Data Analysis....13

II. FUSION CENTER OVERVIEW....17
A. WHAT IS A FUSION CENTER?....17
B. TYPES OF FUSION CENTERS....19
C. FUSION CENTER SPECIAL PROGRAMS AND FEATURES....21
1. Training Programs....23
2. Critical Infrastructure and Key Resources Programs (CI/KR)....24
3. Suspicious Activity Reporting....26
4. Special Events Support....27
5. Watch Centers....28
6. Equipment Loan Programs....29
7. Products and Publications....29
8. The Role of the Criminal Intelligence Analyst....30
D. FUSION CENTER COMMUNICATION TECHNIQUES....31
1. Homeland Security Information Network (HSIN)....32
2. INfraGard....34
3. Regional Information Sharing Systems (RISS)....36
4. Custom-Built Fusion Center Websites....38

III. CASE STUDIES OF PRIVATE PARTNERSHIP PROGRAMS....41
A. CASE STUDY NUMBER ONE, THE LOS ANGELES JOINT REGIONAL INTELLIGENCE CENTER....41
1. Background....41
2. Critical Errors in Planning or Operations....43
3. Obstacles to Success....44
4. Key Program Components and Smart Practices....44
B. CASE STUDY NUMBER TWO, THE COLORADO INFORMATION ANALYSIS CENTER....46
1. Background....47
2. Critical Errors in Planning or Operations....49

3. Key Program Components and Smart Practices 50
C. CASE STUDY NUMBER THREE, THE ORANGE COUNTY SHIELD PROGRAM 52
1. Background 53
2. Critical Errors in Planning or Operations 56
3. Obstacles to Success 56
4. Key Program Components and Smart Practices 56
D. CASE STUDY ANALYSIS 58
IV. FOCUS GROUP INTERVIEWS 63
A. BACKGROUND 63
B. FOCUS GROUP DISCUSSION 65
V. FOCUS GROUP ANALYSIS 69
A. FUNDING 69
B. LEADERSHIP 69
C. PROGRAM OVERSIGHT 71
D. PROGRAM COMMUNICATION METHODS 71
E. SMALL-AGENCY ISSUES 71
F. MENTORING 72
G. PLANNING TEAM CONTINUITY 73
VI. RECOMMENDATIONS AND CONCLUSION 75
A. FINDINGS 75
B. AGENCY SELF-EXAMINATION 76
C. AGENCY CULTURE 76
D. FUNDING 77
E. COMMUNICATION METHODS 77
F. UNDERSTANDING THE PRIVATE SECTOR 78
G. LEADERSHIP INVESTMENT 78
H. RECOMMENDATIONS 79
I. CONCLUSION 80
APPENDIX A. PROGRAM MANAGER INTERVIEW QUESTIONS 81
APPENDIX B. BLUEPRINT GUIDE FOR ESTABLISHING PUBLIC/PRIVATE PARTNERSHIP PROGRAMS IN SMALL FUSION CENTERS: KEY PROGRAM COMPONENTS AND SMART PRACTICES 85
BIBLIOGRAPHY 91
INITIAL DISTRIBUTION LIST 95

LIST OF ACRONYMS AND ABBREVIATIONS

ACAMS	Automated Critical Asset Management System
ACLU	American Civil Liberties Union
ACTIC	Arizona Counter Terrorism Intelligence Center
BJA	United States Bureau of Justice Assistance
CELL	Center for Empowered Living
CI/KR	Critical Infrastructure and Key Resources
CIAC	Colorado Information Analysis Center
COP	Community Oriented Policing
DHS	United States Department of Homeland Security
EMS	Emergency Management Services
FBI	Federal Bureau of Investigation
FBI JTTF	Federal Bureau of Investigation's Joint Terrorism Task Force
FLO	Fusion Liaison Officer
FOUO	For Official Use Only
GIS	Geospatial Information System
HIDTA	High Intensity Drug Trafficking Area Program
HSAC	Homeland Security Advisory Council
HSIN	Homeland Security Information Network
ISE	Intelligence Sharing Environment
LAPD	Los Angeles Police Department
MOU	Memorandum of Understanding
NCISP	National Criminal Intelligence Sharing Plan
NFCG	National Fusion Center Guidelines
NYPD	New York Police Department
OCIAC	Orange County Intelligence Assessment Center
ONDCP	Office of National Drug Control Policy
RISS	Regional Information Sharing Systems
SLATT	State and Local Anti-Terrorism Training
TITAN	Oregon Terrorism Intelligence Threat Assessment Network
TLO	Terrorism Liaison Officer
WSIN	Western States Information Network

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

I owe a tremendous debt of gratitude to an amazing group of people that made the completion of this thesis and program possible.

First of all, I would like to thank my good friend, and Oregon HIDTA Program Director, Chris Gibson, for spending countless hours listening to me complain and eventually helping me focus on a thesis topic. When I started this program at CHDS, my goal was to create a thesis project that would benefit my home agency, the Oregon Department of Justice and the Oregon HIDTA Program. Chris helped me get there with his innovative suggestions, program insight, and his expertise in strategic planning. I owe you one Chris!

As anyone who has created a thesis knows, the project often becomes a group endeavor. Recognizing that fact, I want to thank my colleagues in Cohort 1105 and 1106. The intense discourse during the past 15 months with a group of brilliant people was both challenging and rewarding. I have to say the CHDS program was the most satisfying education program I have ever experienced. A special note of thanks to Professor Chris Bellavita. The "3" you gave me on my first paper, and your endless harassment and lightening-quick wit, kept me focused and engaged. Thanks to all of you!

I was extremely fortunate to establish a number of friendships during this program. I want to especially thank Bill Wickers, Dave Brown, Dave Ferguson, Joel Justice, and Chris Sweeney. Without your friendship and support, countless hours of debate, and your amazing sense of humor, I probably wouldn't have finished this project. You all proved me right when I noted in one of our first essays, "You always learn more from the other students than from the instructors." I look forward to extending our friendships in the years to come. Thanks!

As we all quickly learned, picking the right thesis advisor has a direct correlation to the quality of the end product and the educational experience for the student. I hit the jackpot with my team, Lauren Fernandez and Kathleen Kiernan. Both of these exceptional women provided me countless hours of assistance, guidance, and support. Thank you both for everything!!

I am truly grateful to my supervisor and colleagues at the Oregon Department of Justice, and Criminal Justice Division for picking up the slack when I was gone and providing your never-ending support. Special thanks to Darin Tweedt, Chief Counsel, for allowing me to participate in this program. To Mike Loughary, Steve McIntosh, and Chuck Cogburn, who managed the investigations unit and fusion center in my absence. You guys are awesome!

To gather the data needed for this thesis, I needed to find brilliant leaders who have established and led successful outreach programs. A special thanks to Brenda Leffler, from the Colorado RUBICON team, Regina Miles, from the InfraGard Los Angeles Program, and Heather Houston, from the Orange County SHIELD program. Your insight and expertise was the foundation for this thesis.

This thesis also relied heavily on subject-matter experts who leant their experience and creativity to the project's findings and recommendations. Steve Briggs, Special Counsel for the DEA, Chris Gibson, Oregon HIDTA Director, and James Ferraris, Deputy Chief for the Salem, Oregon Police Department. Thank you all for taking the time to help analyze the data for this thesis. You guys are the best!

Lastly, and most important, I want to thank my wife, Ginny, and my sons, Matthew and Jacob. As of the writing of this paper, Ginny was supporting a graduate student (me), a senior at Oregon State University majoring in Mechanical Engineering (Matthew), and a freshman at Oregon State University majoring in Chemical Engineering (Jacob). Ginny graciously supported me throughout this process by editing papers, listening to me complain, and putting up with the sound of typing late into the night. I am truly blessed to have you guys in my life. I couldn't have done this without you.

I. INTRODUCTION

A. PROBLEM STATEMENT

Federal, state, local, and tribal law enforcement agencies have made great strides in sharing information with one another since the attacks that occurred on September 11, 2011. One of the mechanisms that many states and regions turned to in an attempt to accomplish this goal was the formation of fusion centers. Much has been written about the effectiveness and approach of many of these centers, but little has been detailed about the impact, or lack thereof, of how public enterprise fits into the puzzle. Do private corporations and businesses have a significant role to play in the fight against terrorism in the United States? Many law enforcement professionals think they play a critical role, and have attempted to integrate them directly into the fusion center intelligence cycle.

The U.S. Department of Homeland Security (DHS) and a number of think tanks and Congressional committees have weighed in on the topic of public and private partnerships with fusion centers. In 2006, U.S. DHS released a policy document entitled, *The National Fusion Center Guidelines,* and noted fusion centers should "involve every level and discipline of government, private sector entities, and the public."[1]

The consensus of government agency reports is that private industry and public-sector organizations play a critical role in homeland security.[2] There are three commonly cited reasons for this; private companies own the majority of the critical infrastructure in the United States and can provide expert analysis of vulnerabilities, private company security components can provide a mechanism to report suspicious activity to law enforcement, and partnerships with the private sector can provide law enforcement a direct conduit to educate employees regarding threats and propose mitigation strategies

[1] U.S. DHS -NFCG, *National Fusion Center Guidelines* (Washington, DC: U.S. Department of Homeland Security, 2006), www.it.ojp.gov.

[2] Ibid.

Establishing relationships between law enforcement entities and private partners is the best way to facilitate an open dialogue; thereby, increasing the probability companies will report suspicious activity to the police.[3]

The private sector can provide law enforcement and fusion centers assistance and services not traditionally utilized in criminal intelligence centers. This support can take the form of subject-matter experts in the fields of cyber security and computer operations, or sharing of data on critical infrastructures or business capabilities that could benefit command staff during response to a hazardous materials incident.[4]

The private sector owns or controls the great majority of the country's critical infrastructure, and therefore, has expertise on the risks and vulnerabilities to those properties and installations.[5] The U.S. Department of Homeland Security is required by federal law to evaluate vulnerabilities, disseminate advisories and bulletins, and coordinate with the private sector and state, local, and tribal agencies in an effort to effectively prevent, or respond to terrorist threats.[6] Therefore, partnering with representatives from key private industries would allow fusion center personnel to learn processes and operational capabilities, and apply that knowledge to develop strategies to mitigate threats.[7]

In 2006 and 2007, several Congressional committees requested information from state and local-operated fusion centers in an attempt to assess their operational capabilities and effectiveness. The Congressional Research Service surveyed forty fusion

---

[3] U.S. DOJ-ISE, *U.S. Information Sharing Environment, Guideline 2* (Washington, DC: U.S. Government, Office of the President, 2006), www.ise.gov.

[4] U.S. DHS -NFCG, National Fusion Center Guidelines.

[5] DHS-HSAC, Homeland Security Advisory Council, Private Sector Information Sharing Task Force: On Information Sharing between Government and the Private Sector- Final Report (Washington, DC: U.S. Department of Homeland Security, 2005).

[6] U.S. DOJ-NCISP, *National Criminal Intelligence Sharing Plan* (Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance, 2009), www.it.ojp.gov.

[7] U.S. DOJ-ISE, U.S. Information Sharing Environment, Guideline 2.

centers and issued several comprehensive reports on different aspects of fusion center operations and potential causes for concern.[8] [9]

The research and testimony provided to the committees echoed a number of the federal reports in highlighting the theoretical advantages of government and private-industry partnerships in fusion centers. The authors, however, were skeptical about the practical application of the recommendations and discovered most fusion centers were not making progress integrating private sector participants directly into the centers.[10]

The reasons outlined in the reports included law enforcement's lack of understanding and appreciation for the role the private sector could play in a fusion center, and the federal government's failure to provide a clear strategy.[11] Conversely, the private sector has major concerns about participating in a fusion center, including the fear of industrial espionage, exposing weaknesses to competitors, and a clear lack of government safeguards and protections.[12]

The American Civil Liberties Union (ACLU) is very concerned about the development of fusion centers, and addresses private partnerships directly in their report, *What's Wrong with Fusion Centers.*[13] The report states, "Some fusion centers incorporate private-sector corporations into the intelligence process, potentially undermining privacy laws designed to protect the privacy of innocent Americans, and increasing the risk of a data breach."[14]

---

[8] U.S. Library of Congress, Congressional Research Service, *Fusion Centers: Core Issues and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins., CRS Report RL34177 (Washington, DC: Office of Congressional Information and Publishing, September 19, 2007).

[9] U.S. Library of Congress, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Todd Masse., CRS Report RL34070 (Washington, DC: Office of Congressional Information and Publishing, September 2007.

[10] Siobhan O'Neil, "The Relationship Between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities," *Homeland Security Affairs Journal*, no. Supplement 2 (2008).

[11] Masse, O'Neil, and Rollins, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*

[12] Masse, O'Neil, and Rollins, *Fusion Centers: Issues and Options for Congress*, 5–7, 29, 55–56, 83.

[13] "More about Fusion Centers | American Civil Liberties Union," http://www.aclu.org/spy-files/more-about-fusion-centers (accessed 11/18/2011).

[14] Ibid.

Taking the current literature and direction from the federal government into account, the questions that arise are:

1. What are the fundamental components to be considered when developing a private partnership program for a fusion center?

2. What are the key operational components that make a program successful?

3. What smart practices can be employed when implementing a program for a small fusion center?

4. What are the advantages and limitations of the electronic systems fusion centers use to collaborate with program participants?

A number of fusion centers have initiated extensive private partnership and outreach programs that many intelligence practitioners believe only work under certain circumstances. For instance, many small fusion centers do not enjoy the luxury of having available staff to manage and engage with private sector outreach programs that require regular meetings and briefings. These types of programs take a tremendous amount of daily preparation, gathering of critical information to share with participants, and time and expense to arrange meeting space and facilities. Often times, only large, well-funded fusion centers can implement a program of that size and scope.

A number of outreach programs are centered on Fusion Liaison Officer (FLO), or Terrorism Liaison Officer (TLO) Programs. These programs often involve training a cadre of police officers or first responders to interact with members of the public and private sectors, usually arranged and sorted into groups corresponding to the U.S. Department of Homeland Security's eighteen critical infrastructure and key resource sectors.[15] The FLO programs present the same challenges to small fusion centers, especially when the small fusion center serves law enforcement agencies and jurisdictions that cover a large geographic area. Again, much has been written about these

[15] U.S. Department of Homeland Security, Integrating Critical Infrastructure and Key Resources Protection Capabilities into Fusion Centers, Development and Implementation Considerations, Version 1.0, (Washington, DC, U.S. Department of Homeland Security, April 2011).

programs, but little has been reported about the effectiveness and impact the programs bring the communities, considering the time and expense needed to initiate and sustain these programs.

This research will attempt to identify smart practices for implementing robust private partnership programs and attempt to customize a model program that addresses the unique needs of small fusion centers. Recognizing that many fusion centers have specific missions based on local needs and threats, these programs can take many forms, and aim to accomplish particular results and outcomes. Extensive research is needed to identify scalable programs that can be customized to fit the size, need, budget, and level of oversight available to allow the program to succeed and accomplish the stated mission of the particular center.

B. RESEARCH QUESTIONS

In light of the fact that many fusion centers have implemented programs with the sole purpose of engaging and interacting with public and private enterprise, this research will attempt to answer the following questions:

- What are the fundamental program components fusion center program managers consider when developing a successful private partnership program?
- What smart practices can be employed when implementing a program for a small fusion center?
- What are the advantages and limitations of the electronic systems fusion centers use to collaborate with program participants?

C. LITERATURE REVIEW

1. Introduction and Background

Law enforcement agencies have been forced to change the way they do business in the years following the 9/11 attacks, and the most significant example of this are the methods used to collect and analyze criminal intelligence. Prior to the 9/11 attacks, many metropolitan police departments operated a criminal intelligence unit in one form or

another. The main function of these units historically involved gathering data on gang members, organized crime figures, and suspected narcotics traffickers.

When the National High Intensity Drug Trafficking Area Program (HIDTA) was established in 1990, many of the existing units were enhanced and encouraged to collocate analysts and investigators from federal, state, and local agencies into a common office space. These "Intelligence Support Centers" were regional in nature, and agencies were required to collaborate within the space, produce strategic and tactical intelligence products, and provide an electronic mechanism to share this data with participating agencies within their region. This framework was extremely successful, as it allowed intelligence obtained from three levels of government to be "fused" together to create a common threat picture.

In the aftermath of 9/11, the National Commission on Terrorist Attacks upon the United States made a number of sweeping recommendations, one of which was that the intelligence community made mistakes and information sharing needed to drastically improve. In responding to this call to action, many states and large city police departments decided to create Terrorism Fusion Centers. These centers were similar to the HIDTA Intelligence Support Centers but had a wider collection and dissemination function, and incorporated additional partners relevant to the homeland security mission. The primary focus of these centers was terrorism intelligence, but many morphed into "all-crimes-all threats" platforms.

The U.S. Department of Homeland Security released a policy document entitled, *The National Fusion Center Guidelines,* and noted fusion centers should, "…involve every level and discipline of government, private sector entities, and the public…"[16]

This statement begs the following question: How should fusion centers and law enforcement agencies engage with, and share intelligence with public institutions and the private sector?

---

[16] *National Fusion Center Guidelines*, U.S. Department of Homeland Security, Washington, DC, 2006.

This literature review will examine publications and articles related to current relationships between fusion centers and the public and private sectors, and issues involving the assignment of non-law enforcement participants into fusion centers.

2. Findings and Claims

Much of the literature examined for this review falls into three broad categories: reports written by government agencies or government entities, reports or studies written for the U.S. Congress, or journal articles written to examine specific aspects of fusion centers and their capabilities.

3. Government Publications

The consensus of the government agency reports is that private industry and public sector organizations play a critical role in homeland security.[17] Establishing relationships between law enforcement entities and private partners is the best way to facilitate an open dialogue; thereby, increasing the probability companies will report suspicious activity to the police.[18]

The private sector can provide law enforcement and fusion centers assistance and services not traditionally utilized in criminal intelligence centers. This support can take the form of subject-matter experts in the fields of cyber security and computer operations, or sharing of data on critical infrastructures or business capabilities that could benefit command staff during response to a hazardous materials incident.[19]

The private sector owns or controls the great majority of the country's critical infrastructure, and therefore, has expertise on the risks and vulnerabilities to those

---

[17] *National Fusion Center Guidelines*, U.S. Department of Homeland Security, Washington, DC, 2006.

[18] *U.S. Information Sharing Environment, Guideline 2*, United States Office of the President, Washington, DC, 2006.

[19] *National Fusion Center Guidelines*, U.S. Department of Homeland Security, Washington, DC, 2006.

properties and installations.[20] The U.S. Department of Homeland Security is required by federal law to evaluate vulnerabilities, disseminate advisories and bulletins, and coordinate with the private sector and state, local, and tribal agencies in an effort to effectively prevent, or respond to terrorist threats.[21] Therefore, partnering with representatives from key private industries would allow fusion center personnel to learn processes and operational capabilities, and apply that knowledge to develop strategies to mitigate these threats.[22]

4. Reports for Congress

In 2006 and 2007, several congressional committees requested information from state and local-operated fusion centers in an attempt to assess their operational capabilities and effectiveness. The Congressional Research Service surveyed forty fusion centers and issued several comprehensive reports on different aspects of fusion center operations and potential causes for concern.[23,24]

These products echoed the federal publications in highlighting the theoretical advantages of government and private-industry partnerships in fusion centers. The authors however, were skeptical about the practical application of the recommendations, and discovered most fusion centers were not making progress integrating private sector participants directly into the centers.[25]

---

[20] Homeland Security Advisory Council, Private Sector Information Sharing Task Force*: On Information Sharing between Government and the Private Sector- Final Report*, U.S. Department of Homeland Security, Washington, DC, 2005.

[21] National Criminal Intelligence Sharing Plan, U.S. Department of Justice, Bureau of Justice Assistance, Washington, DC, 2009.

[22] *U.S. Information Sharing Environment, Guideline 2*. United States Office of the President, Washington, DC, 2006.

[23] U.S. Library of Congress, Congressional Research Service, *Fusion Centers: Core Issues and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins., CRS Report RL34177 (Washington, DC: Office of Congressional Information and Publishing, September 19, 2007).

[24] U.S. Library of Congress, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, by Todd Masse., CRS Report RL34070 (Washington, DC: Office of Congressional Information and Publishing, September 2007.

[25] Siobhan O'Neil, "The Relationship Between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities." *Homeland Security Affairs Journal*, Supplement 2 (April 2008).

The reasons outlined in the reports included law enforcement's lack of understanding and appreciation for the role the private sector could play in a fusion center, and the federal government's failure to provide a clear strategy.[26] Conversely, the private sector has major concerns about participating in a fusion center, including the fear of industrial espionage, exposing weaknesses to competitors, and a clear lack of government safeguards and protections.[27]

Siobhan O'Neil exposes serious concerns about private-public-government partnerships in her article, *The Relationship between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities*.[28] O'Neil examines the issues posed by an American Civil Liberties Union (ACLU) report criticizing fusion center partnerships as being reckless and labeling them a "bad idea." The group is fearful private companies will provide private information to the government without proper legal oversight and might use this leverage to gain an unfair business advantage over companies that do not participate in sharing initiatives.[29]

O'Neil's research indicates information exchange between the private sector and fusion centers is very infrequent, and usually occurs after a crime occurs or during an event, as opposed to the fusion center method of sharing intelligence before the event or crime occurs. O'Neil, however, worked to address many of the concerns raised by the ACLU when she reported many states have legal restrictions in place to protect private data, and law enforcement agencies are attempting to find ways to work with industry representatives in a way that protects civil liberties.[30]

5. Journal Articles

Many of the journal articles examined the role of a specific non-traditional fusion center partner, such as fire department and EMS personnel. The literature indicates

[26] Masse, "Homeland Security Intelligence."

[27] Masse, O'Neil, and Rollins, "Fusion Centers: Issues and Options for Congress."

[28] O'Neil, "The Relationship Between the Private Sector and Fusion Centers."

[29] Ibid.

[30] Ibid.

firefighters have a unique role in homeland security, as they are often in homes and businesses providing emergency aid, and in a position to see illegal or suspicious activity.[31] Firefighters expressed the desire to participate in the intelligence sharing process, as they routinely access areas not available to law enforcement and feel their role as "intelligence sensors" would be a valuable asset.[32]

Concerns raised about Emergency Management Services (EMS) personnel participating in fusion centers included the lack of significant discussion between the federal government and the medical community regarding best practices and negative perceptions the partnerships may invoke by the public.[33]

The benefits to the private sector may outweigh the theorized value to the intelligence community. Many fusion centers provide threat briefings and redacted publications to industry security professionals,[34] while some provide a desk and computer equipment to be used by company representatives during emergency situations.[35] Other benefits include access to training to help industry specific representatives learn how to identify suspicious activity and provide them with a secure mechanism to report. Additional training topics could include updates on terrorism planning trends and resources to assist them in creating emergency response plans.[36]

Anthony Newkirk has serious concerns about public-private partnerships and outlines several in his article in Surveillance & Society.[37] Newkirk believes fusion centers, if allowed to have close relationships with the private sector, will lead the country into a "surveillance state." Newkirk notes, "I argue that fusion centers,

---

[31] Bryan Heirston, "Firefighters and Information Sharing; Smart Practice or Bad Idea." *Homeland Security Affairs Journal* 6, no. 2 (May 2010).

[32] Michael Petrie, "Use of EMS Personnel as Intelligence Sensors: Critical Issues and Recommended Practices." *Homeland Security Affairs Journal* 3, no. 3 (September 2007).

[33] Ibid.

[34] Dave Shepherd, "Role of the Private Sector in Fusion Centers." *Security* 48, (January 2011).

[35] O'Neil. "The Relationship Between the Private Sector and Fusion Centers."

[36] Shepherd, "Role of the Private Sector in Fusion Centers."

[37] Anthony B. Newkirk, "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance after 9/11." *Surveillance & Society* 8, no. 1 (2010): 43.

decentralized intelligence-gathering activities mainly run by state and local police departments with federal and corporate support, are byproducts of the privatization of state surveillance and means of assault on civil liberties."[38]

In January of 2012, The National Infrastructure Advisory Council published one of the most comprehensive reports on the issue of private companies participating with the government on homeland security issues. The council is a panel of private-sector appointees that represent the 18 critical infrastructure and key resources (CIKR) sectors of American business enterprise. In their report titled, *Intelligence Information Sharing: Final Report and Recommendations*,[39] the council makes several key recommendations that include interaction with fusion centers and homeland security professionals. The report strongly endorses the relationships between companies and fusion centers and expressed concern the government is not going far enough in exploiting the programs.[40]

D. RESEARCH METHOD

This research will be conducted in three steps. The first step is a case study of three successful private partnership initiatives. During this first step, program managers will be interviewed in order to identify what they perceive as fundamental program components that make their programs successful. In addition, program managers will be asked about federally funded electronic collaboration systems to determine advantages and limitations of the system's functionality. Step two will involve convening a focus group of subject-matter experts to analyze the data collected from the interviews and to identify common operational components and smart practices employed by the programs. The subject-matter experts will be asked to analyze these programs to determine if they could be employed in a small fusion center, and to make recommendations regarding which operational components and strategies should be considered in creating a blueprint

[38] Anthony B. Newkirk, "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance after 9/11." *Surveillance & Society* 8, no. 1 (2010): 43.

[39] Alfred R. Berkeley, *Intelligence Information Sharing: Final Report and Recommendations.* Washington, DC: National Infrastructure Advisory Council, 2012.

[40] Ibid.

to establish a successful program. Lastly, step three will consist of evaluating the recommendations from the focus group to construct a model program blueprint that can be used by small fusion centers or intelligence units to establish a successful private partnership program.

The case study method is appropriate to identify the fundamental program components of successful fusion center partnership programs that can be effectively established in a small fusion center operation. A case study will focus on the identification of smart practices, communication strategies and funding mechanisms. This method will also be used to analyze the advantages and limitations of electronic systems used by fusion centers to collaborate with program participants. Quantitative analysis would not be an effective approach, as statistics and data would be difficult to produce in examining relationships, communication strategies, and key decision-making practices. Fusion centers come in many different sizes and configurations, and applying a qualitative approach to compare programs in an attempt to explain why a program is successful, or why a program appeals to a particular program participant, would not be realistic.

1. Data Sample

The three cases selected for this study are the Orange County Shield, the InfraGard Los Angeles Program, and Colorado's RUBICON program.

Several fusion center directors and law enforcement executives recommended examining these programs because they have been widely recognized as successful, unique, and encompass a variety of participants and strategies. These programs have many things in common but also employ unique program features worth investigating. For instance, a different level of government operates each program: one federal, one state, and one county. Two programs encompass large metropolitan areas; the third's jurisdiction is an entire state, and all three use different techniques to communicate with program participants. All programs have gone through rough times and had functions that failed or did not work properly, causing program managers to re-evaluate processes and utilize subject-matter experts from other state and federal programs to improve their

approach. Lastly, all three use different funding mechanisms to sustain their operations, and one uses private funding to offset operational costs.

2. Data Collection

Data will be collected regarding fundamental operational components of each private partnership and how decisions were made from an executive level to design and implement the program. Information will be gathered on how participants were originally selected, how management determined what communication and collaboration systems to use, and what processes failed and which ones worked and why.

This thesis will also focus on analyzing the process managers and planners use to select particular infrastructure sectors to work with.

Lastly, collecting information about the method agencies used to obtain funding, and how they plan to sustain operations in difficult budget environments will be addressed. This is especially critical for small fusion centers with limited funding and operational space.

Subject-matter experts (the program managers) will be interviewed to gather the majority of data mentioned above. These managers from the selected samples will be interviewed regarding communication techniques, identifying participants, security arrangements and background checks, and the process for disseminating sensitive data to participants.

Program managers are key to this study, as they are in the position to fully understand the internal components of the program. Managers understand how and why the program was designed, what information is exchanged, how individual relationships effect the operations, and what it takes to fund and sustain the program.

See Appendix A for a list of interview questions.

3. Data Analysis

The data collected for this thesis will be analyzed in a unique fashion. A focus group of subject-matter experts will be assembled consisting of three current law

enforcement executives. Each member has extensive experience in managing grant programs, participating on executive boards, and overseeing multi-agency initiatives. In addition, all three members represent different sectors of the criminal justice profession. One is currently an Assistant Chief from a large metropolitan police department, one is a Director of a National Counterdrug Grant program, and the third is a General Counsel Attorney working for a federal drug enforcement agency.

The data collected during the interviews will be sorted and divided into a number of core categories representing operational functions of the individual programs. The data will be presented to the focus group in a "blind review format," and members will not know the name of the program or the person from where the data was collected.

Data will be sorted into the following categories:

- Background Information
  - Size of the program (number of participants)
  - Goal of the program (Intelligence Gathering/Situational awareness/ Training
  - Key features
  - Geographic scope
- Costs and Funding
  - Total start-up cost
  - Continuing operational costs
  - Funding source
  - Funding sustainment strategy
- Participation
  - Total fusion center employees needed to manage the program
  - Type of companies targeted for participation
  - How participants are chosen

- Operations
  - Security protocols and background checks
  - Structure of the program (In fusion center/virtual/ live meetings)
  - Collaboration tool used
  - Communication methods used
  - Tip and leads management method
  - Information dissemination strategy
  - Types of products and publications produced
  - Marketing method and strategy
  - Policy documents and agreements
  - Statistics and reporting
  - Type of program oversight
  - Employee Management and Relationships
- Lessons Learned
  - Avoiding Mistakes

The focus group will be asked to analyze the sorted data and identify the components and other critical functions that they determined made the sample programs successful. It is possible that individual components and their functionality in relationship to a successful program could overlap, or affect one of the other components. This topic will be discussed with the panel, and components that are identified as being critical or distinctive in relation to other functions will be explored and reported.

The focus group will be important to this study, as they can observe the program independently, and attempt to understand how programs compare to one another without emotional attachment or bias. In addition, these experts understand the goals and requirements outlined by the Department of Homeland Security, and how each program fulfills fusion center baseline capability requirements.

Lastly, the panel will be asked to identify “smart practices” that the author will use to make recommendations that can be used as a blueprint by managers representing small fusion centers, intelligence programs, or rural law enforcement agencies preparing to implement a private partnership program.

II. FUSION CENTER OVERVIEW

A. WHAT IS A FUSION CENTER?

For a well-rounded understanding of the purposes of this research, it is important to understand what a fusion center is, how fusion centers operate, and how they currently interact with public and private entities.

The history of fusion centers begins in the early-1990s, when many metropolitan police departments operated a criminal intelligence unit in various forms. Historically, the main function of these units involved gathering data on gang members, suspected narcotics traffickers, and organized crime figures.

When the National High Intensity Drug Trafficking Area Program (HIDTA) was established in 1990, many of the existing intelligence units were enhanced and encouraged to collocate analysts and investigators from federal, state and local agencies into a common office space. These "Intelligence Support Centers" were regional in nature, and participants were required to share criminal intelligence within the space—then disseminate publications and products to program initiatives in their region. This framework allowed intelligence obtained from three levels of government to be "fused" together to create a common threat picture. For instance, intelligence gathered by detectives from a local police department can be compared to information on file at the local Federal Bureau of Investigation (FBI) office. An FBI analyst assigned to the fusion center can conduct a custom query and share the results with special agents assigned to the Joint Terrorism Task Force. Prior to the advent of fusion centers, common intelligence gathering by local agencies was rarely shared with federal agencies, and many connections are criminal commonalities that were probably missed.

Between 2003 and 2007, direction from the Office of the President and the 9/11 Commission led many states and large city police departments to create Terrorism Fusion Centers. These centers were similar to the HIDTA Intelligence Support Centers but had a wider collection and dissemination function, and incorporated additional partners relevant

to the homeland security mission. The primary focus of these centers was terrorism intelligence, but many morphed into "all-crimes-all threats" platforms.

In 2005, the United States Bureau of Justice Assistance (BJA) and the United States Department of Homeland Security published the seminal document on fusion centers and fusion center operations. This document, formally titled, "*Fusion Center Guidelines*,"[41] is a series of formal recommendations and guidelines distributed to fusion center managers and agencies in an attempt to standardize fusion center operations across the nation. According to the guidelines; the formal definition of a fusion center is as follows:

> A Fusion Center is a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity.[42]

The primary function of a fusion center is to act as a centralized operations center where information can be collected from a myriad of sources, analyzed by a cadre of professionally training criminal intelligence analysts, then disseminated to first responders, investigators, and other participants in an effort to anticipate, identify, prevent and monitor criminal activity.[43]

The principal leadership role in most fusion centers is handled by a law enforcement agency. Most centers are operated by a state law enforcement agency (such as a state police department or Attorney General's Office), however, a number of large metropolitan agencies host centers, as does the Federal Bureau of Investigation.

Each fusion center has been custom designed to meet the investigative needs of the agencies and customers with the given region. For this reason, each center has unique

---

[41] *Fusion Center Guidelines*, United States Bureau of Justice Assistance (BJA), the United States Department of Justice, and the United States Department of Homeland Security, Washington, DC, July 2005.

[42] Ibid., 3.

[43] Ibid.

characteristics, participants, and programs that work together to fulfill the mission, but all centers operate under a consistent framework called the *Fusion Center Baseline Capabilities*.[44]

The *Fusion Center Baseline Capabilities* were released by the United States Department of Homeland Security in 2008 and provide an operational blueprint for fusion centers to follow in an effort to standardize operations nationwide.[45] The document describes and recommends a "baseline level of capabilities" for fusion center management to implement in the areas of planning and requirements development, information collection, intelligence analysis and dissemination, management and governance, security procedures, personnel and training, technology, and information privacy protections.[46] . Department of Homeland Security determined that standardizing the basic functions of fusion centers would allow fusion centers to work together more efficiently and provide customers a standardized platform of service delivery regardless of the jurisdiction. It is a tribute to the fusion center community that the vast majority of the recognized state and regional fusion centers have met the minimum standards set forth in the baseline capabilities policy. U.S. Department of Homeland Security requires centers to report their progress on baseline and advanced functionality every year and grades each center on their performance. In addition, DHS provides technical workshops, live training, and special programs to assist fusion center management in reaching their goals of obtaining baseline capability certification.

B. TYPES OF FUSION CENTERS

Most fusion centers are hosted by a state or local law enforcement agency. The FBI also hosts a number of large regional fusion centers. Fusion centers are funded in a variety of ways: Urban Area Security Initiative (UASI) federal grant funding, the State Homeland Security Grant, and direct federal or local funding. Regardless of the funding

---

[44] *Baseline Capabilities for State and Major Urban Area Fusion Centers*, United States Department of Homeland Security, and the United States Department of Justice, Washington, DC, September 2008.

[45] Ibid., 1.

[46] Ibid., iii and chapter overviews.

source, most fusion centers operate in a similar fashion, with the scale of programs hosted by the center being the main difference. Generally, there are two main types of fusion centers—full-service fusion centers and intelligence clearinghouse centers.

Full-service fusion centers[47] usually have a full compliment of criminal intelligence analysts who provide tactical analytical case support and strategic analytical products, such as situational awareness bulletins, threat assessments, and officer safety alerts. Many of these centers, due to their size and large budgets, are also able to provide office space for nontraditional partners, such as firefighters, public health officials, private security personnel, and other federal, state and local law enforcement staff.

In addition to analysts, full-service fusion centers have a full-time, collocated investigative capability within the center. For instance, the ACTIC has a FBI JTTF investigative team attached to the center that conducts counterterrorism investigations.

The third component of most full-service centers is the presence of a robust Terrorism Liaison Officer Program. These programs, now called Fusion Liaison Officer Programs (FLO Programs), enlist a cadre of police officers, firefighters, and other first responders to provide an emergency response element that provides a live connection to major incidents and emergency command centers.

The intelligence clearinghouse fusion centers[48] often do not conduct criminal investigations directly from the center, but instead operate as a criminal intelligence support mechanism for other federal and local agencies. Many of these centers are similar to the pre-9/11 criminal intelligence units, but now offer assistance and support on counterterrorism efforts.

Because these centers do not have an investigative component, most act as a regional clearinghouse for investigative tips, leads, and criminal intelligence. This service is usually in direct support of a regional FBI JTTF operation. Many intelligence

[47] Arizona Counter Terrorism Intelligence Center (ACTIC), NY State Fusion Center, and the Los Angeles Joint Regional Intelligence Center (JRIC).

[48] Oregon TITAN Fusion Center, Orange County Intelligence Assessment Center, Northern California Regional Intelligence Center.

clearinghouse centers host a criminal intelligence database and the U.S. Department of Homeland Security's Homeland Security Information Network (HSIN) to assist state and local law enforcement investigators and first responders communicate sensitive data between agencies.

Similar to full-service centers, clearinghouse centers usually provide tactical and strategic analytical support, and many host Fusion Liaison Officer (FLO) and Critical Infrastructure Protection Programs.

C. FUSION CENTER SPECIAL PROGRAMS AND FEATURES

Based on the mission and operational scope, many fusion centers provide special programs and services for their customers. The following is a synopsis of the most popular programs:

Fusion Liaison Officer Programs, formally called Terrorism Liaison Officer Programs, are programs designed to facilitate the exchange of information between fusion centers and their customers.[49] These customers can include other law enforcement officers and investigators, public sector organizations, such as departments of heath, fire departments, and Child Welfare Departments, and private sector individuals and businesses.

Typically, fusion centers recruit and train individuals who have an interest in becoming a formal liaison between the fusion center and their agency. The majority of the participants are law enforcement officers, but many FLO programs include firefighters, corrections officers, National Guard Soldiers, and some include private citizens. Individuals usually participate on a part-time basis, but a few large fusion centers (Arizona ACTIC) have full-time members who are funded by federal grant programs.

[49] *Establishing a Fusion Liaison Officer Program, Development and Implementation Considerations,* U.S. Department of Homeland Security, U.S. Department of Justice, Fusion Process Technical Assistance Program and Services, Washington, DC, August 2010, version 1.2.

The core mission of the FLO is to act as a liaison between the fusion center and the entity represented by the "officer." The role of the officer can take many forms, but the primary responsibility is to establish a formal information exchange between the two entities. This can be in the form of verbal briefings, electronic information exchange, or by formal published documents and briefings produced by the fusion center. The information can include terrorism and criminal activity indicators and threats, officer safety information and warnings, and basic security tips and procedures. The underlying theory for this exchange of information is that if first responders and the public are educated on how criminals and terrorists operate and accomplish their attacks, they can become "force multipliers" and report suspicious activity through their FLO or local law enforcement agency to help detect, deter and prevent crimes and specifically, terrorist threats.[50]

One of the key responsibilities of the FLO is to deliver situational awareness training to their respective agency or organization.[51] This training, in coordination with the fusion center, can be general or specific in nature depending on current threats and investigations. It is critical that first responders understand what terrorism is and what a terrorist must do to accomplish an attack. This can include information about the terrorism planning cycle, illegal fundraising, obtaining dangerous chemicals and explosive materials, and religious extremism indicators. This knowledge, combined with information and experience gained in the workplace, can mentally prepare first responders to see and recognize threats and indicators of terrorist activity.

These training events can also be used as direct intelligence collection points. For instance, if the fusion center is assisting with a terrorism-related investigation, the FLO can brief the training recipients and ask them for specific information about suspects or

[50] *Establishing a Fusion Liaison Officer Program, Development and Implementation Considerations*, U.S. Department of Homeland Security, U.S. Department of Justice, Fusion Process Technical Assistance Program and Services, Washington, DC, August 2010, version 1.2, 4.

[51] Ibid., 79.

related criminal activity in the area. This request for information can lead to tips and other valuable information that can be funneled directly to the fusion center for inclusion in the investigation.

Some fusion centers deploy FLOs to major incident sites to act as the liaison between the command post and the fusion center. This direct link can provide both sides with valuable resources and services that are unavailable without an on-site participant. For instance, the FLO can request information and intelligence directly from the fusion center about known criminals, criminal activity, chemical storage locations, and building elements, and provide that to on-scene commanders. Conversely, the FLO can pass information to the fusion center regarding the incident that can be shared with other local agencies affected by the incident and even the federal government for situational awareness. Lastly, some FLO programs train their officers to have the ability to assist or conduct threat and vulnerability assessments on public and private buildings and structures.[52]

1. Training Programs

As highlighted by the fusion liaison officer programs, training and situational awareness is a primary function of many fusion centers. Most fusion centers regularly organize and host training seminars and conferences for first responders and intelligence professionals that focus on many topics associated with terrorism and crimes that support terrorism. For example, fusion centers have provided training on the subjects of: criminal intelligence sharing, critical infrastructure protection, financial crimes that support terrorism, illegal charitable fundraising in support of terrorism, basic and advanced terrorism investigation techniques, criminal intelligence analysis, surveillance techniques, and many more. Many fusion centers rely on the federal government, the FBI, U.S. DHS, and the U.S. Justice Department to provide accessible, low-cost training for their staffs and customers.

---

[52] *Establishing a Fusion Liaison Officer Program, Development and Implementation Considerations,* U.S. Department of Homeland Security, U.S. Department of Justice, Fusion Process Technical Assistance Program and Services, Washington, DC, August 2010, version 1.2, 78.

One of the key partners in providing this training is the United States Bureau of Justice Assistance (a department within the Department of Justice) that administers the State and Local Anti-Terrorism Training Program (SLATT). This program is specifically designed to provide cutting-edge training to state, local, and tribal law enforcement executives, command personnel, patrol officers, intelligence officers, investigators, analytical personnel, and prosecutors.[53] State and Local Anti-Terrorism Training trainers are subject-matter experts and provide comprehensive training on the subjects mentioned above, and also host "train-the-trainer" programs to teach FLO program participants and first responders how to train others in terrorism-related topics.

2. Critical Infrastructure and Key Resources Programs (CI/KR)

The fusion center role in the protection of critical infrastructure has evolved over the past five years. Many fusion centers now take an active role in these programs, and often manage the programs and act as a partner to the federal government in electronically tracking these critical assets.

The official definition of critical infrastructure is:

> An asset, systems, and networks, whether physical or virtual, so vital to a community and/or the United States that the incapacity or destruction of such assets, systems, or networks would have debilitating impacts on the community's or the country's security, continuity of government, continuity of operations, public health, public consciousness, or a combination of these effects.[54]

An example of critical infrastructure is the western power grid, a military base, or a police station.

---

[53] *State and Local Anti-Terrorism Training Program,* United States Department of Justice, Bureau of Justice Assistance, Official Agency website: https://www.slatt.org/SLATT/On-Site_Training, accessed 8/24/12.

[54] Integrating Critical Infrastructure and Key Resources Protection Capabilities into Fusion Centers, Development and Implementation Considerations, U.S. Department of Homeland Security, U.S. Department of Justice, Fusion Process Technical Assistance Program and Services, Washington, DC, April 2011, version 1.0.

The official definition of a Key Resource is:

> A publicly or privately controlled resource essential to the minimal operations of the economy and government.[55]

An example of a Key Resource is a local airport, a state college, or a bridge spanning a large river.

Fusion centers have designed customized programs to assist their state's Office of Emergency Management, or Office of Homeland Security, in providing a central repository of threat information, tactical and strategic analytical support, and the ability to conduct CI/KR vulnerability assessments.[56]

Several fusion centers manage a team of individuals who work with public and private sector building and security professionals to conduct the full-spectrum vulnerability assessments. For example, the Colorado Rubicon Team, managed by the Colorado Information and Analysis Center, is comprised of Troopers from the Colorado State Police who identify and assess the state's CI/KR assets.[57] The team conducts on-site inspections to help identify vulnerabilities and recommend mitigation strategies to reduce potential loss of life, property damage, and economic damage caused by crime, natural disasters, and acts of terrorism.[58]

One of the key features of a robust CI/KR program is the ability to store and retrieve data collected during the threat and vulnerability assessments. The Automated Critical Asset Management System (ACAMS) program[59] is a web-enabled database

---

55 U.S. Department of Homeland Security, U.S. Department of Justice, *Fusion Process Technical Assistance Program and Services Integrating Critical Infrastructure and Key Resources Protection Capabilities into Fusion Centers, Development and Implementation Considerations*, Washington, DC, April 2011, version 1.0., 103.

56 Ibid.

57 Ibid.

58 Ibid.

59 Automated Critical Asset Management System, U.S. Department of Homeland Security, Washington, DC, Official Agency website: http://www.dhs.gov/automated-critical-asset-management-system-acams, accessed 8/24/12.

system that provides agencies a set of tools to collect and use critical infrastructure data, assess a structure's vulnerabilities, and develop incident response and recovery plans.[60]

One of the key uses for the ACAMS system is in coordination with the FLO critical response programs described earlier. A first responder, trained by a fusion center in FLO operations, can respond to the scene of a disaster or incident and obtain web access to the ACAMS database. Once accessed, information stored in the database can help incident commanders make decisions about the integrity of the building, where dangerous chemicals might be stored, and even access floor plans and photographs of the building and surrounding structures.

3. Suspicious Activity Reporting

After the events of 9/11, many law enforcement agencies struggled to make the reporting of crime more efficient. In addition, officials came to realize that reporting crime, in and of itself, were not providing criminal intelligence analysts with enough information to produce valuable predictive intelligence products. Typical crime reports were facts, and witness accounts of criminal activity after the event, had actually occurred. What was needed was information and intelligence regarding criminal activity prior to the crime occurring. Law enforcement agencies desired a comprehensive national system to collect, store, and disseminate "suspicious activity, tips, and leads" that could be used to compare incidents and data from across local, state and federal jurisdictional boundaries, in an effort to proactively prevent crime. To answer this demand, the U.S. Department of Homeland Security developed the "If You See Something, Say Something" campaign.[61] The working components of this program are twofold; a system

[60] Automated Critical Asset Management System, U.S. Department of Homeland Security, Washington, DC, Official Agency website: http://www.dhs.gov/automated-critical-asset-management-system-acams, accessed 8/24/12.

[61] *If You See Something, Say Something Campaign*, United States Department of Homeland Security, Washington, DC, Official Agency website: http://www.dhs.gov/if-you-see-something-say-something-campaign, accessed 8/27/12.

of databases and software used to collect and store data, and a public relations campaign to educate the public on the process of how to report suspicious activity to law enforcement.

Fusion centers have taken an active role in this program and many host the computer servers and databases within their operations. The software package allows citizens to access the system via a web-portal, and enter suspicious activity directly into the program. Police dispatch personnel and intelligence center research analysts that receive tips and lead via the phone, email, or other social media systems, can also enter data directly into the system. Once the data has been entered, key fields in the database can be automatically linked with similar data that physically resides in other states and jurisdictions. When data matches preset criteria, officials in the effected state, DHS, and the FBI can be notified of potential matches at which time an analyst or agent can be assigned to research the information more thoroughly.

This system is currently being established in most states, and it will take several years to understand and measure the program's effectiveness and impact on criminal investigations.

4. Special Events Support

One of the operational advantages of a fusion center is the access employees have to valuable criminal justice information. For this reason, fusion centers have become valuable resources during special events and large-venue gatherings.

Many fusion centers offer special events support by establishing an "information command post" at the event site, and provide a myriad of services to the host agencies. As an example, the Eugene Oregon Police Department was responsible for the security management of the 2012 United States Olympic Track and Field Trials, held at Heyward Field in Eugene, Oregon. The Oregon TITAN Fusion Center assisted Eugene PD by staffing their command post with four criminal intelligence analysts. These employees were able to access criminal intelligence databases, law enforcement database, electronic mapping systems, and Closed Caption Television Systems, to provide real-time information and support to agents and officers within the event site.

In addition to on-scene assistance, fusion center analysts and staff can provide strategic intelligence products to event managers. These products can include threat assessments, comprehensive site maps, and if the state integrates a CI/KR program in their fusion center, they can provide insightful information about critical facilities in and around the event site.

5. Watch Centers

Many fusion centers host a "watch center" function. A watch center is usually a 24/7 operation that provides critical information and research capability for investigators and first responders accessed via phone, email, or electronic communication system.

Watch center staff, as mentioned above, has access to a myriad of criminal intelligence, law enforcement, and public information databases for the purpose of conducting in-depth research on a subject, organization, or illegal enterprise. One of the core functions of a criminal investigation is researching the background of all subjects involved in the case, including witnesses, known criminals, and other associates related to the suspects. Criminal investigators and first responders need to know if a subject has a violent history, has attacked or fled from police officers in the past, or has a history of dangerous drug use. Having this information in advance can enhance the investigator's approach to interviewing the subject, allow the investigator to have additional assistance, if there is a safety concern, and allow law enforcement managers and prosecutors the ability to strategize a proper investigative approach the case.

Watch centers also play an important role by providing investigators and first responders with a "deconfliction" tool or program. Deconfliction is a law enforcement technical term for "active tactical sharing" of time sensitive investigative operations. Most criminal intelligence databases today have both a "subject deconfliction" and an "operational deconfliction" function that allows investigators to enter a subject or an operation, and receive notification, if another agency has an operational interest in the case. For instance, if a detective is investigating a subject, he or she could call a watch center and have the analyst conduct a deconfliction search. If the query matches a previously entered subject, the analyst will notify the detective who originally entered the

subject, and introduce both detectives to one another. The goal of the program is to create an investigative partnership or network to allow a more efficient, comprehensive investigation to ensue.

6. Equipment Loan Programs

One of the most valuable services hosted by fusion centers are technical equipment loan programs. These programs pool valuable resources to purchase expensive surveillance and tracking equipment, and then loan the items out to agencies to assist in investigations and security operations.

Most equipment loan programs purchase overt and covert video camera equipment, digital handheld video cameras, undercover body wires systems, electronic satellite tracking beacons, and Title III wiretap equipment and software.

These items are often difficult to purchase for small agencies, and often take highly trained technicians to install and operate. The pooling of the equipment, and the centralization of the technical experts, saves enormous amounts of money for agencies that take advantage of the service.

7. Products and Publications

One of the core responsibilities of a fusion center is strongly worded in Fusion Center Baseline Capabilities, Section 1.E, where it states, "Fusion centers shall develop a high-level dissemination plan that documents the procedures and communication mechanisms for the timely dissemination of the center's various products to the core and ad hoc customers."[62]

Producing intelligence products, such as threat assessments, criminal organization charts, criminal time-lines, and other strategic event warnings and bulletins is a core

[62] *Baseline Capabilities for State and Major Urban Area Fusion Centers*, United States Department of Homeland Security, and the United States Department of Justice, Washington, DC, September 2008.

function of the criminal intelligence analyst. But, these products are only useful if they reach the intended customer for use in planning criminal investigations or creating a security strategy.

Therefore, most fusion centers publish a number of products on a regular, and ad hoc basis. For instance, the Oregon TITAN Fusion Center publishes a weekly threat bulletin that is distributed to over one thousand first responders, investigations, and law enforcement executives statewide. The bulletin contains sections on terrorism-related events worldwide, officer safety information, gang-related information, investigative training opportunities, and a section on wanted subjects.

In addition to the weekly bulletin, the center coordinates and distributes critical event and time-sensitive warning and event alerts in real time. If an amber alert occurs, or if a bank robbery is reported, the fusion center gathers all the pertinent information and creates a professionally designed bulletin and distributes it immediately to all participating agencies. Alerts can contain information about missing persons, crimes that have just occurred, critical officer safety and public safety information, and criminal threat information.

8. The Role of the Criminal Intelligence Analyst

As mentioned above, the central operating function of any fusion or intelligence center is the criminal intelligence analyst. This profession differs greatly from the better-known function of a "crime analyst" whose sole function is to study crime and crime trends, and report that information to department decision makers.

The criminal intelligence analyst is a highly trained research and coordination professional whose value has been rightly elevated since 9/11. The typical function of an analyst in a fusion center revolves around the intelligence collection process and the search for relationships between subjects, organizations, and criminal activity.[63] Many analysts are assigned tactical case support to ongoing criminal investigations, and provide

[63] *Intelligence 2000: Revising the Basic Elements, A Guide for Intelligence Professionals*, The International Association of Law Enforcement Intelligence Analysts and the Law Enforcement Intelligence Unit, Sacramento, CA, 2000, 60.

assistance in coordinating the case, and producing analytical charts consisting of illegal holdings and interests of known criminals, money laundering patterns, telephone toll analysis and the research of associates and other criminal organizations.[64]

The need to disseminate valuable investigative and threat information is important in today's criminal justice world because situational awareness and education of first responders and the public is important in helping law enforcement to identify and prevent terrorism. For this reason, the criminal intelligence analyst must be able to write effectively and publish their products in a professional, easy-to-understand format that can be examined and evaluated by law enforcement professionals and private citizens alike.

Lastly, the criminal intelligence analyst must be able to communicate effectively, and play the role of central coordinator of all information coming into, and out of the fusion center. As we will highlight in Chapter IV, the ability to communicate and interact with all types of business and government officials is important to the success of fusion centers, and public and private partnership programs.

D. FUSION CENTER COMMUNICATION TECHNIQUES

As mentioned in a previous section, fusion centers are uniquely designed to fit the mission and goals of the jurisdictions they serve. This holds true for how fusion centers communicate with nontraditional law enforcement partners such as private company representatives. Many fusion centers house civilian employees who represent private businesses and public agencies directly in the fusion center. For example, large fusion centers commonly accommodate fire fighters, public health professionals, corrections staff, private company security professionals, and other "nontraditional law enforcement partners" within the center. Unfortunately, some centers are unable to do so due to legal restrictions and the lack of space or funding, so they need to utilize electronic mechanisms to communicate with their partners.

---

64 *Intelligence 2000: Revising the Basic Elements, A Guide for Intelligence Professionals*, The International Association of Law Enforcement Intelligence Analysts and the Law Enforcement Intelligence Unit, Sacramento, CA, 2000, 60–61.

When these participants are located directly in the fusion center, all employees (including law enforcement agents and analysts) are typically vetted and must complete a formal background check by the host law enforcement agency. In some instances, many of these employees receive a clearance by either the FBI or DHS, equal in authority to an FBI Secret Clearance.

Once the participant receives a clearance and is approved to operate within the center, that person can communicate and receive information and intelligence products in the same fashion as other sworn employees working in the center. But when circumstances arise that makes it difficult to house the employees directly in the center, management needs to find electronic mechanisms, or other more traditional methods, to exchange threat information and notify participants of important events.

Fusion centers employ a combination of techniques and strategies to communicate nontraditional law enforcement partners, and other valuable participants by hosting regularly scheduled meetings and briefings, and by using an electronic collaboration system. Most fusion centers use one, or a combination of four electronic systems to communicate with private, public, and law enforcement employees working with the center. These systems are the Homeland Security Information System (HSIN)[65], the FBI Infragard System[66], RISS.net Intelligence Sharing Systems[67], and custom-built fusion center websites.

1. Homeland Security Information Network (HSIN)

The Homeland Security Information System is a United States Department of Homeland Security sponsored electronic collaboration system. Homeland Security

65 *Homeland Security Information Network*, United States Department of Homeland Security, Washington, DC, Agency website: http://www.dhs.gov/homeland-security-information-network, accessed 8–31–12.

66 *FBI Infragard System*, United States Federal Bureau of Investigation, Washington, DC, Agency website: http://www.infragard.net/, accessed 8/31/12.

67 *Regional Information Sharing Systems (RISS)*, Murfreesboro TN, Agency website: http://www.riss.net/, accessed 8/31/12.

Information Network is accessed via the Internet by vetted law enforcement employees and private company representatives who are allowed access via fusion center or law enforcement agency sponsors.

The HSIN "portal" is segmented into two main sections, a law enforcement-only section and a public portal. Even though the public portal title might suggest that all members of the public have access, this is not the case. Each state is granted a HSIN law enforcement administrator, usually a manager in a fusion center or intelligence unit. The administrator has the duel role of marketing the system to potential law enforcement and public customers, and issuing encrypted electronic tokens to vetted users. Law enforcement and public users are chosen carefully based on an operational need-to-know basis.

The law enforcement membership access is simple, if you work in a fusion center or intelligence unit, or in a capacity needing terrorism or homeland security information, you can be granted access.

The public access portal is managed more stringently. Public members are chosen based on a criteria outlined by fusion center management in consultation with HSIN policy representatives. Once public participants are selected, the HSIN administrator grants access by issuing a token and an electronic certificate that resides on the user's computer. The user then logs onto the system by entering a user name and password stored and controlled by the HSIN administrator. Upon entering the HSIN site, the public user has access to FOUO (For Official Use Only) and Open Source documents posted by the HSIN administrator, fusion center staff, and U.S. Department of Homeland Security analysis staff. Law enforcement and criminal justice users have access to more sensitive documents in addition to the FOUO and Open Source Content.

HSIN contains thousands of homeland security related documents, threat bulletins, training information, legal briefs and court decisions primarily focused on terrorism issues, but other related crimes and information are also contained within the site.

Aside from document sharing and training information, the HSIN site is designed to act as a collaboration tool. The site allows users to host meetings via an interactive message board that allows for live video conferencing and instant messaging. HSIN also has the capability to allow users to set up segregated work areas for special events that enable participants to exchange information, video, documents, and calendars specifically tailored for the event. So, if a user wanted to host a special site to organize and collaborate during a major event, the user could set up the site, invite law enforcement, public and private sector users, and use the site as an emergency operations communication tool with a minimum level of effort.

Another example of an increasing popular way to use the HSIN public portal is provided by the Oregon TITAN Fusion Center. Oregon creates a separate portal for each U.S. DHS designated critical infrastructure sector and assigns access to vetted public participants directly into the sector matching their employment. The center then posts sector-specific information and publications on the portal and invites comments and additional documents and postings from the participants, creating a "community" approach to exchanging information within a sector.

Based on the numerous features, and the functional design enabling a wide range of communication techniques, the HSIN system is becoming the most popular way for fusion centers and intelligence units to interact with the private sector and their wide variety of customers and partners.

2. INfraGard

The InfraGard program is a nonprofit organization, acting through the auspices of the Federal Bureau of Investigation, to provide a mechanism for the private sector to interact with the FBI. The goal of the program is to encourage private businesses to exchange information with law enforcement through trusted partnerships and the use of the electronic collaboration provided by the FBI.

The FBI, often partnering with state and local law enforcement agencies and fusion centers, coordinates the program through local field offices. Similar to the HSIN program, the FBI assigns a program coordinator, usually a FBI Special Agent, to oversee

and administer the program at the local FBI field office. Individual participants are vetted when they register through the electronic collaboration tool. The vetting occurs with FBI oversight, but this role is administered through an academic partnership with Louisiana State University, who provides staff to coordinate the registration process and conduct background checks on the public applicants.

The local programs are custom designed to meet the needs of the customer base, but usually involve two central features: regularly scheduled training and information sharing meetings, and the use of the InfraGard electronic collaboration tool.

Fusion Center Directors and program managers interviewed for this thesis indicate that regularly scheduled information sharing meetings are the bedrock of their programs. These meetings allow program participants to interact with the FBI agents from the local offices, state and local law enforcement officials, and to receive briefings and training provided by the program. The main goal of the training function is to give the private sector members the information and situational awareness they need to recognize a threat to their respective business enterprise. The program also recognizes that employees of a private business, and specifically security guards and investigators, are the best people to recognize suspicious behavior within their business. The program gives these specific individuals special training and information to build on that local experience and expertise, and to help them identify suspicious behaviors that would be of interest to the FBI to combat terrorism or other serious crimes.

The InfraGard electronic reporting tool is designed differently than the HSIN tool, as its main function is to provide participants with a mechanism to report a perceived threat or suspicious activity to the FBI. Members can log into the system and fill out a specifically designed form to report any type of suspicious activity occurring within their business. This information is routed to a central collection center in Washington, DC, evaluated by an analyst or special agent, and then routed to a local FBI field office or JTTF investigation team for follow-up. If the information does not rise to the level needing immediate investigation, the information can be archived and compared against future tips and leads, which could form the basis for a formal investigation.

3. Regional Information Sharing Systems (RISS)

The RISS system is a collection of regional criminal intelligence sharing programs, located in six distinct regions of the United States. Each program encompasses five to seven states, and hosts a centrally operated criminal intelligence database that connects to the other five databases through a center located in Murfreesboro, Tennessee.

The overall program is funded by a grant administered by the United States Justice Department's Bureau of Justice Assistance. The Bureau of Justice Assistance administers the grant and operates the technical aspects and database design functions in Murfreesboro. The program is different from other federal programs, as it provides funding to the individual regional systems that are then overseen by individual executive boards that hire and support a director responsible for the day-to-day operation of the regional program.

As an example, the Western States Information Network (WSIN) is a RISS regional program located in Sacramento, California. The Western States Information Network regional partners include the states of Oregon, Washington, California, Hawaii, and Alaska. Each state participant is required to provide two executive board members, usually from the state police, and a large metropolitan police department respectively. The board meets regularly, oversees the performance of the appointed director, and approves budgets and operational programs.

Each program is required to host a number of law enforcement investigative support programs, including the operation of a centralized criminal intelligence database that is electronically linked to the central hub in Murfreesboro. In addition to the database, the programs employ criminal intelligence analysts to provide case support to investigators in the field, provide research assistance on major investigations, and often provide a technical equipment loan program to its participants.

The RISS network of programs provides a myriad of services to fusion centers, specifically in the form of intelligence sharing and operational deconfliction. Even though fusion centers are terrorism centric, the majority of the tips and leads that come

into a fusion center are of an “all-crimes” nature, and need to be shared with other law enforcement professionals so important connections between crimes and criminals can be exposed and investigated more efficiently.

The RISS program primarily supports law enforcement partners, and generally allows access to the private sector. Regionally, the program attempted to provide portals for some private sector collaboration, but the HSIN system has taken over that role for the majority of fusion centers.

One of the unique features provided by RISS is a system commonly referred to as “tactical deconfliction.” RISS hosts an electronic system called RISS-Safe, that allows investigators and fusion centers to share information about tactical operations in the field in an attempt to avoid conflicts with on-going operations by other agencies in the same geographic area.

Investigators are encouraged, and now often mandated, to enter all tactical operations into the system. These operations include search warrant operations, SWAT operations, surveillances, vice operations, and “buy-bust” narcotics operations. The investigator enters the operation into the system and automatically creates a Geospatial Information System (GIS) map of the area where the event is taking place. The investigator then creates a “buffer zone” around the event that is coded into the map. The system stores this data, and if another tactical operation is entered into the system that falls within the selected buffer zone, the original investigator who entered the first tactical event is notified that a second tactical event is going to occur within his zone. Fusion center analysts are also electronically alerted to the “tactical conflict” by the system, and notify both investigators to help resolve the tactical conflict.

This system creates two distinct operational advantages for fusion centers and investigators. First, the system helps avoid “cop vs. cop” situations where law enforcement investigators are not aware of a tactical operation occurring in their city. This improves officer safety, and can protect the accidental exposure of sensitive and often dangerous investigations. Secondly, the system acts as a secondary intelligence sharing mechanism as investigators can share investigative operational information

through the system, and if a conflict is discovered, investigators from both sides (each individual operation that were in conflict with one another) can meet and compare investigative data and tactical considerations. Both of these advantages lead to a safer, more efficient, and complete investigation and response, by law enforcement and fusion centers alike.

4. Custom-Built Fusion Center Websites

Many fusion centers, and law enforcement private sector outreach programs, are using custom-built websites and message boards to directly communicate with their partners and participants.

These websites provide fusion centers the flexibility to provide publications and other material content and links to other services provided by host agencies and members. For instance, the Oregon TITAN Fusion Center hosts www.osin.info[68]. This website has a number of the same features as the HSIN system but also allows users to access custom features directly aimed at state and local users within the state of Oregon. One of these features is a web portal for all law enforcement training hosted in Oregon, and a custom tool allowing users to sign up and reserve seats in training classes. The site also allows access to legal documents, like the Oregon Search and Seizure Manual, and legal opinions posted by the Oregon Attorney General and the Oregon Court of Appeals.

One of the most popular features of the osin.info site is the ability for a user to access NCIC directly from the site. This enables the user to conduct legal research, initiate wants and warrants checks on suspects, and obtain criminal history information on known suspects. The user can also access a list of links to common Oregon law enforcement research websites, such as the Oregon Employment Database, the Oregon Secretary of State's Corporation Database, City and County Property Ownership databases, and the Oregon Fishing License Database.

[68] Oregon Department of Justice, Criminal Justice Division, www.osin.info, accessed on 10/17/12.

One of the most professional public outreach websites in the nation is the Los Angeles InfraGard website.[69] This website, cohosted by the Joint Regional Intelligence Center (JRIC) and the FBI, allows participants to communicate with the program management, report suspicious information directly to the fusion center, and view the National Terrorism Advisory System.

The website has sections devoted to training announcements, threat warnings and publications, and the ability for citizens to join LA InfraGard directly from the site. One of the unique features is the site has a custom portal for each critical infrastructure sector. A member can click on a sector and receive an overview of the sector, what types of businesses are assigned to the sector, and links to contacts for threat information directly relating to individual businesses within the sector. In addition, the JRIC has an analyst assigned to each of the 18 sectors, and can be contacted via email directly from the sector portal.

69 InfraGard Los Angeles, http://infragardlosangeles.org, accessed 10/17/12.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CASE STUDIES OF PRIVATE PARTNERSHIP PROGRAMS

A. CASE STUDY NUMBER ONE, THE LOS ANGELES JOINT REGIONAL INTELLIGENCE CENTER

The first case study is one of the largest terrorism fusion centers in the United States, the Los Angeles Joint Regional Intelligence Center, commonly called the L.A. JRIC. Specifically, this report examines JRIC's private sector outreach program called InfraGard Los Angeles.

Program manager, FBI Special Agent Regina Miles, was interviewed for this analysis on August 1, 2012, and the interview was tape recorded and transcribed.

1. Background

The program is one of the largest law enforcement private sector outreach programs operated in the United States. Currently, the program provides services to 2,230 participants in seven large counties in Southern California, including Los Angeles, Orange, Riverside, San Bernardino, San Luis Obispo, Ventura and Santa Barbara.

Originally established in 1996, the main focus of the program is to provide a collaboration platform that allows the FBI and other law enforcement agencies to exchange information with the private sector with the goal of keeping their businesses secure and their employees safe. In return, the FBI anticipates that the participants will share information with the FBI that might alert the agency to suspicious activity or threats that could help them prevent a terrorist attack.

The program is operated out of Joint Regional Intelligence Center but is overseen and managed by the Los Angeles FBI Field Office. The current program manager, Regina Miles, is supervised by a Supervisory Special Agent on the FBI's Liaison Squad within the SHIELD Intelligence Group. Because the program resides within the fusion center, Miles informally reports to managers employed by the Los Angeles Police Department, the Los Angeles County Sheriff's Department, and the U.S. Department of Homeland Security.

The InfraGard Los Angeles program also employs a civilian oversight committee comprised of four executive members and seven board members. These members are nominated by program participants and serve as advisors to the program manager. The committee also helps the program manager handle controversies or complaints that might arise with participants and makes program related recommendations to the FBI.

Miles stated that the program has changed dramatically over its history, making programmatic shifts in 2003 and 2004 when she was assigned as the program manager. Prior to 2003, the program was primarily a resource for the public to report crimes and tips, with an emphasis on terrorism activity. The national program managers determined the program should be more robust and allowed local program managers to institute customized changes to meet the demands of their local businesses.

Nationally, protecting the nation's critical infrastructure was a high priority, and Miles saw the InfraGard program as the perfect tool to connect with private businesses to help keep them safe. In addition, she saw the potential participants as "force multipliers" and the real "eyes and ears" that actually know what is, and is not, suspicious activity within their businesses.

It was during this early phase of the program's development that Miles heard about the Los Angeles Police Department's Archangel program. This program was designed to assist private companies, specifically identified as a critical infrastructure, evaluate their facilities and provide them with strategies to harden them against a terrorist attack and improve overall security. Miles began accompanying the LAPD Archangel officers to learn about the intricacies of this effort, with the goal of integrating their methods and strategies into the InfraGard LA program. Coincidentally, during that same time frame, Miles attended a meeting where the Director of the FBI was giving a speech about counterterrorism efforts within the agency. One of his key points in the speech was that the FBI needed to improve their relationship with the public in regards to critical infrastructure and "share, share, share!" Miles said jokingly, "Holy crap, he's talking to me!"

She used this inspiration to integrate the Archangel critical infrastructure protection strategies into the InfraGard Los Angeles program and establish the main goal of educating private businesses about real-time threats and preventative measures to protect their businesses.

Miles crafted her strategy with the idea that if the FBI and the fusion center provided high-quality publications to the private partners, including real-time threat information and realistic approaches to protect their businesses, the program would grow and so would the participant's trust in law enforcement. The tool they used to disseminate these publications was the InfraGard electronic collaboration portal.

The InfraGard portal is a website managed by the FBI with the assistance of Louisiana State University. Members gain access to the site by filling out a registration form, which allows the FBI to conduct a routine background check of the applicant. Once vetted, members can access the site, read publications produced by the FBI and fusion centers, report threats, tips, and leads directly to the FBI, and access training materials for their businesses.

Miles said she really did not have a formal marketing strategy to attract new participants. Her technique was simple, meet the participants in person, and GO to their meetings! Miles said one of the elements of the program is to encourage the participants to meet on a regular basis to share information and to engage in training. Miles and her colleagues will often provide training on a myriad of criminal justice topics, usually centered on the prevention of terrorism, and encourage the participants to exchange ideas and strategies that have worked for them. Other than the meetings, Miles stated that their website has been an important factor in recruiting new members and so has "word of mouth." Miles contends that if her members find the program useful and beneficial to their business, they will spread the word to other business associates.

2. Critical Errors in Planning or Operations

Miles immediately responded to the topic of critical errors they made by recalling that she accidentally disseminated sensitive information by mistake. She said she has only done this once in eight years of managing the program, but it was an important

learning experience for her. It taught her the program's credibility was the most important feature, and that if you are not careful with privacy issues, or the sensitive nature of intelligence operations, the programs can fail due to poor reputation alone. Understanding that security of information is paramount has helped Miles improve her operation and focused her and her coworkers to take this topic seriously and remain vigilant to this issue.

3. Obstacles to Success

When asked about what obstacles affected the operation or success of the program, Miles said her coworkers did not understand or see the value of the program. Miles said her fellow FBI agents did not take the program seriously and did not understand the value to the community or the Bureau.

Miles was determined to succeed and felt she needed to build trust over time and prove the program could accomplish its goals and mission. She said, "…nobody knows what the program is until it grows and gets a reputation!" She said a strong program name is very important, so people can link the name to the services being rendered. Once people automatically recognize the name and attach the name to the program's credibility and important services, the program will grow and become popular with other agents and managers. Miles said it took a number of years, but she kept pushing allowed the success of the program to speak for itself. Now, other FBI agents understand the program's value and often volunteer to help give training or participate in other ways.

4. Key Program Components and Smart Practices

Miles identified a number of key features that are significant to the overall success of the InfraGard Los Angeles program. They are:

1. Program managers need to understand their partners and make a concerted effort to learn the business landscape in their area. Talking to business leaders, security professionals, and technology specialists is difficult if you do not understand their unique jargon and concerns. The only way to learn about the business environment is to get out and talk to people.

2. The program should only specialize in one main service. If the program has too many features or services, you lose expertise and need additional staff to handle it. For instance, Miles focuses only on outreach and education, and does not try to recruit her members as informants or intelligence sources. She believes that if members think she is always trying to obtain information from them, they will lose trust and not participate. She leaves the intelligence gathering business to her FBI and fusion center colleagues.

3. Program managers and law enforcement participants need to show up to meetings and events as a team. Participants must see a team effort and cooperation between law enforcement agencies to build trust.

4. Understand the premise that law enforcement does not know everything and has a lot to learn from the private sector. Miles said a critical mistake is to go into a business and pretend to know what they do and what the threats are. “Don’t be afraid to learn. It’s good!”

5. Make sure to establish and keep and engaged policy board or oversight committee. The members must take an active role in the operation and be “true believers” in the cause. Members who are there for personal enrichment must be removed, as it is often obvious to members and creates a poor example.

6. Program management must keep the participants engaged and constantly sharing or the program will falter. They must feel they are part of the system, have a trusting relationship with other members and the sponsoring agency members, or you will lose them.

7. Establish a nonprofit or other mechanism to generate private funding for the program. Nationally, politicians and civic leaders do not yet understand the value of these programs and are reluctant to provide the appropriate funding. Private donations, fund raising events, and user fees are examples of ways to raise money to purchase supplies, pay for training venues, and buy needed equipment.

8. Social media and websites are important in today’s technological world. If you do not have a website or some type of alternative media position, you will lose out on potential participants. websites are the easiest way to reach people with a minimal amount of staff. The content on the sites can include marketing information, meeting announcements, and training opportunities.

9. If possible, send your publications and bulletins directly to the user. Do not just post them on a site and force them to log-on to get them. People are too busy and want the convenience of receiving publications by email.

10. Provide valuable tools to participants that they can put to use immediately. For instance, the InfraGard LA team produced a model emergency operations plan that businesses can customize with very little effort. These types of tools are great for the business and they achieve immediate results.

11. The InfraGard LA program created an Infrastructure Liaison Officer program, similar to the LAPD Archangel program. This group works in concert with the Infragard members and provides vulnerability assessments for businesses who participate in the program

12. Lastly, you must be all-inclusive. Every business should be able to participate. Miles said that "mom and pop" stores are often very familiar with neighborhood problems and criminal activity, but are often overlooked by law enforcement outreach programs. The common practice is to focus on the biggest employer in the region, and even though that is very important, strategic businesses in areas not traditionally targeted for these programs might be more beneficial partners. This strategy coincides strongly with the first key feature. Knowing the businesses in your geographic jurisdiction, and the value they might bring to the program is critical.

B. CASE STUDY NUMBER TWO, THE COLORADO INFORMATION ANALYSIS CENTER

The second case study is another large private sector outreach program operated by a state-sponsored fusion center, the Colorado Information Analysis Center (CIAC). Specifically, this analysis examines CIAC's critical infrastructure protection outreach program called RUBICON.

Program manager Lieutenant Colonel Brenda Leffler was interviewed for this report on July 13, 2012, and then again on July 31 for a series of follow-up questions. The interviews were tape recorded and transcribed.

1. Background

Colonel Leffler began the interview by giving an overview of the history of the fusion center itself, as she felt the operational changes in the management of the fusion center would help explain how the RUBICON program was established.

The CIAC serves as the state fusion center and serves approximately 4,000 law enforcement and criminal justice professional customers across the state of Colorado. The CIAC is staffed by 30 employees from a multitude of local, state and federal agencies and is the central point for inter-agency information gathering and is responsible for review, analysis and dissemination of this information. The center acts as a formal liaison between the assigned agencies, to combat major criminal threats and improve the sharing of counterterrorism information.

The center's other role involves private industry, as it now provides threat warning information to businesses to ensure safety and security.

Lastly, the fusion center has the important role as acting as a "terrorism early warning system" for the Governor's office and the state's elected officials.

The original CIAC was established in 2002, but it went through a painful reorganization and restructuring in 2004 and 2005 after an audit was conducted on U.S. Homeland Security Grant funds from the 2002 grant allocations. Leffler said the results were "absolutely embarrassing to the state" and the governor stepped in and replaced every member of the staff who had originally started the program. The program was turned over to the Colorado State Patrol, which was followed by several years of attempting to repair the center's credibility and damaged relationships.

One of the significant changes that resulted from the reorganization, bolstered by the theory that the agency had to repair partnerships with the private sector, was the establishment of the RUBICON program.

Leffler describes the program as a hybrid: a combination of a traditional terrorism liaison officer program and a critical infrastructure outreach program. The official mission of the RUBICON team is to work with private industry and public agencies to

conduct “full-spectrum vulnerability assessments” on critical infrastructure and key state assets. The team conducts the assessments and provides the business owners and management with a threat mitigation plan they can use to strengthen security and harden the physical buildings to an attack. The team also collects a plethora of technical data about each facility and enters it into the Automated Critical Asset Management System (ACAMS), which is a web-enabled portal managed by the U.S. Department of Homeland Security to store and track critical infrastructure across the nation.

When asked how the team was initially designed, Leffler laughed and said, “We made it up as we went along!” She said the original group that was responsible for the assessments was the Colorado National Guard. The team was already conducting studies and assessments on large-scale, high-visibility targets like movie theaters, stadiums and shopping malls. Leffler’s group met with the National Guard employees and modeled the RUBICON program to mimic what they were doing. Leffler sent Colorado State Troopers to specialized training, a two-week infrastructure assessment school, and the National Guard team mentored the troopers for a couple of months to get them started.

Once the program goals were established, the Colorado State Patrol decided that a dedicated five state troopers could do the assessments full-time, with the oversight provided by one assigned Sergeant as the team’s supervisor. The entire program would be overseen by the traditional chain of command, with additional oversight and direction from the fusion center management team, including Leffler. The program does not have a separate oversight board or committee.

The team operates on a very small budget, approximately $350,000 per year for personnel costs, and an equipment and supplies budget of approximately $25,000. The rest of the hidden costs (vehicles, standard police equipment, and training) are absorbed in the State Patrol baseline budget.

The program can also draw funds from a unique program sponsored by a local nonprofit in Denver called the Center for Empowered Living and Learning, CELL. The program developed a community education program that they deliver to members, and

the RUBICON team members actually teach. The program is mobile and is presented in schools and other civic venues, and it focuses on terrorism prevention, resiliency, and home and business security awareness.

In addition to the actual assessments, the program provides continuing support to their customers in the form of publications and training. The small contingent of RUBICON team members partner with the fusion center's fusion liaison officer program to provide this information. When RUBICON learns of new techniques or specialized threats that might target a specific type of infrastructure, (e.g., the power grid) they produce a white paper and distribute it using the Homeland Security Information Network (HSIN) or the InfraGard program.

The team communicates with the over six hundred FLO participants, and countless community members via a custom-designed list serve program. The team sends reports on training opportunities, terrorism trends, national crime reports, protective measures and best practices, and direct threat information, to participants via the list serve. This direct communication keeps participants engaged and aware of all program activities.

Leffler said the RUBICON program does not employ a formal marketing program, but it maintains the philosophy that if you show up, people with listen. Leffler said they attempt to attend any meeting or public event where people are talking about crime, terrorism, or security. One of their main goals is to try to participate in every event by providing some type of training as often as possible.

2. Critical Errors in Planning or Operations

Leffler stated she believed the management team made two key errors when establishing and operating the program.

The first was they did not have a plan to sustain operations. They gave zero, or very little thought to how the daily operation of the program could last, how it would be funded five years in the future, or if the "powers to be" would think the program was

valuable and wanted it to continue. They knew federal funding was currently available, but did not foresee the massive government shortfalls and the shrinking grant allocations.

Secondly, and more important, was the team did not reach out to local law enforcement as a partner. Leffler explained that when the program first started, private companies were very concerned about the security of their information and specifically, proprietary information. They did not want local law enforcement to be involved in the "out-briefings" because they were afraid the information would be documented and disclosed in law enforcement reports that were available to the public. The RUBICON team listened, and kept local law enforcement out.

Leffler said this completely alienated local law enforcement agencies where the private businesses were located. The local cops did not get to learn what the vulnerabilities of the businesses were, and they were unable to make suggestions to mitigate threats based on local knowledge and expertise. So, in trying to protect the business owners, Leffler said, "…we paid hell for that for a couple of years." Relationships were damaged and local police chiefs and sheriffs thought they were trying to intrude into local responsibilities and business relationships.

Once RUBICON managers realized what was happening, they changed course and reached out to the locals for ideas and assistance. The new policy of the RUBICON team is that they do not do the assessments unless the business agrees to allow local law enforcement and fire representatives to be part of the out-briefing.

3. Key Program Components and Smart Practices

When questioned about key components and strategies that have led to the success of the RUBICON program, Leffler listed the following tips and suggestions:

1. Program leaders need to set aside the egos and work to establish partnerships with the private sector. Leffler said, "We thought, because we were troopers, we can do anything and get it done by ourselves just by hard work. We completely undervalued what everyone else could bring to the programs and the processes that we were trying to develop."

   One of the key strategies is to put in the effort to understand the role of the business in the community and get a firm grasp on what the business does

everyday and how it impacts the city and state. This will allow you to have meaningful conversations with business leaders, and they will see you have done your homework and understand their value.

2. Build and maintain a high level of credibility. Leffler felt this was the most important aspect of her job. Being honest, transparent, straightforward and trustworthy buys a tremendous a tremendous amount of credibility currency.

3. Never promise more than you can deliver. When you start a new program, and participants start to interact with your team and a level of trust is established, the participants will naturally ask for more services and products. The team's natural inclination would be to step outside of the stated mission and try to help. Try to avoid this as the everyday stress on a program involves delivering the main product, in this case complex security assessments. If dabbling in a side project reduces the main deliverable, your reputation for high quality of work will diminish.

4. Create an emergency access list of subject-matter experts in all fields within your jurisdiction that can be contacted 24/7 during an emergency or crisis. Understand that business leaders usually want to help, and when they finally do receive that emergency call, they will tell everyone they know that the government reached out and asked for help. Dedication to the program is a two-way street.

5. Follow-up after a service is delivered. The policy of the RUBICON program is after an assessment is done, someone from the team follows up with the business to see if they implemented any of the protective measures that they asked them to try. This sends a message that you care, but also allows the business to share critical feedback on what mitigation techniques work, and which ones do not. Management needs to review the feedback in an effort to make improvements in the program as it matures.

6. Attempt to work with existing business groups or associations. Downtown business groups, for example, are always trying to keep involved in civic issues, and crime and crime prevention are always important. If you can tap into an existing group, not only will you identify potential business customers, but also address security issues across a broad spectrum of businesses all in one place. Conversely, many of these groups are established based solely on the business category, for instance a technology business group. These sector-specific groups allow team members to feel the pulse of a particular sector and get a wide variety of expert opinions in one specific area.

7. Program team members must participate in public forums, InfraGard chapter meetings, etc. Not just program managers or agency heads. Program participants want to hear from the real experts, not the managers.

8. The program must have complete political support from agency management and city or state leadership. In Colorado, from the Governor down, the message is, "this program is very important, our businesses and their security is very important, and you will not fail to provide this valuable service!"

   That being said, all levels of agency and government management must have a complete understanding of the program, how it works, which businesses are targeted and why. This is key as the public will ask government leaders about the program, and if the official supports the program. If business leaders feel political leadership or agency executives do not understand or hold the program in high regards, they will not play.

9. If you are starting a new program, invest in a professionally designed project management program. There are low-cost software products available to help managers project costs, track tasks and goals, and set design milestones. Many of these programs include GANT charts to help participants visually see the project components and timelines. These programs also allow you to review your progress, and when you are done, go back and debrief the design plan to help improve the plan for the next big project.

10. Lastly, you need to consider how your new project will affect other programs and operations inside your agency. When a new project is being implemented, everyone's eyes are on it, and the agency is expending resources and manpower to get it established. But, in reality, funds and manpower are being diverted to the new program from an existing program or service. Leffler said, "You know outreach, you think you understand the politics and legislation and funding, but do you know the cascading effects of making this decision and how it affects X, Y and Z decisions? If you are going to do this, you should be at least considering these things as well!"

C. CASE STUDY NUMBER THREE, THE ORANGE COUNTY SHIELD PROGRAM

The third case examines a private sector outreach program operated by a local fusion center, the Orange County Intelligence Assessment Center (OCIAC). The program operated by the center is the nationally known Orange County SHIELD program.

Program manager, Heather Houston, was interviewed for this report on July 13, 2012, and then on several other occasions for follow-up questions. The interviews were tape recorded and transcribed.

1. Background

The Orange County SHIELD Program (referred to as SHIELD from this point forward) was originally established in 2002, but as the other two programs examined in this thesis went though a name change in 2007, it was transferred to the newly formed Orange County Intelligence Assessment Center to manage. The program was formally called the Private Sector Terrorism Response Group, and originally fell under the management of the Orange County Terrorism Early Warning Group (which was later renamed as the Orange County Intelligence Assessment Center.

The program's mission is to reach out to private sector security directors in the Orange County Metropolitan area and bring these important assets into the homeland security discussions, exercises, and training to increase awareness of crime trends and provide them with crime prevention strategies.

The current manager of the program is Heather Houston, who was appointed to oversee the program in 2001 by the Orange County Sheriff. Houston said the Sheriff travelled to New York and was impressed by the private sector response to the attack on the Twin Towers. Houston's research led her to understand how important the private sector can be in the aftermath of a catastrophic event the size and scope of the September 11 attacks. Moreover, she saw how her own community came together and responded in the aftermath of enormous wild fires. Houston said, "I saw the corporate folks bring truckloads of resources to the affected areas. The goal is to work with private sectors partners and begin a collaborative relationship before a crisis presents itself"

Houston took the lead of establishing the new program, and felt her twenty-year background with Bank of America helped prepare her for the challenges of communicating with the business community. Houston is a civilian employee and reports through the Orange County Sheriff's Department chain-of-command.

Her research led her to the origins of the NYPD Shield program, as well as, successful private outreach programs in Great Britain called Project's Griffin and ARGUS. Both of these programs incorporate the public and private business into the framework of the county's terrorism prevention and response strategy. The local police in England train citizens and host exercises to prepare them for mass casualty events, natural catastrophes, evacuations, and major public health emergencies.

Houston said she had to break through strong cultural traditions in terms of allowing private sector employees into security and homeland security discussions, which did not happen before the program was established. She stated there was a very strong "us versus them" culture and tradition in the law enforcement community that she desperately needed to change. "And I would say the hardest thing I had to do was to work to break that wall so that law enforcement saw private sector security as a force multiplier and a partner in our homeland security efforts." Houston reports that the majority of SHIELD members are security directors, business continuity officers, business resumption professionals, and health and safety officers. She said the membership is very diverse, representing business and industry, academia, and of course, shopping/resort properties (Disneyland!).

Houston took a unique approach when first deciding whom to recruit to join the program. She asked herself, "Okay, what do I want to build and who is going to play? We have Anaheim as our resort center, Irvine is our business center, and Santa Ana is our government seat. We are very deep in targets here and generate a GNP of approx. $200 billion dollars. So there are two threats: threats against assets, and threats against our population density. So, when I look at the county, I think anyone should be allowed in. Unless there's a reason for me not to do business with somebody, I don't have a problem with everybody doing business in Orange County being part of Shield!"

The SHIELD program's primary function is education, and they accomplish this in two ways. The first is by producing and disseminating a weekly briefing report, called appropriately, "The SHIELD." The bulletin is produced by Houston and analysts from the fusion center and contains national threat briefings and alerts, local and regional crime trends, crime prevention tips, and updated alerts about training opportunities for

members. The SHIELD is emailed to the over 850 members every Friday, and acts as an education tool and marketing service all in one product.

The second part of the program is the membership and training meetings held every other month. Each meeting has an overall training theme, chosen by fusion center staff or by actual program participants. The fusion center analysis group will usually conduct a briefing on threats and tips and leads that have come into the center since the last meeting. They will discuss current trends and participate in a round-table conversation about the topics. In addition to the formal meetings, the program hosts four additional meeting jointly with the Terrorism Liaison Officer (TLO) program participants who are primarily police officers and firefighters. These joint meetings are very valuable as the TLO's can share trends and issues that are currently being discussed in law enforcement agencies.

The SHIELD program is one of the few programs in the country that does not use an electronic collaboration tool like InfraGard or HSIN. Houston said she encourages members to join the InfraGard Los Angeles program and get access to HSIN but feels managing a system is not wise due to the lack of funding and additional personnel to oversee a system of that size. Additionally, Houston does not vet program participants. Again, this is not the traditional approach, however, she believes vetting is difficult, expensive and a manpower draw on a program. She explains that the bulletins do not contain national security information and are primarily open source or For Official Use Only (FOUO) and do not need a security clearance or background to access.

Houston said the program has a very small budget and is now managed directly by the fusion center. She said the budget only pays her salary, and federal grant funds pay for training as long as TLOs are in the meeting as well. All other SHIELD meetings are hosted by the Orange County Sheriff's Department at no cost to the participant.

Houston does not employ a formal marketing strategy, but she produces and disseminates a tri-fold brochure describing the program whenever she is at a public event. She also knows the TLOs do a tremendous amount of marketing, as they interact with the public and often recommend private sector professionals to join SHIELD.

2. Critical Errors in Planning or Operations

Houston said the program's biggest mistake in planning was the initial strategy of primarily targeting only the biggest businesses in the county. She said the program (before she took over) was viewed as an "exclusive club." They did not recruit smaller businesses or mom- and pop-type companies that are in a position to have first hand information on local threats and crime issues.

3. Obstacles to Success

Houston viewed the law enforcement culture as the largest obstacle to the program. She said, "Law enforcement historically viewed private sector security as untrusted, undertrained and ineffective. So, the way they viewed private sector security was not only grossly inaccurate, but it was dangerously unfair. So my biggest battle was on my home front. This is a different world, and I don't want to be someone who's sitting on information and doesn't share it with stakeholders when IT hits the fan. I don't want to be that guy!"

She went on to say it is primarily the more senior (time, not age) officers that do not think the public should be a part of the police world. She said this is almost impossible to overcome, especially for a civilian woman in law enforcement.

4. Key Program Components and Smart Practices

Houston listed a number of key components and smart practices she believed were the bedrock of the SHIELD program. They are:

1. You must keep participants constantly engaged or you will lose them. Her best strategy for that is the weekly SHIELD bulletin.

2. Provide free training as often as possible. The private sector's main goal is to make money, and outside training opportunities are rarely provided. People generally are hungry for cutting-edge information, and feel engaged when they understand the threats and solutions if presented in a professional way.

3. Allow participants to have input into the training agenda. ASK THEM what THEY need to learn. Don't always assume your best topic is the one they want or need. Customize the training to the group, do not cookie-cutter the training.

4. Combine resources, especially other law enforcement groups like TLO's or other first responders. If you allow these groups to mingle with the private sector, magic will happen.

5. Only operate the program as a liaison program only, as a buffer between the public and law enforcement. The program should not be seen as a crime-fighting, counterterrorism unit- the primary mission is information sharing, networking and education. This training/outreach role always makes the public more comfortable and elicits more participation and engagement.

6. Do not be selective of the program participants. The guy who owns the gas station is probably the guy with the best view of the world. Do not leave him out.

7. Do not turn down anyone who wants to join unless there are security issues or concerns with a person's motivation to join. Vendors are the exception; they are not invited to join to market products or services.

8. Do not conduct background checks on the participants. It is costly (often a very high hidden cost) and is not functionally effective. A very cursory background check can give you a false sense of security. You rarely get people who do not have good intentions trying to join these programs. We deal in open source information.

9. Pick a civilian as the director! Houston thinks participants are quicker to accept a civilian in public/law enforcement partnership role.

10. Learn who your audience is! Work hard to create an open communication environment that builds trust. This will increase information flow and is the bedrock of any successful program.

11. The most important function is to act in <u>support</u> of the local law enforcement agency! Do not alienate the locals by coming in and presenting yourself as the all-knowing expert on security issues.

So when I go out to a private sector asset, I am extremely clear that I'm not a bigger law enforcement presence than their locals, that I'm operating absolutely as a support to their locals and I encourage them to meet them. You know, bring in their law enforcement, bring their fire department, bring in their county health officials so that they become familiar with

their asset, they become familiar with their management team, let the SWAT players train in there at night at their facility.

D. CASE STUDY ANALYSIS

From the outside looking in, the three programs appear to be similar. They all have exceptional reputations within the law enforcement community and are meeting the goals set forth by their leadership and Department of Homeland Security standards and milestones. But when you examine the programs more carefully, all three have many characteristics in common, but achieve their missions in different ways.

One of the most intriguing aspects that emerged from the case studies was that two of the programs made drastic changes in their operations after several years of mediocre performance. The LA JRIC program changed in 2003 and 2004 to include critical infrastructure issues and increase participation of businesses and the public. The RUBICON program's change was forced from the outside as a government audit revealed poor performance. The reorganization lead to the establishment of the critical infrastructure analysis program and the partnership created with Colorado's Fusion Liaison Officer Program. And although Heather Houston from the Orange County SHIELD program did not focus heavily on the issue of operational change during her interview, when she took over the program in 2007 the program was completely changed from a small operation within the Private Sector Terrorism Response Group to an independent private sector outreach group with its own leadership and mission.

All three of the program managers were innovative in their approaches in custom designing their programs to meet the needs of their local constituents. Regina Miles and Heather Houston both found programs that had components they wanted to emulate, and customized them to fit their demands. Miles came into contact with the LAPD Archangel program and incorporated ideas they developed to analyze critical infrastructure and involving local businesses in their threat assessments. Houston was able to merge the most successful qualities of three regional programs, the New York SHEILD program and Britain's Griffin and ARGUS projects.

Brenda Leffler said their approach was to "make it up as they went along." Even though she was being modest in her response, when you examine the efforts she took to research the existing Colorado National Guard infrastructure program and the national training she identified to educate her employees, these actions are the foundation to designing a successful program. Taking successful attributes of existing programs, while simultaneously using strategies that are already working, (and eliminating functions that do not work), seems to be a recipe for success in law enforcement programs.

Another surprising element that emerged from the interviews was the importance placed on the issue of understanding your program partners. The three managers all insisted that law enforcement continues to do a poor job of learning from, and integrating the knowledge of the private sector into their operations. Leffler stated, "We completely undervalued what everyone else could bring to the programs and the processes that we were trying to develop."

Leffler summarized this topic by identifying and comprehending what the private sector does allows us to get a firm grasp on what a company does, and how it might impact the day to day operation of the city and the state. This knowledge, coupled with the understanding of the existing terrorism and criminal threat, empowers law enforcement to make meaningful recommendations to business leaders about how to protect their businesses and employees.

Funding was also an important topic during the interviews, and it is noteworthy that the three programs operate on a very small yearly budget. This being said, the addition of supplemental funds by innovative fundraising allowed two of the programs to continue to operate even though operational funding was limited.

The RUBICON program is not a "nonprofit" but established a valuable partnership with community training and education program called the Center for Empowered Living and Learning, CELL. RUBICON is allowed to accept private funds from CELL, in exchange for specialized training and programs presented on behalf of CELL at quarterly meetings. The LA JRIC partners with Louisiana State University to

save money on the cost of vetting participants and also takes donations directly from program members to pay for training venues and meeting essentials like basic supplies and break snacks.

These small but effective fundraising efforts go a long way to making a program successful. When federal grant funds and local law enforcement budgets are crafted to fund special programs, little consideration is given to small administrative functions that often make the difference between failure and success. The cost of conducting background checks on program participants could be extremely cost prohibitive, but the extra effort displayed by Regina Miles and her team to take full advantage of an academic resource to improve the value and productivity of their program makes all the difference.

Relating to the funding issues discussed during the case studies, the issue of program sustainability was an important topic for the locally managed programs. The SHIELD program and the RUBICON team program manager both emphasized the importance of planning ahead with a focus on long-term funding. Leffler said they gave "zero" thought to how the daily operation of the program could last, or how it would be funded five years in the future. She hoped the department executives would see the value of the program and just pay for it. Both managers thought federal funding would continue to pay for the program and never saw the impending impact of the massive government shortfalls and shrinking grant allocations.

Strategic planning plays a critical role in program development, but very little thought is given to the impact of sustaining the funding. Law enforcement agencies fall into the same traps as state and local governments do; they use current tax revenues to fund programs and only look as far as the next budget cycle as a horizon. Programs need stable funding, usually over a long period of time to remain vital. Innovative funding strategies, nonprofit program status, and working with established civic programs that can provide emergency or operational funding, must be explored during the program's design phase.

When asked what obstacles were in place that may have hampered or damaged the growth or successful operation of the program, both Leffler and Houston thought that their law enforcement colleagues posed a significant problem. Houston noted that law enforcement "cultural traditions," in terms of allowing the private sector into the policing profession, were strongly opposed to inclusion. The strong, "us versus them" culture caused problems building relationships, and Miles said her fellow FBI agents did not take the program seriously and did not understand the value to the community or the Bureau.

This deep-seated culture can be directly tied to many police officers' perceptions of Community Oriented Policing (COP) programs that became popular in the late 1990s. Patrol officers believed the programs were "fluff" or a politically correct effort to appease the community's fear of the police after negative press in the aftermath of the Rodney King riots in the early 1990s. Many police officers believed that in an era of reduced funding for law enforcement, spending time attending community meetings was not cost effective, and took valuable police resources off the street resulting in critical officer shortages.

Understanding these cultural aspects of a law enforcement agency can be critical to the program's success and communication with officers about how the relationships can benefit the department and the community should be enhanced when starting a private outreach program.

Another error common to two of the programs was the failure to involve local law enforcement into the planning and operation of the program. The SHIELD and RUBICON programs both have a large geographic scope, involving numerous local and county law enforcement agencies. Houston and Leffler both noted that their agencies did a poor job of involving the local agencies when then delivered services into the local communities.

Leffler reported that when RUBICON first started conducting critical infrastructure evaluations for private sector businesses, the security professionals involved were concerned about company secrets and did not want local law enforcement involved in the reviews. Leffler listened, and excluded local law enforcement

representatives from participating. She said this was a big mistake as local Sheriff's and Police Chiefs resented their omission and made complaints. Houston echoed this concern, and said their office often alienated locals by meeting with important business leaders, and representing themselves as experts on security issues in that city. Again, this caused friction with local police leaders.

Leffler and Houston's experience in this area highlights the importance of understanding who your customers really are. When establishing a public outreach program, agencies must consider the wide-reaching impact of the program, and the down-stream affect on other agencies and services. Most programs are not confined to a small jurisdiction, so networking and communication is critical to maintaining healthy relationships between law enforcement entities.

Lastly, leadership was the most prominent factor that stood out when examining these three programs. All three program managers were intelligent, enthusiastic, and proud of their accomplishments.

When queried about why their programs were successful, or what key features were implemented that worked well, the managers all talked about educating themselves, and tried to understand the underlying relationships and nuances that would give them an edge-up to advance their program. They all studied the details of successful programs, networked with other program managers, and asked to "job shadow" with other existing groups in an effort to learn what works and what fails.

One of the most striking similarities between the interviews was the repeating theme finding the courage to ask questions of the public. All three managers made it a point to emphasize that law enforcement officers think they "know it all" because they routinely interact with the public during emergencies, and fail to really understand what makes a business tick. Regina Miles summarized this by stating, "Program managers need to understand their partners and make a concerted effort to learn the business landscape in their area. Talking to business leaders, security professionals, and technology specialists is difficult if you do not understand their unique jargon and concerns. The only way to learn about the business environment is to get out and talk to people!"

IV. FOCUS GROUP INTERVIEWS

A. BACKGROUND

On September 17, 2012, a focus group of subject-matter experts was assembled to analyze the interview responses of the program managers. The panel consisted of three law enforcement executives with over seventy years of combined experience in the field.

Steven Briggs is currently the Drug Enforcement Administration Counsel for Oregon, Washington, Idaho and Alaska. He previously served as the Chief Counsel of the Oregon Department of Justice Criminal Division, overseeing a variety of criminal investigatory, prosecution and intelligence functions, including the state's Terrorism Fusion Center, the Organized crime section, the District Attorney Assistance Section, the State Intelligence Center, and the Internet Crimes Against Children program. Mr. Briggs is an accomplished trial attorney having handled numerous high profile capital murder cases, twice receiving the Department of Justice Outstanding Service award, as well as an award from the National District Attorney Association. He has lectured nationally and internationally on a variety of topics including trial practice, terrorism, ethics, organized crime and fraud. Mr. Briggs is a graduate of Dartmouth College and the University of Oregon School of Law.

Chris Gibson was appointed as the Oregon High Intensity Drug Trafficking Area (HIDTA) program Executive Director on November 1, 2006. The HIDTA program is a federally funded counter-drug grant program administered by the Office of National Drug Control Policy (ONDCP). Prior to his appointment as Oregon HIDTA Director, Mr. Gibson served for 18 years in local law enforcement and achieved the rank of Deputy Chief of Police at the Beaverton City Police Department (A large suburb of Portland). Mr. Gibson graduated in 1990 from Portland State University with a Bachelor of Science degree in the Administration of Justice, and again in 2011 with an Executive Master of Public Administration. Mr. Gibson is also a graduate of the 205th Session of the Federal Bureau of Investigation's National Academy.

James C. Ferraris is an Oregon law enforcement veteran of nearly 34 years and is currently the Deputy Chief of Police of the Salem, Oregon Police Department, serving since 2011. James was previously employed by the Portland Police Bureau, having served in several executive level positions including Commander of the Police Bureau's North Precinct from 2006 to 2011. He was responsible for the leadership of more than 200 employees providing police services to 165,000 residents in a 63 square mile area, while managing a $24 million operating budget. Mr. Ferraris has many years of service as a Critical Incident Commander in charge of the Special Emergency Reaction Team (SERT), the Hostage Negotiations Team (HNT) and the Explosives Disposal Unit (EDU).

In 2003, Mr. Ferraris was appointed as the Assistant Chief of Police in charge of the Investigations Branch, where for three years he led 350 employees, managed a $45 million budget and provided oversight of all investigative functions. Mr. Ferraris is a graduate of the FBI National Academy, Session 201, and currently an executive board member of the Oregon Partnership, Inc. (an organization that promotes drug prevention) and the Oregon HIDTA Program.

Prior to the focus group meeting, a spreadsheet was provided to each of the participants that containing the 54 questions asked of the program managers and their responses. (See list of questions in Appendix A) In addition, the group was asked to consider the following questions:

1. Would a nonprofit organization designed to support a public outreach program work in Oregon?
2. What is your opinion about the importance of a policy board or oversight committee?
3. Are Memorandums of Understanding (MOU) or other inter-agency agreements important to establishing a law enforcement program?
4. Should all program participants be vetted?
5. Would virtual participation work for this type of program?

6. Does the manager of this type of program have to be a sworn police officer or can a civilian employee be used?

7. Most of these programs have a limited geographic scope…can a state agency handle these programs with a small number of employees?

B. FOCUS GROUP DISCUSSION

During the focus group meeting, the participants discussed these eight topics in detail and produced the following recommendations based on their subject-matter expertise:

1. Would a nonprofit organization designed to support a public outreach program work in Oregon?

The participants provided three different views to this question. Briggs stated he is opposed to the government taking private donations of any kind, especially for small communities. The risk is that citizens could view the donations as an attempt to secure favoritism. In addition, the history of these donations is often available to the public, and can lead to an unwarranted allegation of favoritism, if the entity giving the money is also under suspicion of criminal or regulatory wrongdoing.

Ferraris supports soliciting private donations under limited circumstances. For instance, private companies offer law enforcement grants, usually tied directly to the purchase of specialized equipment (computers, weapons, etc.). If the grants are competitive, this can remove the suspicion that the funds were donated to secure favorable treatment.

Gibson stated nonprofit donations only work if you have a separate fiscal staff to monitor the funds. Once you start a donation program, the management and tracking of the funds is critical to the integrity of the program. If the fund is “blind” it is even better. If a person can donate and the operations manager and the program participants do not know the source of the donation, it shields the operation from attack.

2. What is your opinion about the importance of a policy board or oversight committee?

All three stated that a policy board or oversight committee should be a mandate. You need to have a buffer to provide liability protection, to have a sounding board for making major program changes, and to handle complaints or issues raised by outsiders and participants. Lastly, the board can be in place to hold program managers and participants accountable to policies, procedures, or by-laws.

3. Are Memorandums of Understanding (MOU) or other inter-agency agreements important to establishing a law enforcement program?

Briggs believes MOUs, or Letters of Agreement, are good but are not enforceable in regards to the stated legal penalties. They are important from a framework perspective in that the agreements lay out a course of conduct, or the terms of the program that can be used to enforce program goals, eliminate users that do not perform properly, and to educate outsiders, the press, or potential participants as to the operation integrity of the program.

Ferraris says that nondisclosure agreements for private participants are critical. The agreements lay out a foundation for privacy issues, protected information, and other security arrangements. In addition, the agreements have the added value of scaring away people who might have ulterior motives regarding their participation in the program.

4. Should all program participants be vetted?

The consensus of the group is that some type of vetting is critical to operational integrity and the reputation of the program.

Ferraris gave the example of a person participating in a program was found to be a known child predator. This information was exposed in the media, and it damaged the reputation of the program. He also stated that background checks have helped to expose bad actors, and people who attempted to infiltrate the program in an attempt to damage the program from within. Without the background checks, the people would not have been discovered.

Background checks also have the same affect as the Non-Disclosure Agreement, as they may scare away some people that have an ulterior motive to participate. People's identities need to be verified, either by a simple National Criminal Information Center (NCIC) check or some type of interview and background query.

5. Would "virtual" participation work for this type of program?

Briggs says that virtual participation only works in a limited fashion, as personal relationships are the "heart and soul" of any successful program. Studies have shown that live, face-to-face contact with participants is critical, even if these occur on a limited basis.

Gibson suggests a combination of virtual and live communications. For example, quarterly live meetings and training, supplemented by weekly email or message board communications.

All three are interested in how social media can be leveraged in terms of messages, warnings, links to bulletins, etc. All believe these would work, if the program coordination does not get overwhelmed with the use.

Ferraris is concerned about having participants log onto a proprietary system. He believes people are often overwhelmed at work already and having to log on to a system on a regular basis becomes tedious and results in deteriorating usage of the system. People need to be regularly engaged, and the program needs to drive the participation.

6. Does the manager of this type of program have to be a sworn police officer or can a civilian employee be used?

Gibson says it generally does not matter, but believes the "talent of the individual is more important than if they are a sworn or civilian employee."

Briggs says depending on whom the audience is, it could take some work for a civilian employee to gain confidence and trust of participants. If the participants are all civilians, it may not matter, but if some of the participants are retired LE, or current LE, then having some type of sworn presence could improve the trust level of the participants.

Ferraris stated the potential leader (regardless of their sworn status) needs to have some expertise in the field of the program. Mastery of the content, and the program features and goals, builds immediate trust and integrity.

7. Most of these programs have a limited geographic scope…can a state agency handle these programs with a small number of employees?

A major flaw of many programs is the program management "bites off more than it can chew." The panel strongly recommended starting a program with a limited scope that participants and employees could master and build a level of expertise. If the agency cannot handle the program with a limited staff, management should be honest and evaluate whether or not they should establish the program with the existing staff levels.

When features and services are added, managers should try to determine if the core mission can still be delivered without a drop off of service quality. If not, expanding will kill the program. Become "great" at the core mission, everything else is secondary and can damage the reputation and quality of the program.

V. FOCUS GROUP ANALYSIS

A. FUNDING

One of the serious issues facing law enforcement agencies today is paying for important programs and services during a decade of shrinking budgets and reduced federal grant funding. The focus group discussed this issue in great detail, primarily talking about alternative forms of funding like federal grants, business grants, and private donations. It was interesting that all three members of the group focused heavily on the appearance of impropriety that private funding can elicit. Mr. Briggs was chiefly concerned as he led the Oregon Department of Justice's Criminal Justice Division, which is the primary agency in Oregon that investigates political malfeasance and public corruption cases. He was concerned that private donations, regardless of how they were handled can lead to allegations of misuse and influence peddling.

Blind trusts were discussed as a method to mitigate the potential for public scrutiny, but all three members ended the discussion with a recommendation that private funding should only be considered in limited circumstances where program managers can make specific purchases, such as special investigative equipment. This direct purchase strategy, coupled with transparent accounting practices, should thwart public concerns about the misuse of donated funding.

B. LEADERSHIP

Several of the questions posed to the group led to in-depth conversations about the importance of leadership and the host agency's full understanding of the scope and function of the proposed program. The group strongly agreed that the selection of the program manager is the one decision that agency executives will make that has the most direct correlation to the eventual success of the program.

Gibson and Briggs agreed that it did not matter if the manager for a private outreach program was a police officer or a civilian employee, but they would probably try to locate a sworn law enforcement officer to establish the program. This issue is important because sharing information with the private sector carries extensive legal and

operational burdens not commonly confronted by private companies and their employees. Extensive knowledge of state and federal intelligence laws and protocols is needed to protect sensitive information where the inadvertent dissemination could severely damage the agency's reputation. For these reasons, the members stated they would lean towards hiring a police manager with experience in these topics, which would lend instant credibility to private participants.

The panel emphasized that an agency should not begin the process of starting the program unit you have the perfect person to run it. Without the right person, with the right skill sets and experience, the program will probably fail. This sentiment was repeated throughout the panel discussions and became the focal point of almost every topic segment. The panel emphasized that most agencies make the mistake of selecting an existing employee who already heads the division where the new program will be placed. For instance, if the new program is an undercover vice program, the current manager of the investigations unit will often be put in command. Does the investigation's manager have expertise in vice related cases? Does he or she understand the complicated set of sex-crimes laws and court decisions that can doom a vice unit if not fully appreciated? In the case of a private outreach program, many police managers have very little experience supervising civilian employees or working with the business community. Candidates within a police department that are involved in crime prevention, intelligence investigations, budget management, or other administrative functions should be considered when seeking a program manager.

Agencies are reluctant to look outside of the agency for a new manager, as union pressures to hire from within, and the budget impact of adding an additional manager, are important considerations for many agencies. But, leadership often involves careful consideration of all options, and picking an existing manager to run a program without the proper training and expertise can often lead to program failure. Steve Briggs ended the discussion by stating, "The whole program hinges on the proper personality fit of the leader!

C. PROGRAM OVERSIGHT

The discussion of program oversight was very short because all three panel-members immediately agreed that a program of this type should never be established without a policy board or some type of oversight committee. Anytime a police agency establishes a program that is not a traditional law enforcement service, the chances of failure are high due to a host of factors including a lack of business and civilian management expertise. For these and many other reasons, gathering a group of business, government, and citizen members together to oversee a program provides a strong sounding board when making program adjustments, negotiating contracts, handling complaints, and setting the strategic course for the program.

D. PROGRAM COMMUNICATION METHODS

The panel members were concerned that many law enforcement agencies are beginning to rely too heavily on the Internet and other electronic mediums to communicate with the public. The main reason for concern was the reduction of personal interaction and the panel's belief that the lack of face-to-face communication leads to weaker personal relationships that eventually will cause the program to fail. Chris Gibson put it best when he stated that program managers needed to focus heavily on how the participants interact with other sworn staff, and a delicate combination of virtual and live meetings needs to be established to enhance these relationships. Logging into a website on a regular basis does not build a healthy working relationship between law enforcement and the private sector. Personal relationships are a key factor in enhancing trust and open information exchange within the program.

E. SMALL-AGENCY ISSUES

It is easy to examine another agency that hosts a successful program, and say, "we can do that!" Just because an agency has a successful program, does not mean you can replicate it, as the program has to fit your agency's culture, budget, and mission for it to succeed. But law enforcement executives, especially from small agencies, often overlook the intricacies of a program and most importantly, the expertise and capabilities of the employees involved. Resources, processes, and values of a particular organization are

difficult to evaluate and measure from afar. When closely scrutinizing a successful function within a program, one or two employees often have the "it" factor: a combination of knowledge, experience, savvy, and interpersonal skills, that elevates the program to success. Executives need to honestly evaluate their own agency's processes and values to see if the existing staff has the minimum set of skills for the job. If there is a shortage of expertise, this can drastically change the outlook for success. Additional training, mentoring, or hiring new staff who have the existing tools to do the job, must be explored prior to beginning the program.

For these reasons, determining if the program can be operated without affecting the delivery of other core services needs to be examined and considered in great detail. Without comprehensive research and a thorough analysis of existing programs, employees, and resources, small agencies will be unable to clearly evaluate their ability to undertake this type of venture.

F. MENTORING

The focus group noted that the U.S. Department of Homeland Security hosts a series of professional mentoring programs for agencies establishing a variety of different programs. These programs include assistance in starting a fusion centers and emergency operations centers, fusion center and fire service information sharing programs, fusion liaison officer's programs, fusion center outreach programs, critical infrastructure programs and fusion center health security coordination programs. The group highly recommended networking with U.S. DHS on these programs, as they pair agencies up with experienced managers who have started similar programs.

Finding a mentor who has done it before and not "reinventing the wheel" was a repeated topic discussed by the panel. Executives should conduct extensive research into existing programs prior to beginning the planning process and not be afraid to copy these programs and involve the existing program's managers into the planning of the new program. Even though the agency could be confident in the program's planning direction, another agency may have established a similar program and save the planning process valuable time and energy.

G. PLANNING TEAM CONTINUITY

The focus group recommended that executives and managers beginning the process of establishing a new outreach program fully understand the goals, program expectations and mission. Even though this sounds rudimentary, executives often assume that all parties involved in the initial planning of a program are “on the same page.” Hosting frequent planning meetings where the goals, expectations and mission are formally stated, documented, and agreed upon before hiring staff and expending program funds should be considered. These formalities are redundant but will often save the group valuable time, if questions and concerns are addressed early in the process.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. RECOMMENDATIONS AND CONCLUSION

> I am a firm believer in the people. If given the truth, they can be depended upon to meet any national crisis. The great point is to bring them the real facts. —**Abraham Lincoln**

> A pessimist sees the difficulty in every opportunity; an optimist sees the opportunity in every difficulty. —**Winston Churchill**

A. FINDINGS

This research has examined the complex road travelled by executives and managers when trying to determine the most effective way to establish a law enforcement outreach program. With a focus on small police agencies and fusion centers established in smaller states or regions, fundamental elements, and key considerations emerged from the program manager interviews and focus group debates.

The goal of this research was to answer three distinct questions:

1. What are the fundamental program components fusion center program managers consider when developing a successful private partnership program?

2. What smart practices can be employed when implementing a program for a small fusion center?

3. What are the advantages and limitations of the electronic systems fusion centers use to collaborate with program participants?

The process of interviewing the three program managers, and the focus group discussions and analysis, produced six significant findings. The findings are documented in three separate sections of this chapter. Question One is answered below. Due to the large number of smart practices identified, the findings related to Question Two will be enclosed in a separate document called the “Blueprint Guide.” This document will be attached as Appendix B. Question Three will be addressed below under in the “Communication Methods” section.

The consensus opinion of the subject-matter experts was that the following six topics should be carefully studied in great detail by any law enforcement agency prior to establishing a private sector outreach program.

B. AGENCY SELF-EXAMINATION

Admitting that you cannot do something is one of the most difficult things for government agency leaders to do. But when confronted with the directive to establish a program of any type, many leaders fail to look within the agency in an attempt to evaluate if they have the expertise, culture, and sustainable funding to accomplish the task at hand.

Agency executives should start the process by asking themselves, "Are we the right agency to host this program?" Competition between jurisdictions is fierce in the law enforcement culture, especially between state and local agencies, and the federal government. For this reason, many law enforcement leaders are reluctant to admit that they might not have the capability to manage the program successfully, and perhaps a neighboring agency, jurisdiction, or federal agency might be better equipped.

Once an honest, analytical appraisal of the host agency has been completed, and it is determined that the agency is the right fit for the program, the process can move forward to examining the culture of the agency.

C. AGENCY CULTURE

The program manager interviews revealed that establishing private outreach programs was difficult because police officers had a mistrust of the private sector and did not understand the value of these partnerships. The program managers and focus group panel members believe a huge cultural shift is still needed before a successful partnership can be formed between law enforcement agencies and the business community.

Agency executives should survey agency employees to determine the level of willingness to integrate private sector employees into their operational framework. If resistance to this approach is revealed, extensive training and education of existing staff is recommended prior to bringing private sector employees into the organization.

D. FUNDING

Many law enforcement executives leave the issue of budgets and budget forecasting to professional fiscal staff, and rightfully so. However, the process of determining the startup cost of a program is complicated and the importance of securing sustainable, long-term funding is often overlooked.

Understanding the scope of the program, and the number of employees needed to interact and manage the private participants is one of the key factors to an accurate budget forecast. A careful analysis of the business community in the agency's jurisdiction, an evaluation of the existing critical infrastructure, and comparisons to other existing programs and their size and scope is critical to predicting costs.

One of the difficulties of the budget process is attempting to forecast the growth of a program once the program is established and becomes popular. If private businesses see the program as important, more will want to join, creating the need for additional staff, supplies, and possibly office space. Anticipating expansion and the additional costs associated with managing people, providing meeting space, establishing communication methods, and other intrinsic costs will help management plan for the need of additional funding.

The focus group panel recommended separating the budget process in two distinct phases: Begin with a "pilot program," then transition to a formal, permanent program. This strategy will allow the agency to work with their host city, county or state government, and recognize the potential for expansion and the need for re-evaluating the cost of doing business during the transition period.

E. COMMUNICATION METHODS

One of the goals of this research was to examine the advantages and limitations of the electronic systems fusion centers use to collaborate with program participants. This analysis ended rather quickly, as the program managers conveyed enthusiastic opposition to using electronic collaboration tools as the sole means to interact with program participants.

The consensus of the program managers and the panel is that regular face-to-face communication is fundamental to building trusting relationships and the continued involvement of participants.

In today's busy world, the popular approach is to rely upon technology as a method to make communication more efficient and easier to manage. Program managers stated that when email and websites were used as platforms to communicate, participation would start out strong, but decline rapidly over time. A combination of methods needs to be employed, including frequent dissemination of publications and emails, and regularly scheduled in-person meetings and training events, to keep the interaction between all parties vibrant and productive.

F. UNDERSTANDING THE PRIVATE SECTOR

The program managers felt that they, along with their law enforcement colleagues, all failed to fully understand how the private sector would interact with law enforcement, and what their concerns were regarding privacy issues, intellectual property rights, and the potential for corporate espionage.

Understanding that competition and realizing profits is the goal of private enterprise, and that this process is in direct conflict with the idea of the open sharing of information with the government, is the first of many issues law enforcement agencies need to address before establishing a program.

Again, obtaining training and education resources for management and staff involved in the program regarding these vital issues will be critical to the early success of the program.

G. LEADERSHIP INVESTMENT

The early involvement of law enforcement executives in private partnership initiatives is a key component to success. Program managers report that unlike many other law enforcement efforts, private outreach programs have a unique impact on the host agency, as they put business leaders in regular, direct contact with agency employees. If the agency leadership is not engaged in this interaction, business leaders

quickly become disenchanted and come to believe the agency is disinterested in their participation. In simple terms, agency executives need to show their enthusiasm for these programs by participating and leading by example. Show up to meetings, participate in round table discussions, and attend joint training. Do not establish the program if the agency leadership is not fully vested.

In addition to the findings outlined above, a "Blueprint" guide containing recommendations and smart practices generated by the program managers and members of the focus group can be found in Appendix B.

H. RECOMMENDATIONS

As mentioned earlier, the recommendations and smart practices formulated by the program managers and subject-matter experts are contained in a separate document entitled, *"A Blueprint Guide to Establishing a Public/Private Outreach Program."*

In addition to these findings, this research has produced a number of questions and concerns that should be addressed in future studies.

In general, law enforcement agencies do a poor job evaluating special programs. The difficulty of establishing accurate metrics to measure the value of relationships is one of the key reasons. Trusting relationships with the public, and other nontraditional law enforcement partner's, leads to an increased flow of tips and intelligence. This information flow has led to the prevention of crime and increased the efficiency of criminal investigations at all levels of government. Unfortunately, this information is primarily anecdotal in nature, and very few statistics are generated for this topic.

It is essential that law enforcement agencies improve the internal tracking of tips and leads, and openly report the anecdotal results as it applies to these private partnership programs. Reporting the success (or failures) of these programs with accurate data will highlight their value and bring them to the attention of key decision makers in the federal government.

Conversely, very little attention has been focused on the value these programs impart on the private sector. Again, this could be attributed to the lack of metrics.

Business leaders "feel" these programs are beneficial to the participating companies and government agencies. Interacting with law enforcement agencies, establishing emergency operations plans, and creating mechanisms to report illegal activities are all positive outcomes for the participants. These outcomes should be measured and studied in a comprehensive way to determine if the federal government should maintain funding, and even potentially expand their support for these programs.

Lastly, a comprehensive study is needed to focus on the effectiveness of electronic communication systems utilized by federal homeland security programs. Currently, different segments of the federal government (FBI, U.S. Department of Homeland Security, U.S. Department of Justice and the Military Services) use different, and often times competing electronic information sharing systems.

State and local law enforcement agencies are forced to choose between the systems, creating competition and damaged relationships. In addition, a myriad of valuable services are hosted on these systems, and if agencies align themselves with one system or another, they may be missing critical information from another agency not participating on the current system.

The federal government, or perhaps the Director of National Intelligence, should convene an intelligence-sharing panel to address this important issue. Topics to be discussed should include use by nontraditional law enforcement partners, prosecutors, and non-investigative police staff. These valuable criminal justice professionals are currently locked out of the criminal intelligence sharing cycle.

I. CONCLUSION

This research has validated the often-quoted idiom, "*The devil is in the details*." Law enforcement executives attempting to establish a private sector outreach program (and do it correctly the first time) are in for a challenging endeavor. The process of making important decisions, however, does not have to occur within a vacuum. Gifted program managers have paved the road to success, and if agency leaders take the time to analyze smart practices and recognize the dynamics of key operational components that actually make a program successful, the process can be more effective and rewarding.

APPENDIX A. PROGRAM MANAGER INTERVIEW QUESTIONS

Questions for program managers:

1. What is the size of the program (number of participants)?
2. What is the current goal of the program (Intelligence Gathering/Situational awareness/ Training?
3. Why did you start the program and what were the intended goals?
4. Who determined how the program was initially designed?
5. Did you use consultants or subject-matter experts?
6. What agencies sponsor the program?
7. What are the key features?
8. What is the geographic scope?
9. What was the total start-up cost?
10. What are the yearly operational costs?
11. How many employees are needed to manage the program?
12. Who are the participants?
13. Are particular critical infrastructure “sectors” considered as part of the process to select participants?
14. How did you (or do you) choose what critical infrastructure sectors to target with your outreach?
15. Do you target all 18?
16. How do participants approach center management about problems, complaints or concerns about the program?

17. What is the process to respond to these issues?
18. Are participants housed within your fusion center?
19. If so, who pays for their equipment and supplies?
20. If not housed within your center, how do the members participate?
21. What types of companies targeted for participation?
22. How are participants identified and chosen?
23. What types of security protocols are in place for participants?
24. How do you handle security violations with private partners?
25. Are participants required to complete a background check or receive some level of official clearance?
26. How do you address privacy concerns regarding your participants?
27. What is the physical structure of the program (In fusion center/virtual/ live meetings)?
28. What electronic collaboration tool is used?
29. How does staff communicate with participants?
30. Is a nationally recognized electronic such as HSIN or Infraguard used as a communication tool?
31. If not, what do you use?
32. What features of the system are most helpful in your outreach?
33. Does your system have an audit tool?
34. Does your system store tips and leads?
35. Does your system allow you to forward information to the FBI or other investigative agencies?

36. How do you provide technical support for the system?
37. How do you manage tips and leads generated by the participants?
38. How do you share information with the participants?
39. How is the program funded?
40. Are private funds utilized?
41. Is your program a non-profit?
42. How is funding sustained?
43. What types of products or publications does the program produce?
44. Do you have a marketing method or strategy?
45. What marketing plans have worked, and which ones have failed.
46. What types of policy documents and agreements do you employ?
47. What types of statistics do you track?
48. How do you report accomplishments?
49. What type of program oversight is in place?
50. What mistakes were made when designing the program?
51. What obstacles affected the program and how did you overcome or mitigate them?
52. Can you give an example(s) of a case or situation where partnerships were exploited to initiate a criminal investigation or solve a case?
53. What is your secret for enhancing relationships?
54. What doesn't work or has failed for you?

Focus Group Interview Questions

The focus group participants were asked to consider the following questions:

8. Would a non-profit organization designed to support a public outreach program work in Oregon?
9. What is your opinion about the importance of a policy board or oversight committee?
10. Are memorandums of understanding (MOU) or other inter-agency agreements important to establishing a law enforcement program?
11. Should all program participants be vetted?
12. Would virtual participation work for this type of program?
13. Does the manager of this type of program have to be a sworn police officer or can a civilian employee be used?
14. Most of these programs have a limited geographic scope…can a state agency handle these programs with a small number of employees?

APPENDIX B. BLUEPRINT GUIDE FOR ESTABLISHING PUBLIC/PRIVATE PARTNERSHIP PROGRAMS IN SMALL FUSION CENTERS: KEY PROGRAM COMPONENTS AND SMART PRACTICES

The following "Blueprint Guide" is a compellation of suggestions and recommendations made by subject-matter experts who have established and managed law enforcement Public/Private Partnership Programs. The material should not be considered an all-encompassing checklist, but a tool for managers to use in the planning phase of the project and to discuss and debate important topics. All suggestions made by the subject-matter experts are their personal and professional opinions, based on years of experience managing similar programs.

Building and Maintaining Relationships

- Program leaders need to set aside their egos and work to establish partnerships with the private sector. One of the key strategies is to put in the effort to understand the role of the business in the community and get a firm grasp on what the business does everyday and how it impacts the city and state. This will allow you to have meaningful conversations with business leaders, and they will see you have done your homework and understand their value.

- Program managers need to understand their partners and make a concerted effort to learn the business landscape in their area. Talking to business leaders, security professionals, and technology specialists is difficult if you do not understand their unique jargon and concerns. The only way to learn about the business environment is to get out and talk to people.

- Build and maintain a high level of credibility. Being honest, transparent, straightforward and trustworthy buys a tremendous amount of credibility currency.

- Never promise more than you can deliver. When you start a new program, and participants start to interact with your team and a level of trust is established, the participants will naturally ask for more services and products. The team's natural inclination would be to step outside of the stated mission and try to help. Try to avoid this as the everyday stress on a program involves delivering the main product, in this case complex security assessments. If dabbling in a side project reduces the main deliverable, your reputation for high quality of work will diminish.

- Follow-up after a service is delivered. This sends a message that you care, but also allows the business to share critical feedback on what parts of the program are working, and which ones do not. Management needs to review the feedback in an effort to make improvements in the program as it matures.

- Program managers and law enforcement participants need to show up to meetings and events as a team. Participants must see a team effort and cooperation between law enforcement agencies to build trust.

- Program management must keep the participants engaged and constantly sharing or the program will falter. They (private sector participants) must feel they are part of the system, have a trusting relationship with other members and the sponsoring agency members, or you will lose them.

- Allow participants to have input into the training agenda. ASK THEM what THEY want to learn. Don't always assume your best topic is the one they want or need. Customize all training to the group. Do not cookie-cutter the training.

- Program team members (law enforcement) must participate in public forums, Infragard chapter meetings, etc. Not just program managers or agency heads. Program participants want to hear from the real experts, not just the managers.

- Learn who your audience is! Work hard to create an open communication environment that builds trust. This will increase information flow and is the bedrock of any successful program.

- Lastly, you must be all-inclusive. Every business should be able to participate. Small "mom and pop" stores are often very familiar with neighborhood problems and criminal activity, but are often overlooked by law enforcement outreach programs. The common practice is to focus on the biggest employer in the region, and even though that is very important, strategic businesses in areas not traditionally targeted for these programs might be more beneficial partners. Knowing the businesses in your geographic jurisdiction, and the value they might bring to the program is critical.

Key Components and Services

- The program should only specialize in one main service. If the program has to many features or services, you lose expertise and will need additional staff to handle it.

- Be careful with participants. Attempting to recruit them as informants or intelligence sources could damage your program. If members think you are always trying to obtain information from them, they will lose trust and not participate. Leave the intelligence gathering business to your investigative and fusion center colleagues.

- Consider creating an emergency access list of subject-matter experts in all fields within your jurisdiction that can be contacted 24/7 during an emergency or crisis. Understand that business leaders usually want to help, and when they finally do receive that emergency call, they will tell everyone they know that the government reached out and asked for help. Dedication to the program is a two-way street.

- Attempt to work with existing business groups or associations. Downtown business groups, for example, are always trying to keep involved in civic issues, and crime and crime prevention issues are always important. If you can tap into an existing group, not only will you identify potential business customers, but also address security issues across a broad spectrum of businesses all in one place. Conversely, many of these groups are established based solely on the business category, for instance a technology business group. These sector-specific groups allow team members to feel the pulse of a particular sector and get a wide variety of expert opinions in one specific area.

- Provide valuable tools to participants that they can put to use immediately. For instance, the InfraGard LA team produced a model emergency operations plan that businesses can customize with very little effort. These types of tools are great for the business and they achieve immediate results.

- Consider establishing an "Infrastructure Liaison Officer Program." The InfraGard LA program created a program similar to the LAPD Archangel program. This group works in concert with the Infragard members and provides vulnerability assessments for businesses that participate in the program.

- Provide free training as often as possible. The private sector's main goal is to make money, and outside training opportunities are rarely provided. People generally are hungry for cutting-edge information, and feel engaged when they understand the threats and solutions if presented in a professional way.

- Combine resources, especially other law enforcement groups like TLO's or other first responders. If you allow these groups to mingle with the private sector, magic will happen.

- Give strong consideration to operating the program as a "liaison program" only, as a buffer between the public and law enforcement. The program should not be seen as a crime-fighting, counterterrorism unit. This training/outreach role always makes the public more comfortable and elicits more participation and engagement.

Choosing Participants

- Do not be selective of the program participants. The guy who owns the gas station is probably the guy with the best view of the world. Do not leave him out.

- Do not turn down anyone who wants to join.

- Conducting background checks on participants does not have to be a burden. It is costly (often a very high hidden cost) and is not often functionally effective. You rarely get people who do not have good intentions trying to join these programs.

Leadership

- The program must have complete political support from agency management and city or state leadership. The mindset should be, "This program is very important, our businesses and their security is very important, and you will not fail to provide this valuable service!"

- All levels of agency and government management must have a complete understanding of the program, how it works, which businesses are targeted and why. This is key as the public will ask government leaders about the program, and if the official supports the program. If business leaders feel political leadership or agency executives do not understand or hold the program in high regards, they will not play.

- Establish and maintain an engaged policy board or oversight committee. The members must take an active role in the operation and be "true believers" in the cause. Members who are there for personal enrichment must be removed as it is often obvious to members and creates a poor example.

Key Planning Strategies

- Admitting that you cannot do something is one of the most difficult things for government agency leaders to do. But when confronted with the directive to establish a program of any type, many leaders fail to look within the agency in an attempt to evaluate if they have the expertise, culture, and sustainable funding to accomplish the task at hand.

- Agency executives should start the process by asking themselves, "Are we the right agency to host this program?" Competition between jurisdictions is fierce in the law enforcement culture, especially between state and local agencies, and the federal government. For this reason, many law enforcement leaders are reluctant to admit that they might not have the capability to manage the program successfully, and perhaps a neighboring agency, jurisdiction, or federal agency might be better equipped.

- Establishing private outreach programs is difficult because police officers often have a mistrust of the private sector and may not understand the value of these partnerships. Frequently, a huge cultural shift is needed before a successful partnership can be formed between law enforcement agencies and the business community.

- Agency executives should survey agency employees to determine the level of willingness to integrate private sector employees into their operational framework. If resistance to this approach is revealed, extensive training and education of existing staff is recommended prior to bringing private sector employees into the organization.

- If this is the first time starting a new program, consider investing in a professionally designed project management software program. There are low-cost software products available to help managers project costs, track tasks and goals, and set design milestones. Many of these programs include GANT charts to help participants visually see the project components and timelines. These programs also allow you to review your progress, and when you are done, go back and debrief the design plan to help improve the plan for the next big project.

Important Agency Considerations

- Give serious consideration how your new project will affect other programs and operations inside your agency. When a new project is being implemented, everyone's eyes are on it and the agency is expending resources and manpower to get it established. But, in reality, funds and manpower are being diverted to the new program from existing programs or services. Consider the cascading affects of making decisions and how it affects other critical operations.

- Understand the premise that law enforcement does not know everything and has a lot to learn from the private sector. It is a critical mistake is to go into a business and pretend to know what they do and what the threats are. Don't be afraid to learn. It's good!

- One of the most important functions is to act in support of the local law enforcement agency! Do not alienate the locals by coming in and presenting yourself as the all-knowing expert on security issues.

Budget and Funding Considerations

- Many law enforcement executives leave the issue of budgets and budget forecasting to professional fiscal staff, and rightfully so. However, the process of determining the startup cost of a program is complicated and the importance of securing sustainable, long-term funding is often overlooked.

- Understanding the scope of the program, and the number of employees needed to interact and manage the private participants is one of the key factors to an accurate budget forecast. A careful analysis of the business community in the agency's jurisdiction, an evaluation of the existing critical infrastructure, and comparisons to other existing programs and their size and scope is critical to predicting costs.

- One of the difficulties of the budget process is attempting to forecast the growth of a program once the program is established and becomes popular. If private businesses see the program as important, more will want to join, creating the need for additional staff, supplies, and possibly office space. Anticipating expansion, and the additional

costs associated with managing people, providing meeting space, establishing communication methods, and other intrinsic costs will help management plan for the need of additional funding.

- Strongly consider separating the budget process in two distinct phases: Start with a "pilot program" then transition to a formal, permanent program. This strategy will allow the agency to work with their host city, county or state government, and recognize the potential for expansion and the need for re-evaluating the cost of doing business during the transition period.

- Consider establishing a non-profit or other mechanism to generate private funding for the program. Nationally, politicians and civic leaders do not yet understand the value of these programs and are reluctant to provide the appropriate funding. Private donations, fund raising events, and user fees are examples of ways to raise money to purchase supplies, pay for training venues, and buy needed equipment.

- With this in mind, consider utilizing private funding in <u>limited circumstances</u> where program managers can make specific purchases (such as special investigative equipment). This direct purchase strategy, coupled with transparent accounting practices should thwart public concerns about the misuse of donated funding.

<u>Communication Methods</u>

- Regular face-to-face communication is fundamental to building trusting relationships and the continued involvement of participants.

- In today's busy world, the popular approach is to rely upon technology as a method to make communication more efficient and easier to manage. A combination of methods needs to be employed, including frequent dissemination of publications and emails, and regularly scheduled in-person meetings and training events, to keep the interaction between all parties vibrant and productive.

- Social media and websites are important in today's technological world. If you do not have a website or some type of alternative media position, you will lose out on potential participants. websites are the easiest way to reach people with a minimal amount of staff. The content on the sites can include marketing information, meeting announcements, and training opportunities. (But do not forget that face-to-face communication is still critical).

- If possible, send your publications and bulletins directly to the user. Do not just post them on a website and force them to log-on to access them. People are too busy and want the convenience of receiving publications by email.

BIBLIOGRAPHY

"A Summary of Fusion Centers: Core Issues and Options for Congress – Open CRS," 2012. http://opencrs.com/document/RL34177/2007–09–19/.

Berkeley, Alfred R. *Intelligence Information Sharing: Final Report and Recommendations*. Washington, DC: National Infrastructure Advisory Council, 2012.

Carter, David L., and Jeremy G. Carter. "The Intelligence Fusion Process for State, Local and Tribal Law Enforcement." *Criminal Justice and Behavior* 13 (2009): 1323.

Chambers, John T. *Public-Private Sector Intelligence Coordination*. Washington, DC: National Infrastructure Advisory Council, 2006.

DHS-HSAC. *Homeland Security Advisory Council, Private Sector Information Sharing Task Force: On Information Sharing between Government and the Private Sector-Final Report*. Washington, DC: U.S. Department of Homeland Security, 2005.

Duarte, Nestor and Naval Postgraduate School. *Unleashing Our Untapped Domestic Collection is the Key to Prevention*. Monterey, California: Naval Postgraduate School, 2007. http://edocs.nps.edu/npspubs/scholarly/theses/2007/Sep/07Sep%5FDuarte.pdf; http://handle.dtic.mil/100.2/ADA473968.

Gutierrez, Michael J. *Intelligence and High Intensity Drug Trafficking Areas (HIDTA's)*. Monterey, Calif.; Springfield, Va.: Naval Postgraduate School; Available from National Technical Information Service, 2004.

Heirston, Bryan. "Firefighters and Information Sharing; Smart Practice Or Bad Idea." *Homeland Security Affairs Journal* 6, no. 2 (May 2010).

Homeland Security Advisory Council. *Private Sector Information Sharing Task Force; on Information Sharing between Government and the Private Sector-Final Report*. Washington, DC: U.S. Department of Homeland Security, 2005.

"Intelligence and Information-Sharing Elements of S. 4 and H.R. 1 – Open CRS," 2012. http://opencrs.com/document/RL34061/2007–06–26/.

The International Association of Law Enforcement Intelligence Analysts and the Law Enforcement Intelligence Unit. *Intelligence 2000: Revising the Basic Elements, A Guide for Intelligence Professionals*, Sacramento, CA, 2000, 60–61.

Logan, Keith Gregory. *Homeland Security and Intelligence*. Santa Barbara, Calif.: Praeger Security International, 2010.

"More about Fusion Centers | American Civil Liberties Union," 2011. http://www.aclu.org/spy-files/more-about-fusion-centers.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report, Authorized Edition*. New York: W.W. Norton, 2004.

Newkirk, Anthony B. "The Rise of the Fusion-Intelligence Complex: A Critique of Political Surveillance After 9/11." *Surveillance & Society* 8, no. 1 (2010): 43.

O'Neil, Siobhan. "The Relationship between the Private Sector and Fusion Centers: Potential Causes for Concern and Realities." *Homeland Security Affairs Journal* no. Supplement 2 (2008).

Oregon Department of Justice, Criminal Justice Division, www.osin.info, accessed on 10/17/12.

Petrie, Michael. "Use of EMS Personnel as Intelligence Sensors: Critical Issues and Recommended Practices." *Homeland Security Affairs Journal* 3, no. 3 (September 2007).

Regional Information Sharing Systems (RISS), Murfreesboro TN, Agency website: http://www.riss.net/.

"Report - What's Wrong with Fusion Centers? American Civil Liberties Union," 2011. http://www.aclu.org/technology-and-liberty/report-whats-wrong-fusion-centers.

Shepherd, Dave. "Role of the Private Sector in Fusion Centers." *Security* 48, (January 2011).

Simeone, Matthew J. and Naval Postgraduate School. *The Integration of Virtual Public-Private Partnerships into Local Law Enforcement to Achieve Enhanced Intelligence-Led Policing*. Monterey, California: Naval Postgraduate School, 2007.

Straw, Joseph. "Fusion Centers: Smashing Intelligence Stovepipes." *Security Management* 53, no. 3 (2008).

"Terrorism Information Sharing and the Nationwide Suspicious Activity Report Initiative: Background and Issues for Congress - Open CRS," 2012. http://opencrs.com/document/R40901/2009–11–05/.

United States Department of Homeland Security. *Automated Critical Asset Management System*, Washington, DC, Official Agency website: http://www.dhs.gov/automated-critical-asset-management-system-acams.

———. *Integrating Critical Infrastructure and Key Resources Protection Capabilities into Fusion Centers, Development and Implementation Considerations, Version 1.0*. Washington, DC: U.S. Department of Homeland Security, 2011.

———. *Homeland Security Information Network*, Washington, DC, Agency website: http://www.dhs.gov/homeland-security-information-network.

———. *If You See Something, Say Something Campaign*, Washington, DC, Official Agency website: http://www.dhs.gov/if-you-see-something-say-something-campaign.

———. NFCG. *National Fusion Center Guidelines*. Washington, DC: U.S. Department of Homeland Security, 2006.

United States Department of Homeland Security and the United States Department of Justice. Fusion Process Technical Assistance Program and Services *Establishing a Fusion Liaison Officer Program, Development and Implementation Considerations*, Washington, DC, August 2010, version 1.2.

———. *Fusion Process Technical Assistance Program and Services Integrating Critical Infrastructure and Key Resources Protection Capabilities into Fusion Centers, Development and Implementation Considerations*, Washington, DC, April 2011

United States Department of Justice-ISE. *U.S. Information Sharing Environment, Guideline 2*. Washington, DC: U.S. Government, Office of the President, 2006.

United States Department of Justice-NCISP. *National Criminal Intelligence Sharing Plan*. Washington, DC: U.S. Department of Justice, Bureau of Justice Assistance, 2009.

United States Federal Bureau of Investigation. *FBI Infragard System*, Washington, DC, Agency website: http://www.infragard.net/, accessed 8/31/12.

United States Library of Congress. Congressional Research Service. *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by Rollins John and Anna C. Henning. CRS Report R40427. Washington, DC: Office of Congressional Information and Publishing, March 10, 2009.

———. Congressional Research Service. *Fusion Centers: Core Issues and Options for Congress*, by Todd Masse, Siobhan O'Neil, and John Rollins. CRS Report RL34177. Washington, DC: Office of Congressional Information and Publishing, September 19, 2007.

———. Congressional Research Service. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches,* by Mark A. Randol. CRS Report RL33616. Washington, DC: Office of Congressional Information and Publishing, January 14, 2009.

———. Congressional Research Service. *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches,* by Todd Masse. CRS Report RL34070. Washington, DC: Office of Congressional Information and Publishing, September 2007.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Oregon Department of Justice
   Oregon TITAN Fusion Center
   Chuck Cogburn, Director
   Salem, Oregon

4. Oregon HIDTA Program
   Chris Gibson, Director
   Salem, Oregon