NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

AN INTELLIGENCE-SHARING CONTINUUM: NEXT GENERATION REQUIREMENTS FOR U.S. COUNTERTERRORISM EFFORTS

by

David Carabin

September 2011

Thesis Advisor:	Robert Simeral
Second Reader:	Patrick Miller

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** September 2011	**3. REPORT TYPE AND DATES COVERED** Master's Thesis	
4. TITLE AND SUBTITLE An Intelligence-sharing Continuum: Next Generation Requirements for U.S. Counterterrorism Efforts			**5. FUNDING NUMBERS**
6. AUTHOR(S) David Carabin			
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 September 11, 2001 terrorist attacks were a major catalyst for intelligence reform in the United States. Since this date, most government agencies have strived to evolve and advance in this capacity. One such way has been through the development of multi-agency, multi-disciplinary intelligence centers, such as the National Counterterrorism Center, the Interagency Threat Assessment and Coordination Group, and the 72 state and major urban area fusion centers established throughout the nation. However, despite the changes that have occurred throughout the U.S. intelligence and law enforcement communities, significant issues still remain that are impeding the creation and flow of actionable intelligence to support domestic counterterrorism efforts. This has been identified from research conducted on numerous sources. Several policy, technological, cultural and political challenges exist, all contributing to the less-than-perfect nature of the United States' existing counterterrorism framework.

This thesis aims to identify potential solutions that leverage existing intelligence operations to promote an intelligence-sharing continuum across all tiers of U.S. government. The author provides an analysis of specific, priority issues that require fixing within our nation's counterterrorism system, and provides evidence-based recommendations to improve the capability and value of existing intelligence support structures and further-develop the desired intelligence-sharing continuum.

14. SUBJECT TERMS Fusion center, Interagency Threat Assessment and Coordination Group, intelligence requirements, information sharing, National Counterterrorism Center, terrorism, law enforcement, Department of Homeland Security, Federal Bureau of Investigations, analysis, September 11, 2001			**15. NUMBER OF PAGES** 169
			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

AN INTELLIGENCE-SHARING CONTINUUM: NEXT GENERATION REQUIREMENTS FOR U.S. COUNTERTERRORISM EFFORTS

David Carabin
Director, Boston Police Department
B.S., Westfield State College, 2002

Submitted in partial fulfillment of the
requirements for the degree of

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

from the

NAVAL POSTGRADUATE SCHOOL
September 2011

Author: David Carabin

Approved by: Robert Simeral
Thesis Advisor

Patrick Miller
Second Reader

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

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The September 11, 2001 terrorist attacks were a major catalyst for intelligence reform in the United States. Since this date, most government agencies have strived to evolve and advance in this capacity. One such way has been through the development of multi-agency, multi-disciplinary intelligence centers, such as the National Counterterrorism Center, the Interagency Threat Assessment and Coordination Group, and the 72 state and major urban area fusion centers established throughout the nation. However, despite the changes that have occurred throughout the U.S. intelligence and law enforcement communities, significant issues still remain that are impeding the creation and flow of actionable intelligence to support domestic counterterrorism efforts. This has been identified from research conducted on numerous sources. Several policy, technological, cultural and political challenges exist, all contributing to the less-than-perfect nature of the United States' existing counterterrorism framework.

This thesis aims to identify potential solutions that leverage existing intelligence operations to promote an intelligence-sharing continuum across all tiers of U.S. government. The author provides an analysis of specific, priority issues that require fixing within our nation's counterterrorism system, and provides evidence-based recommendations to improve the capability and value of existing intelligence support structures and further-develop the desired intelligence-sharing continuum.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
- A. PROBLEM STATEMENT....1
- B. RESEARCH QUESTION....4
- C. RESEARCH SIGNIFICANCE....4
- D. LITERATURE REVIEW....4
  - 1. Fusion Center Development—Past to Present....5
  - 2. Fusion Center Missions and Designs....6
- E. INFORMATION SHARING....7
  - 1. Insufficient Information-Sharing Channels....8
- F. LITERATURE QUALITY....9
- G. METHODOLOGY....10
- H. CHAPTER SUMMARY....11

II. TRANSFORMATION: THE U.S. RESPONSE TO THE EVOLVING THREAT ENVIRONMENT....13
- A. THE POST-SEPTEMBER 11, 2001, THREAT ENVIRONMENT....13
- B. INTELLIGENCE....15
- C. ORGANIZATIONAL INTELLIGENCE REFORM....20
  - 1. Federal Reform....20
  - 2. State and Local Reform....22

III. ENHANCED INTELLIGENCE SUPPORT STRUCTURES TO COUNTER THE TERRORIST THREAT....25
- A. STATE AND MAJOR URBAN AREA FUSION CENTERS....25
- B. NCTC—THE U.S. 'FUSION CENTER' OF TERRORISM-RELATED INTELLIGENCE....29
- C. THE GOLDEN THREAD TO THE INTELLIGENCE COMMUNITY?....31
  - 1. Information Sharing Environment....31
  - 2. ITACG Detail....34

IV. METHODOLOGY....39
- A. TRIANGULATION....39
- B. THE DELPHI METHOD....40
  - 1. Thesis Intelligence Delphi Panel....43
  - 2. Questionnaire 1....44
  - 3. Questionnaire 2....46

V. WHAT IS WRONG WITH FUSION CENTERS?....47
- C. INTELLIGENCE PRODUCTION, SHARING, AND SATISFACTION....49
- D. INTELLIGENCE CYCLE....51
  - 1. Planning, Requirements, and Collection....51
  - 2. Synthesis and Analysis, Dissemination, and Feedback....53

VI. FEDERAL INTELLIGENCE-SHARING CHALLENGES 57
A. FEDERAL AGENCY SUPPORT TO STATE AND LOCAL OFFICIALS 58
B. NCTC: STATE AND LOCAL SUPPORT? 62
C. ITACG: THE MISSING LINK? 66
1. Past and Present Challenges 66
D. CONCLUSION 76

VII. RECOMMENDATIONS: MAKING FUSION CENTERS WORK 79
A. THE PUBLIC SAFETY "MEGACOMMUNITY" 79
1. Collaboration 79
2. Capabilities and Limitations 84
3. Development of Intelligence Liaison Officer Programs 86
B. CONCLUSION 91

VIII. IMPROVING THE FEDERAL MODEL: ADVANCING THE INTELLIGENCE-SHARING CONTINUUM BY HARNESSING THE ITACG 93
A. MULTI-LEVEL LEADERSHIP 95
B. OVERHAULING THE DIGITAL BACKBONE OF THE CONTINUUM 99
C. ENHANCING HUMAN CAPITAL: PHASE 2, POST-DETAIL DEPLOYMENT 103
1. Extending Joint-Duty: Integrating Elements from Both Sides of the Continuum to Enhance Knowledge, Skills and Abilities ... 106
5. Joint Duty Case Study: Boston ODNI RASER Team 108
D. CONCLUSION 111

APPENDIX DELPHI PANEL 117
A. DELPHI PANEL: QUESTIONNAIRE 1 FEBRUARY 13, 2008 117
B. DELPHI PANEL: SUMMARY OF RESPONSES PROVIDED FOR QUESTIONNAIRE 1 MARCH 16, 2008 118
C. DELPHI PANEL: QUESTIONNAIRE 2 MARCH 27, 2008 125
D. DELPHI PANEL: SUMMARY OF RESPONSES PROVIDED FOR QUESTIONNAIRE 2 MAY 7, 2008 132

LIST OF REFERENCES 145

INITIAL DISTRIBUTION LIST 153

LIST OF FIGURES

Figure 1. The Intelligence Cycle 17
Figure 2. Intelligence Collection Disciplines 19
Figure 3. Common Intelligence Product Categories 20
Figure 4. National Network of Fusion Centers 27
Figure 5. Office of the Director of National Intelligence and Coordination with the Intelligence Community: 32
Figure 6. Information-sharing Environment: Framework for Sharing Information with SLTTP Partners.....33
Figure 7. ITACG Intelligence Product Augmentation Methodology.....36
Figure 8. Information Sharing Complexity 63
Figure 9. ITACG Facilitated Dissemination Procedure 71
Figure 10. Example of Roll Call Release 74
Figure 11. ITACG Intelligence Guide for First Responders 75
Figure 12. Public Safety Megacommunity Stakeholder Matrix.....83
Figure 13. Public Safety Megacommunity.....91
Figure 14. ITACG Coordinated Dissemination 102
Figure 15. ITACG Local Collection and IC Integration Model.....105
Figure 16. Intelligence Community with SLTT Joint Duty Participation.....107
Figure 17. Public Safety Megacommunity with Enhanced Fusion Center 111
Figure 18. Recommended Model with Intelligence-Sharing Continuum 115

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

9/11	September 11, 2001
9/11 Act	Implementing Recommendations of the 9/11 Commission Act of 2007
CIA	Central Intelligence Agency
CRS	Congressional Research Service
DHS	Department of Homeland Security
DOJ	Department of Justice
FBI	Federal Bureau of Investigations
Global	Global Justice Information Sharing Initiative
HIR	Homeland Information Reports
HS-SLIC	Homeland Security—State and Local Intelligence Community
HSDN	Homeland Secure Data Network
HSIN	Homeland Security Information Network
HVE	Homegrown Violent Extremist
I&A	Office of Intelligence & Analysis
IC	Intelligence Community
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISE	Information Sharing Environment
ITACG	Interagency Threat Assessment and Coordination Group
JTTF	Joint Terrorism Task Force
LES	Law Enforcement Sensitive
MOA	Memorandum of Agreement
NCTC	National Counterterrorism Center
NGA	National Governors Association
NIE	National Intelligence Estimate
NIS	National Intelligence Strategy for the United States of America
NOL-S	NCTC Online SECRET
NSA	National Security Agency
ODNI	Office of the Director of National Intelligence

PERF	Police Executive Research Forum
PM ISE	Program Manager Information Sharing Environment
SBU	Sensitive But Unclassified
SLTTP	State, Local, Tribal, Territorial and Private Sector
TS/SCI	Top Secret/Sensitive Compartmented Information
U.S.	United States of America
U.S. GAO	United States Government Accountability Office
WMD	Weapons of Mass Destruction

ACKNOWLEDGMENTS

First and foremost, I would like to thank my family for tolerating the demands producing this thesis imposed upon our family life. To my friends: thank you for standing by me after I disappeared from your lives for so long while completing the requirements of this program. A very large debt of gratitude is owed to Naval Postgraduate School Center for Homeland Defense and Security faculty and staff, as the superior education they provided opened doors to a whole new world for me, both personally and professionally. Without the motivation and relentless encouragement of Dr. Christopher Bellavita, the guidance of Captain Robert Simeral and Chief Patrick Miller, and the brainstorming sessions with Dr. Lauren Wollman, I would not have completed this thesis. To my current and former colleagues at Boston Police Department, especially Carl Walter: thank you for providing me the opportunity to attend this program during such a critical time in the operational development of the Boston Regional Intelligence Center. To Keith Squires and Jeff Carr: thank you for recognizing my potential and giving me the chance to leverage the knowledge gained through this education to develop the foundations of the Utah Statewide Information & Analysis Center. Last, but not least, to Dr. Kate Loring, Robert Benjamin, and Moray Cucchiari: thank you for your time, guidance, patience, and encouragement—without you this education would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

A. PROBLEM STATEMENT

In the years leading up to September 11, 2001, there were serious problems with the way that terrorism information was exchanged amongst federal, state, and local law enforcement and intelligence agencies. The 9/11 Commission honed in on this shortcoming and identified the need for better information-sharing practices among all levels of government in order to prepare for and prevent future terrorist attacks within the United States. The *9/11 Commission Report* is filled with references that clearly demonstrated the Commission's focus on issues related to information sharing and analysis. One such reference states that "the biggest impediment to all-source analysis—to a greater likelihood of connecting the dots—is the human or systemic resistance to sharing information."[1]

Over the last 10 years, there has been a process of transformation taking place across the various tiers of the U.S. government in order to bolster counterterrorism efforts and improve the information and intelligence sharing. The impetus behind this transformation was the *Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)*. The Act restructured the U.S. Intelligence Community (IC) and mandated processes to improve information sharing amongst the IC, state and local officials, and other critical stakeholders. In addition, the law included several of the initiatives suggested in the *9/11 Commission Report*.[2]

Most government agencies have strived to evolve and advance in this capacity; one such way has been through the development of multi-agency, multi-disciplinary intelligence centers, such as the National Counterterrorism Center (NCTC) and the 72 state and major urban area fusion centers (fusion centers) established throughout the

---

[1] National Commission on Terrorist Attacks upon the United States, *Final Report of the National Commission on Terrorist Attacks upon the United States* (New York: W.W. Norton & Company, 2004), 416–417.

[2] *Intelligence Reform and Terrorism Prevention Act of 2004*, Public Law 108-458, 108th Cong., 1st Sess. (December 2004).

nation. Moreover, the Office of the Director of National Intelligence (ODNI) designated a Program Manager (PM ISE) responsible for the development of the Information Sharing Environment (ISE); more recently, the United States Congress mandated the creation of the Interagency Threat Assessment and Coordination Group (ITACG), and former President Bush issued the first *National Strategy for Information Sharing*. Many of these developments are relatively new, and therefore have yet to be comprehensively implemented or thoroughly tested. Despite the new models, laws, and practices that have emerged from recent initiatives, information processing, and sharing has improved but is not yet to a satisfactory level. The October 2007 *National Strategy for Homeland Security* acknowledges this fact, as significant obstacles still remain that are affecting horizontal and vertical information sharing between federal, state, and local agencies.[3] Furthermore, the near success of accused terrorist Umar Farouk Abdulmutallab on Christmas Day 2009 indicates that there is still much room for improvement.

Some of America's most critical assets for collecting, collating, analyzing, and sharing terrorism-related information and intelligence appear to be falling short of expectations. The NCTC was established to be the primary government organization responsible for providing national coordination of foreign and domestic terrorism and counterterrorism analyses, intelligence production, and strategic operations.[4] Additionally, the NCTC is responsible for disseminating transnational terrorism information and threat analyses to the Executive Branch and for supporting the Department of Homeland Security (DHS), Department of Justice (DOJ), and other federal agencies as they fulfill their responsibility to disseminate terrorism information to state and local agencies.[5] While the NCTC is comprised of several IC and federal agencies, it has no state or local representation. Consequently, the majority of the NCTC's support has been provided to the IC and high-ranking government officials; little direct assistance has been provided to fusion centers, as its mission is not intended to

---

[3] Homeland Security Council, *National Strategy for Homeland Security* (Washington D.C.: Homeland Security Council, 2007), 7.

[4] Executive Order 13354: National Counterterrorism Center, *Federal Register* 69, no. 169 (August 2004).

[5] Ibid.

directly support state and local agencies.[6] According to a 2006 self-assessment study of the NCTC, "methods for ensuring that homeland security and terrorism information is shared among non-Federal Government entities and the Federal Government remains inadequate."[7] This highlights the perpetual challenge of horizontal and vertical information sharing from this center. At the state and local level, fusion centers are best positioned to distribute useful intelligence, gathered both locally and from federal sources, to the widest and most appropriate audience. According to DHS:

> State and major urban area fusion centers serve as primary focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information among federal, state, local, tribal, and territorial (SLTT) partners. Located in states and major urban areas throughout the country, fusion centers are uniquely situated to empower frontline law enforcement, public safety, fire service, emergency response, public health, and private sector security personnel to lawfully gather and share threat-related information.[8]

Currently, gaps exist disrupting the flow of useful intelligence from the IC, and leaders from both fusion centers and the IC have yet to collaborate to establish a "best practice" for the tailoring and dissemination of terrorism related intelligence to state and local consumers. As a result, the "boots on the ground," the approximate 800,000 state and local police officials, and the hundreds of thousands of additional public safety and private sector security personnel, best suited to be the eyes and ears for counterterrorism support, can be left uninformed and lacking much-needed guidance regarding current threats. Additionally, those agencies producing and analyzing intelligence are still—perhaps inadvertently—acting as information silos, as the information needed by those in the field remains locked up behind closed doors.

---

[6] Patience Wait, "Where the Data Meets the Road," *Government Computer News*, August 9, 2005, http://www.gcn.com/print/24_25/36781-1.html (accessed March 2, 2008).

[7] National Counterterrorism Center, *NCTC and Information Sharing: Five Years Since 9/11: A Progressive Report* (Washington, D.C.: National Counterterrorism Center, 2006), www.nctc.gov/docs/report_card_final.pdf (accessed March 2, 2008), 10.

[8] U.S. Department of Homeland Security, "Fusion Center Fact Sheet," http://www.dhs.gov/files/programs/ (accessed February 12, 2011).

B. RESEARCH QUESTION

What practices and processes should be implemented among state and major urban area fusion centers and the IC to promote an intelligence-sharing continuum and make fusion centers more effective in meeting the needs of their consumers?

C. RESEARCH SIGNIFICANCE

This thesis aims to examine practices and processes that have to be effective in connecting fusion centers to both federally- and locally-derived intelligence to improve public safety and national security. Furthermore, it seeks to demonstrate how national, state, and regional intelligence support can be leveraged to make a fusion center more effective in satisfying the needs of its intelligence consumers. As such, the research conducted will benefit the U.S. government (all levels) and private and public sector entities that are consumers of and contributors to fusion center-generated intelligence. Homeland security practitioners and national leaders will benefit from this research through a greater understanding of the role state and local agencies play in our nation's domestic counterterrorism efforts.

D. LITERATURE REVIEW

There is a dearth of literature related to state and local fusion centers owing to their relatively new emergence in the homeland security arena, which began taking shape shortly after the September 11, 2001 terrorist attacks. In contrast, literature regarding information-sharing deficiencies between federal agencies and state and local officials is vast; this comes as no surprise considering the fact that a major discovery in the *9/11 Commission Report* was related to failures in information sharing amongst all agencies and levels of government.

For the purposes of this thesis, the literature can be separated into five categories:

1. Documents written by federal, state, and local government committees to be used as guidelines for counterterrorism information sharing and fusion center processes, development, and operations.

2. Reports written by government-sponsored agencies as evaluations of information sharing and fusion center development, operations, policies, and strategies.
3. Congressional testimony of federal officials and fusion center administrators regarding the need for improved federal information-sharing processes and practices.
4. Transcripts of speeches by high-ranking officials regarding fusion centers and their role in homeland security.
5. Articles written by academics and reporters/news media regarding deficiencies in information sharing, and the purpose and progress of fusion centers.

1. Fusion Center Development—Past to Present

Fusion center development began around 2003, and, initially, the few that were built were strictly for counterterrorism purposes. To date, 72 fusion centers have been established throughout the country.[9] Research suggests that there is no "cookie cutter" approach to the development and operation of these centers; therefore, there are significant differences between them.[10] As the evolution of fusion centers has continued, they have become more "crime" and "hazards" focused and structured and oriented according to the needs of the jurisdiction the center serves. Some researchers believe that this movement is eclipsing antiterrorism information and analysis functions as more fusion centers focus efforts on criminal intelligence.[11]

There are several events and publications that appear to have been catalysts for much of the recent fusion center development. In surveys published by the National Governors Association (NGA) in 2005, 2006, and 2007, "developing a state intelligence fusion center," and "using fusion centers for intelligence collection, analysis, dissemination and intelligence sharing among federal, state, and local governments,"

---

[9] U.S. Department of Homeland Security, "Activities & Programs: State and Local Fusion Centers," http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm (accessed March 30, 2008).

[10] Todd Masse, Siobhan O'Neil, and John Rollins, *Fusion Centers: Issues and Options for Congress* (Washington, D.C.: Congressional Research Service, 2007), www.fas.org/sgp/crs/intel/RL34070.pdf (accessed September 9, 2007), 19.

[11] Alice Lipowicz, "CRS: Mission Creep at Fusion Centers," *Government Computer News*, July 9, 2007, http://www.gcn.com/online/vol1_no1/44629-1.html (accessed August 10, 2007).

ranked among the organization's top recommendations.[12] Moreover, the Homeland Security Advisory Council (HSAC) recommended in 2005 that each state, "…establish an information center that serves as a 24/7 all source, multi-disciplinary, information fusion center." This trend has continued as the years have progressed:[13]

In July of 2007, the Chairman of the House Homeland Security Committee stated:

> The nationwide network of fusion centers intended to gather counterterrorism intelligence is suffering from a lack of direction from the Homeland Security Department. Because of a lack of effective federal leadership, however, state and local [agencies] have taken it upon themselves to create these centers with varying levels of success.[14]

It was not until September of 2008 that minimum standards—which came in the form of guidelines—were created to ensure that fusion centers operated efficiently, are being built to interact with other fusion centers as a network, are being designed to sustain possible future budget deficits, or are meeting the needs of state and local intelligence consumers.[15] Still, many have little private sector input, encounter difficulties with the classification of information, and have limited access to relevant information databases.[16] Additionally, many suffer from what they consider a lack of actionable, specific intelligence generated from federal sources regarding threats posed to their jurisdictions.

2. Fusion Center Missions and Designs

The latest reports written by government-sponsored agencies indicate that fusion centers apply a variation of four primary roles and responsibilities to their respective missions: an orientation towards "all crimes," an orientation towards "all hazards," a combination of both, or a strictly counterterrorism focus. Some centers are oriented

---

[12] Masse, O'Neil, and Rollins, *Fusion Centers*, 18.

[13] Ibid, 19.

[14] Wilson Dizard III, "Study: Flaws in Fusion Centers," *Government Computer News*, July 30, 2007, http://www.gcn.com/print/26_19/44738-1.html?topic=state-local (accessed August 10, 2007).

[15] Global Justice Information Sharing Initiative, U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers* (Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2008).

[16] Lipowicz, "CRS: Mission Creep at Fusion Centers."

towards prevention, while others are focused on response and recovery. According to a July 2007 Congressional Research Service (CRS) report, each fusion center's interpretation of the aforementioned focus areas differs, resulting in different products and operations.[17] Fusion centers are mostly "grassroots" establishments, and with that, each center's development is dependent on the needs of the state or region in which the fusion center is operated. Where each state or region has identified its own risks, threats, and vulnerabilities, their respective fusion center has been designed to serve functions fit for these identified areas. However, it is unclear at this time whether or not those working at fusion centers have in fact adequately identified the most significant risks, threats, and vulnerabilities within their jurisdictions, or are sufficiently fulfilling their missions to mitigate them.[18]

Evaluations and reports suggest that the vast majority of fusion centers have been built at the state level. Additionally, the number of fusion centers within one state varies from two to eight, which has given rise to recent literature debating the practicality of implementing multiple centers within one state.[19] Policymakers and evaluators are cautious about the competition for resources between same-state centers and about the possibility of creating multiple intelligence silos within one state due to a lack of information sharing. However, research suggests the effective interaction and collaboration between multiple agencies and disciplines that is in practice at regional fusion centers appears to justify their existence within a state that already has a "state" fusion center.[20]

E. INFORMATION SHARING

While information-sharing strategies have improved since the September 11, 2001 terrorist attacks, they have not yet reached an adequate level of satisfaction amongst most

---

[17] Masse, O'Neil, and Rollins, *Fusion Centers*, 19.

[18] Lehew Miller and David Carabin, "Perspectives from the Field on the 2010 Baseline Capabilities Assessment" (Presented at the Critical Operational Capabilities Gap Mitigation Workshop, Washington, D.C., August 24–25, 2010).

[19] Masse, O'Neil, and Rollins, *Fusion Centers*, 23.

[20] Ibid., 20.

stakeholders. Current literature illustrates a clear sentiment of dissatisfaction with the effectiveness of information sharing between the federal government and state and local officials. During the last nine years, information sharing has been hampered by a number of impediments that recent legal enhancements and organizational changes have not been able to fix thus far. Some of the most recognized issues are related to information security classifications, the absence of standards for "sensitive but unclassified" (SBU) information, inadequate information-sharing channels, and a lack of specific and/or actionable intelligence products provided to state and local stakeholders from the IC.

1. Insufficient Information-Sharing Channels

Efforts have been made, to different degrees of success, to create Internet portals for sharing unclassified information between various levels of government, agencies, and fusion centers. Such portals have helped bring counterterrorism and threat information to the computers of those working at fusion centers across the nation. However, numerous sources indicate that these information-sharing portals, in their current state, have not provided an acceptable solution to improve information sharing.

According to recent literature, the overabundance of information-sharing portals has proven to be problematic. As stated in a testimony before the House Homeland Security Committee:

> What has resulted [from efforts to improve information sharing] is a wide variety of information sharing systems that in many cases republish the same information. Having to view multiple systems is labor intensive, time consuming and after a period of time loses its value.[21]

Analysts working at fusion centers have to log on to multiple portals each day to read the most recent threat reporting and gather the complete spectrum of available information that has been provided by various agencies in the different systems. At a Congressional hearing, discontent was expressed about the fact that federal agencies have

[21] Norman Beasley, "The Way Forward with Fusion Centers: Challenges and Strategies for Change," *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, 110th Cong., 1st sess., September 27, 2007, http://www.fas.org/irp/congress/2007_hr/092707beasley.pdf (accessed October 16, 2007).

yet to consolidate the numerous information-sharing systems that currently exist, which is necessary to help streamline daily processes for gathering threat information at fusion centers.[22]

Most agree that it is time to identify "a primary federal agency responsible for the reception and dissemination of terrorism-related information to and from local and state fusion centers."[23] The NCTC is likely best suited to facilitate this function, with the support of the ITACG and DHS.[24]

F. LITERATURE QUALITY

The various categories of literature specific to fusion centers provide researchers with a comprehensive review of what has taken place in the last nine years of fusion center development; however, the literature falls short in areas of future development. While many sources are quick to point out that fusion centers are not effectively "fusing" counterterrorism data as expected and that they are relying too heavily on the federal government for support, before 2009 very little was written to suggest strategies to correct these issues. Documents existed that were viewed as a broad framework for fusion center development and operation; however, until recently, updates were not provided to show what from these documents should be standardized to ensure effective functions or what should or should not be implemented based on the experiences of those in the field.

The CRS report, *Fusion Centers: Issues and Options for Congress*, is one of few initial documents that provided direction for future fusion center development.[25] This report suggests a national strategy for fusion centers and calls for a networked approach for "second generation" fusion efforts. Additionally, it offers a variety of strategies for

---

[22] Ben Bain, "Confusion Over Fusion Centers," *Federal Computer Week*, October 8, 2007, http://fcw.com/Articles/2007/10/04/Confusion-over-fusion-centers.aspx?p=1 (accessed October 10, 2007).

[23] Kenneth Bouche, "State and Local fusion Center and the Role of DHS," *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, 109th Cong., 2nd sess., 2006, http://www.fas.org/irp/congress/2006_hr/090706bouche.pdf (accessed October 16, 2007).

[24] Beasley, "The Way Forward with Fusion Centers."

[25] Masse, O'Neil, and Rollins, *Fusion Centers*.

Congress to consider regarding future support to fusion centers, including recommendations regarding the ITACG, which is rare amongst the other documents of its kind.

On the topic of information sharing, the literature conveys a message that state and local fusion centers are at a loss without efficient aid from a national intelligence support structure capable of sharing information regarding threats collected and analyzed from a national perspective. While fusion centers may be in an excellent position to provide an effective means of sharing information with state and local stakeholders, the efforts will fall short without an effective process for sending and receiving information from the IC. As stated in one Congressional testimony:

> The critical link in the overall National intelligence process is the agencies that are closest to their communities... The challenge faced by the National Intelligence Community is how to establish real time linkages between state and local agencies that allows both receiving information from and providing information to their fusion centers.[26]

G. METHODOLOGY

To execute the requirements of this thesis, the author used a triangulation methodology and analyzed various organizational structures, policies, practices, and initiatives to identify strengths and weaknesses based both against what they are intended to be doing (both independently and in coordination), and what they are actually doing. The triangulation methodology assists researchers in the synthesis and integration of multiple data and information sources for evaluation and ultimately, policy recommendations.[27] Triangulation can make use of pre-existing data and information, allowing for a rapid understanding of a given situation to expedite decision-making. By examining information collected by different people and methods, and both qualitative and quantitative studies, making use of expert judgments, the resultant findings can corroborate each other and reduce the effect of both systematic bias and random error

---

[26] Ibid.

[27] World Health Organization, *Overview of Triangulation Methodology: Synthesis of Multiple Data Sources for Evaluation and Decision-making in HIV Epidemics, Based on Initial Experiences*, http://www.searo.who.int/LinkFiles/Facts_and_Figures_08Tri-Resource_Guide_Generalized.pdf (accessed February 12, 2011), 7–8.

present in a single study.[28] Using triangulation can make findings more robust, as it is a means for combining research methods to give a range of perspectives.[29] Gap analyses are utilized to assess an organization's current capabilities in comparison with its potential and to determine what is leading to the identified disparity, or "gap." Gap analyses were used in this thesis to identify and isolate the issues that are contributing to inadequate intelligence production and information sharing at state and local fusion centers.

Additionally, the author coordinated a Delphi panel that consisted of 22 intelligence professionals from federal, state, local, and private sector organizations. The Delphi method is a structured communication process for collecting and refining knowledge from a group of experts by means of a series of questionnaires and controlled feedback; it is a technique that is often used when there is a complex problem, a lack of knowledge available to answer a research question, and when anonymity is necessary.[30] A total of two iterations of questionnaires were created, disseminated, and analyzed for the purpose of identifying problems in the national counterterrorism intelligence system and fixing the problems.

H. CHAPTER SUMMARY

Chapters II and III were written to provide the reader with a background of the various laws, strategies, and organizational roles that combine to provide national security for the United States in response to the threat posed by international terrorism. Chapter IV gives a detailed description of the methodology used to analyze the problems disrupting intelligence production and sharing, while Chapters V and VI present the analytic findings. The final policy recommendations are illustrated in Chapters VII and VII, providing the reader with prospective solutions to increase the efficiency of both

---

[28] World Health Organization, *Overview of Triangulation Methodology*.

[29] United Nations World Food Program, Office of Evaluation and Monitoring, *Choosing Methods and Tools for Data Collection*, http://documents.wfp.org/stellent/groups/public/documents/ko/mekb_module_13.pdf (accessed August 13, 2011).

[30] Harold A. Linstone and Murray Turnoff, *The Delphi Method: Techniques and Applications* (Newark, NJ: Information Systems Dept., New Jersey Institute of Technology, 2002), http://www.is.njit.edu/pubs/delphibook (accessed January 23, 2008).

fusion center intelligence operations and the national intelligence sharing system of the federal government. Materials and resources from the author's research can be found in the appendix and list of references at the conclusion of the thesis.

II. TRANSFORMATION: THE U.S. RESPONSE TO THE EVOLVING THREAT ENVIRONMENT

A. THE POST-SEPTEMBER 11, 2001, THREAT ENVIRONMENT

On February 18, 2008, in a presentation to the Washington Institute for Near East Policy, Michael Leiter, Director of the National Counterterrorism Center, made the following remarks:

> It has been six and a half years since 9/11. More than seven years since the attack on the USS Cole. Almost ten years since the attacks on the U.S. embassies in Kenya and Tanzania. Nearly 15 years since the first attack on the World Trade Center and twenty-five years since the bombing of the U.S. Marine Corps barracks in Beirut. Over that quarter-century, the threat we face from terrorism has constantly mutated, sometimes in tragically unexpected ways. This has compelled us to adapt and evolve as well.[31]

Furthermore, Leiter went on to state, "Above all, the United States remains the top target for al Qa'ida's operational commanders, who continue to look for ways to smuggle Western-savvy operatives into our borders, or, inspire those already here to act."[32] Leiter's presentation continued to discuss, in greater depth, the threat posed to the U.S. by al Qa'ida, and al Qa'ida-inspired terrorist cells, as well as the protective measures in which the U.S. government has invested to counter this and similar threats. As indicated above, 9/11 was not the first time the U.S. was affected by international terrorism, although it was the tipping point that lead to drastic changes in U.S. policy and the government's approach to terrorism and national security. Consequently, this new and evolving threat represents a major change from that of the Cold War—where much of U.S. military and security efforts were focused during the mid-1940s through the early 1990s—and thus requires a far different approach to overcome it.

---

[31] Michael Leiter, "Looming Challenges in the War on Terror" (Remarks Presented to the Washington Institute for Near East Policy, Washington, D.C., February 13, 2008), http://www.nctc.gov/press_room/speeches/wash-inst-written-sfr-final.pdf (accessed March 7, 2008), 1.

[32] Ibid., 7.

The Cold War was driven by geo-political tensions between the U.S. and the Soviet Union, the differing political philosophies (Democracy vs. Communism) of the two superpowers, and a race to advance militarily, industrially, and technologically. The threat posed today by international terrorism is primarily driven by a radical, Islamic religio-political ideology, supported by both foreign Islamic states and non-state sponsors, in response to the effects of Western ideologies, globalization, and a non-Islamic "Western" presence in the Middle East. In the former Cold War era, the threat was of economic challenges, military action against the U.S., nuclear proliferation and attacks and the end of the "free world;" whereas the threat posed today by terrorism is asymmetric in nature, stemming from both politically and religiously motivated networks of clandestine operatives and lone actors that aim to instill fear and commit acts of violence without warning. Perhaps most astounding, as realized from 9/11 and subsequent terrorist events, is not just terrorists' ability to carry out large-scale operations while evading detection, but their willingness to take their own lives while carrying out acts of violence to influence political and religious objectives.

Additionally, this threat is further exacerbated by the spread of its violent ideology, propagating through the media, Internet, religious institutions, or conventional social clubs, and thus, promoting "homegrown" Islamic radicalization within the U.S. (now referred to as homegrown violent extremists or HVEs). In light of this threat, U.S. agencies engaged in counterterrorism missions must refrain from violating the legal rights guaranteed to American citizens in the U.S. Constitution—particularly, the First and Fourth Amendments (freedom of religion, press, and expression; and provisions against unreasonable searches and seizures)—while aiming to suppress the proliferation of violent rhetoric and criminally-related extremism in the U.S.

David Tucker, an expert in the field of terrorism, has argued two critical points that are highly relative to understanding the U.S. changing threat environment: terrorism has not necessarily changed in the years leading up to or following 9/11, rather "9/11 changed us;" and, the attacks on 9/11 were not necessarily the result of religious

fanaticism but instead a violent clandestine organization's attempt to mobilize a large, sympathetic population, through the use of violence, for a political purpose.[33]

B. INTELLIGENCE

One of the United States' most critical tools for counterterrorism is the use of intelligence operations "to detect terrorist activity before it manifests itself in an attack so that proper preemptive, preventive, and protective action can be taken."[34] As realized from 9/11, the U.S. must engage more than just the Intelligence Community, which has traditionally focused intelligence efforts on international issues. All U.S. government agencies and organizations—domestic and international—with the legal authority to administer intelligence operations must be engaged in such practices for counterterrorism purposes, for as we have experienced, future attacks are likely to originate within the U.S., rather than directly from abroad. Mark Lowenthal, former Assistant Director of the Central Intelligence Agency, has defined *intelligence* as follows:

> Intelligence is the process by which specific types of information important to national security are requested, collected, analyzed, and provided to policymakers; the products of that process; the safeguarding of these processes and this information by counterintelligence activities; and the carrying out of operations as requested by lawful authorities.[35]

David Carter, Professor of Criminal Justice at Michigan State University, has provided a slightly different definition of the term intelligence, suggesting a distinction between what intelligence means to law enforcement agencies versus its interpretation by the agencies that form the U.S. Intelligence Community:

> Intelligence is the product of an analytic process that evaluates information collected from diverse sources, integrates the relevant information into a cohesive package, and produces a conclusion or estimate about a criminal phenomenon by using the scientific approach to problem solving (i.e., analysis). Intelligence, therefore, is a synergistic

---

[33] David Tucker, *The Unconventional Threat to Homeland Security: An Overview* (Video lecture, Naval Post Graduate School, Monterey, CA, 2006).

[34] Office of Homeland Security, *National Strategy for Homeland Security* (Washington D.C.: Office of Homeland Security, 2002), 15.

[35] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 3rd ed. (Washington, DC: Congressional Quarterly Press, 2002), 9.

> product intended to provide meaningful and trustworthy direction to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.[36]

Thus, for the objectives of law enforcement agencies, intelligence is "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."[37] Yet, in the capacity of its use by the U.S. Intelligence Community—such as described by Lowenthal—intelligence focuses on a much broader array of issues that have significance to national security and U.S. interests, ranging from military action, standard politics, foreign relations, and, most notably, domestic and international terrorism. The subtle differences in these definitions is beyond the scope of this thesis; however, it is important for the reader to recognize the key concept found within both definitions—intelligence as the outcome of a process that includes analyzing collected, relevant information, based on an identified need, in order to arrive at a conclusion, and, ultimately, provide a final "product" to influence and fortify a decision. Additionally, based on these different definitions of the same term, one can see that the main products created as a result of each may differ, as a different scope of requirements is presented by each.

Intelligence is conducted and prepared through a methodology known as the intelligence cycle, or what Lowenthal refers to as "intelligence as process."[38] According to the *National Criminal Intelligence Sharing Plan*, "The intelligence cycle is the means of developing raw information into finished intelligence products for use in decision making and formulating policies and actions."[39] While numerous variations of the intelligence cycle have been expounded in academia, in the traditional sense, it is a process that typically consists of six primary "steps": planning and direction, identifying

---

[36] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies* (Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, and Michigan State University, 2004), 7.

[37] Ibid., 8.

[38] Lowenthal, *Intelligence: From Secrets to Policy*, 9.

[39] Global Justice Information Sharing Initiative, National Criminal Intelligence Sharing Plan (Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2003), 7.

intelligence needs or requirements, collection, synthesis and analysis, production, dissemination, and feedback (see Figure 1). Depending on the agency or individual administering the intelligence cycle, various steps are often combined or divided.

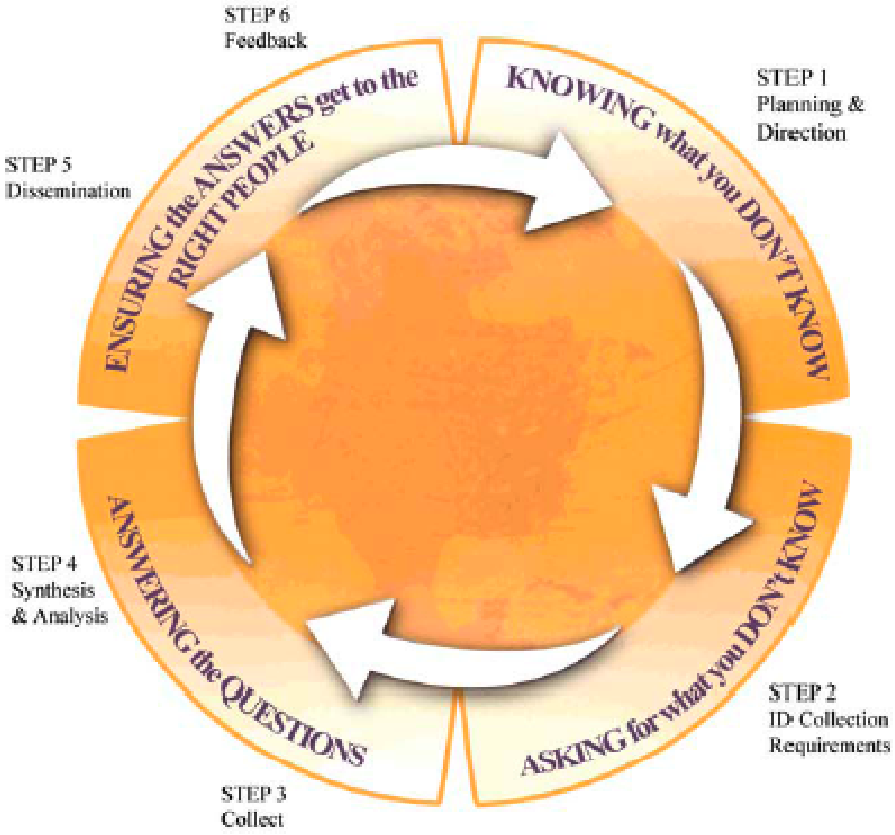


Figure 1. The Intelligence Cycle[40]

Furthermore, intelligence is the byproduct of analyzed, often targeted, information; it results when one provides relevance and meaning to facts and indicates why some piece of information is important. As such, intelligence is more than

[40] Masse, O'Neil, and Rollins, *Fusion Centers*, 89

information; it is knowledge that has been specially prepared to answer a question, verify a situation, or provide an understanding, in actionable terms, to an individual's unique circumstances.[41]

Thus, while intelligence is derived from information gathered through the exploitation of various sources, intelligence ultimately requires human, analytic involvement to add value to that which is collected and tailor a product to fit a consumer's needs. This analytic requirement of meeting the consumer's needs is of significance to this thesis. Figures 2 and 3 provide a list of intelligence collection disciplines, as well as a list of common intelligence product categories:

[41] Lisa Krizan, "Intelligence Essentials for Everyone," *Occasional Paper Number Six* (Washington, D.C.: Joint Military Intelligence College, 1999), 7.

Intelligence Collection Disciplines

Source	Discipline	Types/Attributes	Analytic Use
People	Human Source Intelligence (HUMINT)	Controlled Sources (agents, investigators), informants, eyewitnesses, subject-matter experts, professional researchers, information specialists	Transfer of first-hand knowledge, referral to other sources
Objects	Imagery Intelligence (IMINT)	Photo/digital, electro-optical, multispectral, infrared, radar; physical /functional characteristics of areas, objects, equipment, materials, or products, such as texture, shape, side, location, and distinctive markings, discerned through observation	Basis for emotive but objective reporting on composition, condition, origin, or human purpose
Emanations (a)	Signals Intelligence (SIGINT)	Communications, Electronic, Telemetry; Acoustic; Chemical Biological, Radiological, Nuclear, Explosive (CBRNE) Detection; detectable phenomena given off by natural or manmade objects; electromagnetic energy, heat, sound, footprints, fingerprints, and chem	Scientific and technical analysis
Emanations (b)	Measurement and Signatures Intelligence (MASINT)		
Records	Open Source Intelligence (OSINT)	Public Documents, Books and Journals, Newspapers, Television, Radio, Video, Internet websites and chatrooms; symbolic (written and oral reports, numerical tabulations) and non-symbolic (images, recordings of data)	Research, background information, translation, conversion to usable form

Figure 2. Intelligence Collection Disciplines[42]

[42] Krizan, "Intelligence Essentials for Everyone," 23.

Intelligence Products

By Subject	By Use
Criminal	Operational
Military	Investigative
Political	Warning
Sociological	Research
Geographic	Current
Economic	Estimative
Biographic	Scientific and Technical
Scientific	
Technical	
Transportation	
Communications	

Figure 3. Common Intelligence Product Categories[43]

C. ORGANIZATIONAL INTELLIGENCE REFORM

1. Federal Reform

Prior to September 11, 2001, a lack of communication and collaboration existed amongst the agencies within the U.S. intelligence and law enforcement communities as each operated within fragmented information stovepipes. Those responsible for the production of intelligence to support the U.S.'s counterterrorism efforts failed to share terrorism-related information rapidly and efficiently within the Intelligence Community, and with federal, state, local, and tribal law enforcement agencies.[44] This "failure" was indicated in the reports of both the 9/11 Commission and Weapons of Mass Destruction Commission as a critical factor that prevented the U.S. from thwarting al Qa'ida's September 11 terrorist attacks.[45] As a result, efforts have been made to improve the U.S. government's domestic and international intelligence composition in order to prevent future terrorist activity within the U.S. and upon U.S. interests. Several laws and

[43] Krizan, "Intelligence Essentials for Everyone," 9.

[44] Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States* (Washington, D.C.: 2005), 281.

[45] National Commission on Terrorist Attacks, *9 /11 Commission Report.*

strategies have since been established and/or restructured, and numerous organizational changes have been implemented to strengthen intelligence practices at all levels of government.

In response to the perceived transformation in the U.S. threat environment, former President George W. Bush issued the nation's first *National Strategy for Homeland Security* in July of 2002 as a means of providing a comprehensive and shared vision for how to achieve the goal of protecting the U.S. from future terrorist attacks.[46] The 2002 strategy prioritized three strategic objectives, "Prevent terrorist attacks within the U.S., reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[47] The 2002 strategy also focused U.S. homeland security functions into six "critical mission areas:" "intelligence and warning, border and transportation security, domestic counterterrorism, protecting critical infrastructure, defending against catastrophic terrorism, and emergency preparedness and response," all of which are significant to this thesis.[48] In the eight years that followed the drafting of this document, several additional national strategies were drafted by the U.S. government to assist in the effort to combat terrorism and improve homeland security.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) restructured the U.S. Intelligence Community and mandated processes to improve information sharing amongst the Intelligence Community, state and local officials, and other critical stakeholders. The law included several of the initiatives suggested in *The 9/11 Commission Report*.[49] As stated by former President George W. Bush, "The many reforms in this act have a single goal: to ensure that the people in government responsible for defending America have the best possible information to make the best possible decisions."[50] In 2005, the *National Intelligence Strategy for the United States of America* (NIS) was drafted to provide direction for carrying out the requirements of the IRTPA

---

[46] Office of Homeland Security, *National Strategy for Homeland Security*, 1.

[47] Ibid., 1.

[48] Ibid., 2.

[49] White House, "President Signs Intelligence Reform and Terrorism Prevention Act," December 17, 2004, http://www.whitehouse.gov/news/releases/2004/12/20041217-1.html (accessed July 10, 2007).

[50] Ibid.

and thus overhaul the U.S. Intelligence Community. Among the NIS' 15 objectives, it aimed to change, and thus improve, the role of organizations, culture, and collaborative behaviors within the Intelligence Community; enhance the propensity to disseminate information and intelligence by embracing a "need to share" mentality; and improve information collection, the depth and quality of analysis, the ability to forecast potential problems, stop the proliferation of weapons of mass destruction (WMD); and, ultimately, defeat terrorism.[51]

Furthermore, the revised *National Strategy for Homeland Security*, issued in October 2007, identified a commitment to improve and increase the effectiveness of horizontal and vertical information sharing among federal, state, and local governments.[52] According to the report:

> Such information (regarding homeland security, terrorism, and law enforcement) can be used by agencies from all levels of government in support of efforts to prevent terrorist acts; develop critical infrastructure protection and resilience plans; prioritize emergency management, response, and recovery planning activities; devise training and exercise programs; and determine the allocation of funding and other resources for homeland security-related purposes.[53]

2. State and Local Reform

Considering the current threats presented to the U.S. by both domestic and international terrorism, including HVEs, state and local agencies play a key role in public safety and national security through their routine engagement with the communities they serve. State and local law enforcement and public safety agencies have been identified as our nation's first line of defense against terrorism—they have been dubbed "our nation's first preventers and responders"—particularly for their role in identifying terrorist activity and emerging terrorist plots within each agency's respective jurisdiction and for their role

---

[51] Office of the Director of National Intelligence, *National Intelligence Strategy for the United States of America* (Washington, D.C.: Office of the Director of National Intelligence, 2005).

[52] Office of Homeland Security, *National Strategy for Homeland Security*, 12, 68.

[53] White House, *National Strategy for Information Sharing* (Washington, D.C.: White House, 2007), 1.

in responding to emergencies.[54] Personnel from state and local agencies possess a wealth of knowledge regarding the communities they patrol, inspect, and respond to, as well as the businesses and people that they routinely interact with through their daily course of business. In contrast, federal intelligence agencies lack this "boots on the ground" capability within the U.S. According to the Police Executive Research Forum (PERF), "such interaction could help in preventing a terrorist attack or aid in its investigation."[55] This "local knowledge" provides these agencies with a significant tool for U.S. counterterrorism efforts; thus, the reception of relevant, timely, and actionable intelligence regarding pertinent terrorist threats and tactics is vital to their ability to effectively train, prepare, and allocate resources in order to prevent terrorist acts or respond accordingly.

Furthermore, federal agencies rely on information generated at the local level to develop leads, open investigations, and assess threats to national security that may be developing domestically. As such, communication channels are necessary to share information vertically between local agencies with inside knowledge of their communities and those working within the Intelligence Community on issues of national and international relevance. Ultimately, an intelligence-sharing continuum must be established between all entities in our nation's intelligence, public safety, and national security apparatus: from the signals analyst at the National Security Agency (NSA) to the State Department field officer at the London embassy; from the Central Intelligence Agency (CIA) analyst working in Washington, D.C. to the Federal Bureau of Investigation (FBI) agent in Chicago; from the ambulance driver in Scottsdale, Arizona to the cop walking a beat in Boston, Massachusetts; from the DHS Protective Security Advisor in Salt Lake City, Utah to the Marriott Hotel security manager in Sacramento, California. All levels of government and all entities assigned a safety and security role

---

[54] Michael Chertoff, "Remarks by the Secretary of Homeland Security Michael Chertoff at the International Association of Chiefs of Police Annual Conference," remarks presented to the International Association of Chiefs of Police Annual Conference, Boston, MA, October 16, 2006, http://www.dhs.gov/xnews/speeches/sp_1161184338115.shtm (accessed June 9, 2007); White House, *National Strategy for Information Sharing*, 3.

[55] Marie Rosen, *Chief Concerns: A Gathering Storm–Violent Crime in America* (Washington, D.C.: Police Executive Research Forum, October 2006), 12.

must be kept alert to counter the threat of terrorism in the U.S., and each must function as our nation's eyes and ears, within their respective legal authorities. The national network of fusion centers can assist in this requirement by functioning as a critical analytic component and facilitator of the intelligence-sharing continuum connecting federal, state, local, and private sector organizations to intelligence of relevance to their respective operational missions.

III. ENHANCED INTELLIGENCE SUPPORT STRUCTURES TO COUNTER THE TERRORIST THREAT

A. STATE AND MAJOR URBAN AREA FUSION CENTERS

At the state and local level of government, the development of intelligence fusion centers is a relatively new trend in U.S. homeland security that began taking shape shortly after the September 11, 2001, terrorist attacks. The 9/11 Commission recommended, "…unifying the many participants in the counterterrorism effort and their knowledge in a network-based information-sharing system that transcends traditional government boundaries."[56] In an effort to support this recommendation and, ultimately, enhance public safety and national security, fusion centers have been created within state and local governments to foster both collaboration and the exchange of intelligence between law enforcement, first responder, public health, critical infrastructure (private sector), and other agencies involved in public safety, homeland security, and counterterrorism from all levels of government.

As stated in the *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, "A fusion center is an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources."[57] Additionally, the National Governors Association (NGA) Center for Best Practices has encouraged the development of fusion centers, indicating that they are "instrumental in improving the quality of intelligence by closing information gaps that

[56] National Commission on Terrorist Attacks, *9 /11 Commission Report*, 400.

[57] Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era* (Washington, DC: Global Justice Information Sharing Initiative, Department of Justice, 2006), 2.

previously have hampered counterterrorism efforts at the state and local level."[58] As a result of this endorsement, fusion centers have become a major component of homeland security programs in nearly every state.[59]

To date, a total of 72 state and major urban area fusion centers have been established and operate at various stages of development throughout the U.S. (see Figure 4).[60] Most centers are developing to serve as the primary hub for the collection, collation, analysis, production, and dissemination of information and intelligence related to crime, terrorist threats, and other public safety matters within their respective state or region. As such, each center bears the responsibility of delivering timely, valuable intelligence products to their fellow homeland security and public safety partners.

---

[58] Joe Trella, "State Intelligence Fusion Centers: Recent State Actions," *Issue Brief*, July 7, 2005, (Washington, DC: National Governors Association Center for Best Practices), 1.

[59] Ibid.

[60] U.S. Department of Homeland Security, "Activities & Programs."

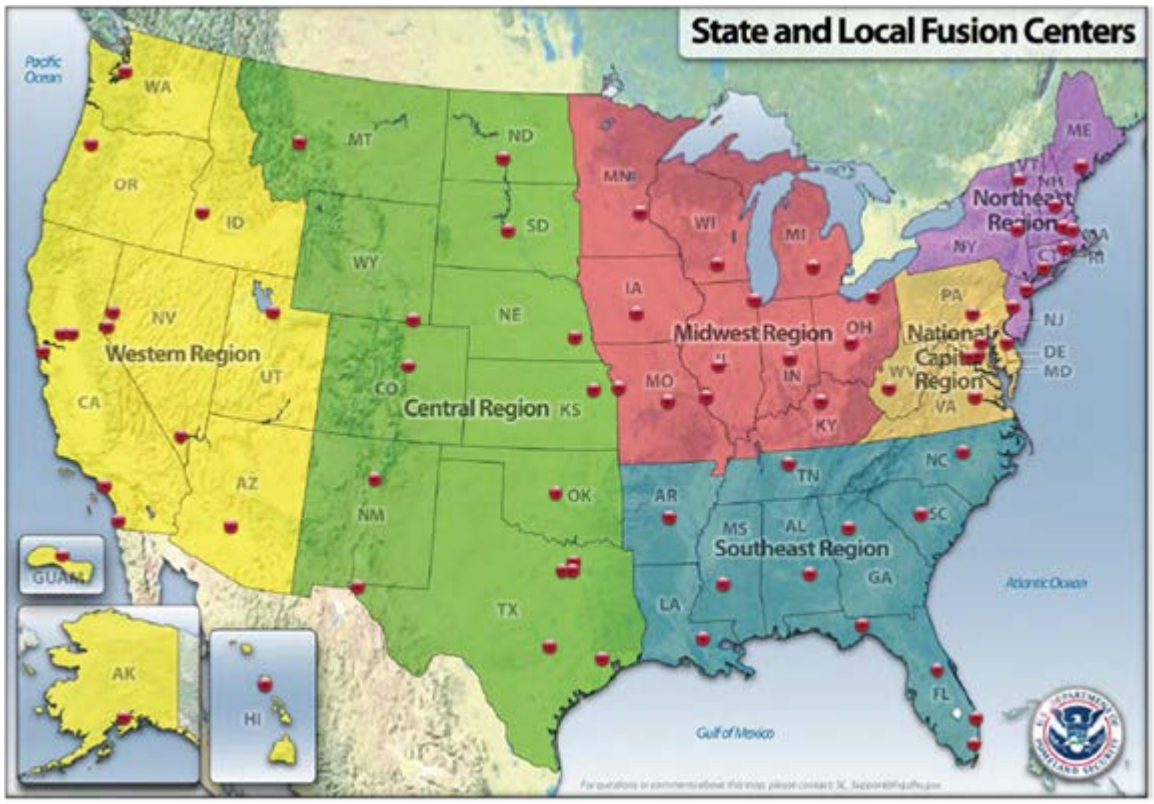


Figure 4. National Network of Fusion Centers[61]

For intelligence production and sharing purposes, a give-and-take relationship is required between each fusion center and its respective partners, as each center is expected to collect, collate, synthesize, and analyze information, provided from various sources, in order to produce intelligence products of value regarding terrorist threats, indications, and warnings of criminal and terrorist activity, and both tactical and strategic intelligence assessments to support decision making for public safety and national security. Thus, operational personnel from all agencies and levels of government are expected to provide information of significance to the center for further integration and analysis, such as suspicious activity reports, self-produced intelligence reports, crime related data, and other classifications of data and information specifically targeted to satisfy unique

[61] Jamison Moody, "DHS Office of Intelligence and Analysis Support to State and Local Governments" (adapted from U.S. Department of Homeland Security, State and Local Program Office presentation to Utah Statewide Information & Analysis Center Governance Board, Sandy, UT, January 26, 2010).

information needs. Such information is intended to be used to support analytic assessments of criminal intent and capability, as well as the risk presented to individuals, critical infrastructure assets, jurisdictions, and regions of concern.

Analyst working at each center must understand the intricacies of their respective areas of responsibility (i.e., critical infrastructure, hazards and vulnerabilities present; population densities) to effectively correlate and assess the context of a given threat stream and its potential application to this area (i.e., if threat "X" is implemented within area of responsibility "Y" by an individual/group with terrorist/criminal intent, what might be targeted, and how, when and where might this present the greatest risk?). The resulting assessments should provide decision makers with a greater level of knowledge on a subject than previously held and should be disseminated to targeted audiences according to need and applicability in a timely manner so that appropriate actions can be taken to mitigate the threat or risk. One fusion center manager summed this concept up well by stating, "Our intent is to develop an environment within our State in which public safety partners can give the fusion center a 'quarter', and in return the center will provide them with a 'dollar.'"[62]

However, questions remain as to whether or not intelligence support has been adequately provided from state, local, and private sector agencies and the IC alike, and if the necessary information conduits have been created to facilitate the essential information sharing. Additionally, many have questioned the effectiveness of fusion centers since their initial implementation:

- Are they working as they are intended?
- Do they incorporate multi-discipline participation?
- Are they providing value-added analysis by effectively implementing the intelligence cycle?
- Are their products meeting the needs of their consumers?
- And perhaps most significant: Are the 72 existing centers working together as a formal network by sharing information, finished analyses and

[62] Raymond Guidetti (New Jersey State Police), interview with author, Monterey, CA, June 24, 2010.

> assessments, and knowledge in a manner that informs and prepares—and thus strengthens—the network, and reduces redundant efforts and the strain on limited resources?

For several years following 9/11, al Qa'ida and al Qa'ida-inspired terrorist activity occurred in greater frequency overseas than within the U.S., as indicated by successful and disrupted attacks in the United Kingdom, Spain, Pakistan, Afghanistan, Iraq, India, and Algeria. In light of this, fusion center personnel have relied on information and intelligence received from the Intelligence Community regarding patterns and trends in terrorist activity and information regarding terrorist threats, tactics, techniques, and procedures that have transpired abroad. This type of reporting ultimately influences each fusion center's intelligence priorities, as well as each state and local jurisdiction's homeland security and counterterrorism strategies. This information informs analytic assessments produced at fusion centers by providing greater context of what might transpire locally if the same tactics, techniques, and procedures are applied by individuals aiming to carry out similar actions. Thus, quality intelligence support from the Intelligence Community is a significant factor in the success of fusion centers. In recent years, additional organizations have been created specifically for the analysis of terrorist-related activity and to help bridge the intelligence gaps that once existed between disparate agencies and levels of government.

B. NCTC—THE U.S. 'FUSION CENTER' OF TERRORISM-RELATED INTELLIGENCE

As recommended in the *9/11 Commission Report* and codified in the December 2004 IRTPA, the National Counterterrorism Center (NCTC) was established to be the primary government organization responsible for providing national coordination of foreign and domestic terrorism and counterterrorism analyses, intelligence production, and strategic operations.[63] Additionally, the center is responsible for disseminating transnational terrorism information and threat analyses to federal agencies with counterterrorism responsibilities, and the Executive Branch, in order to assist them in fulfilling their respective missions to protect the U.S. and its interests from terrorist

[63] *Executive Order 13354.*

activities.[64] The NCTC integrates more than 500 analysts and other personnel from more than 16 federal agencies for analytic intelligence production purposes, and synchronizes counterterrorism strategic operational planning for 22 federal departments and agencies for our nation's *War on Terror*.[65] According to the center's director:

> The creation of NCTC was a deliberate break from the Government's history of creating "stovepiped" agencies to address what were frequently cross-cutting problems. Terrorism involves such a range of activities and enablers—from propaganda campaigns to gain new recruits, to organized camps to train terrorists, to smuggling and drug operations to provide funding, to potential suicide bombers that sow fear—that to combat the threat requires leveraging all elements of national power. From domestic intelligence and law enforcement to foreign intelligence and military action…[all] must work in a coordinated fashion to address the threat.[66]

The NCTC was created to provide greater security for U.S. citizens, as it serves as our nation's fusion center for terrorism-related information and intelligence activities. Analysts working within the confines of the NCTC have access to a large number of classified information networks and systems through which all terrorism-related information available to the federal government is provided to the center.[67] Analysts leverage this central repository of terrorism information as they work collaboratively with their counterparts from various agencies within the Intelligence Community to produce tactical and strategic analytic products in support of policy development by the Executive Branch, and foreign and domestic field operations. The center also hosts several daily secure video teleconferences to keep the Executive Branch and the Intelligence Community informed about terrorist activity and counterterrorism operations worldwide.[68]

---

[64] *Executive Order 13354.*

[65] National Counterterrorism Center, "About the National Counterterrorism Center," http://www.nctc.gov/about_us/about_nctc.html (accessed August 14, 2011).

[66] Leiter, "Looming Challenges in the War on Terror," 2.

[67] Ibid., 3.

[68] M. Scott. Mahaskey, "Scott Redd: Imagination, Collaboration Keys to Counterterrorism," *Federal Times*, August 6, 2007, http://www.federaltimes.com/index.php?S=2945016 (accessed August 14, 2011).

The "value added" that was foreseen in the inception of the NCTC is the result of the various counterterrorism information streams collectively integrated and fused within the center, combined with the diverse subject matter expertise from individuals originating from numerous agencies and specialties, collocated within the center to complement one another. This represents a dynamic shift from the U.S. government's pre-9/11—and hence, pre-IRTPA—intelligence enterprises that focused almost exclusively within their own "information silos" and signifies a revolution in the way analysis is conducted to triumph over a common threat. However, questions remain pertaining to the frequency in which analyses originating at the NCTC—or other federal agencies—reach a state and local audience and the degree in which the products that are in fact delivered are deemed "useful" or "relevant" to the daily operations of state and local officials. Furthermore, as an organization that is mandated to provide direct support *only* to federal agencies engaged in counterterrorism missions, how are non-federal agencies—particularly those at the state and local level—affected by the NCTC's work?

C. THE GOLDEN THREAD TO THE INTELLIGENCE COMMUNITY?

1. Information Sharing Environment

The 2004 IRTPA included several additional requirements to enhance the U.S. government's intelligence capacity. In addition to the creation of the NCTC, the IRTPA required that the President "establish an Information Sharing Environment (ISE) for the sharing of terrorism information in a manner consistent with national security, and with applicable legal standards relating to privacy and civil liberties."[69] Furthermore:

> In accordance with IRTPA, the ISE will reflect the combination of policies, procedures and technologies connecting the resources (information, organizations, services and personnel) of the Federal, State, local, and tribal governments, and as appropriate, the private sector [SLTTP] and foreign allies, to ensure terrorism information sharing, access and collaboration among users is readily available.[70]

---

[69] Program Manager, Information Sharing Environment, *Information Sharing Environment Implementation Plan* (Washington, D.C.: Office of the Director of National Intelligence, 2006), 3.

[70] Ibid., 7.

To facilitate this obligation, the Office of the Director of National Intelligence (ODNI)—yet another recommendation of the IRTPA, created to oversee, coordinate, and direct the implementation of the National Intelligence Program (see Figure 5)—designated a Program Manager (PM ISE) responsible for the ISE's development. In November of 2006, the PM ISE issued the *Information Sharing Environment Implementation Plan*, which prioritized the ISE's role in "facilitating, coordinating, and expediting access to protected terrorism information" and creating a trusted partnership between all levels of government, select foreign partners, and the private sector. [71]

Figure 5. Office of the Director of National Intelligence and Coordination with the Intelligence Community:[72]

The *ISE Implementation Plan* recommended the development of the Interagency Threat Assessment and Coordination Group (ITACG), co-located at the NCTC, to help facilitate the sharing of terrorism-related information amongst federal, state, local, tribal, and private sector officials.[73] The ITACG was passed into law on August 3, 2007 as part of the *Implementing Recommendations of the 9/11 Commission Act of 2007* (the "9/11

[71] Program Manager, *Information Sharing Environment*, 10.

[72] David J. Pile, "Overview of the Office of the Director of National Intelligence and Current Intelligence Initiatives," presentation to the Naval Postgraduate School, Monterey, CA, July 28, 2008.

[73] Program Manager, *Information Sharing Environment Implementation Plan*, 28.

Act"), and it was officially implemented in October of 2007. Also in October of 2007, in response to previous recommendations from the WMD Commission, President Bush released the *National Strategy for Information Sharing: Successes and Challenges in Improving Terrorism-Related Information Sharing*, which provided a definition of the ITACG's role in regards to interagency information-sharing processes. [74] This was the first time a national strategy provided *direction* for implementing the administration's vision for sharing terrorism-related information between the various levels of government, disciplines, and security domains in support of the ISE (see Figure 6).[75]

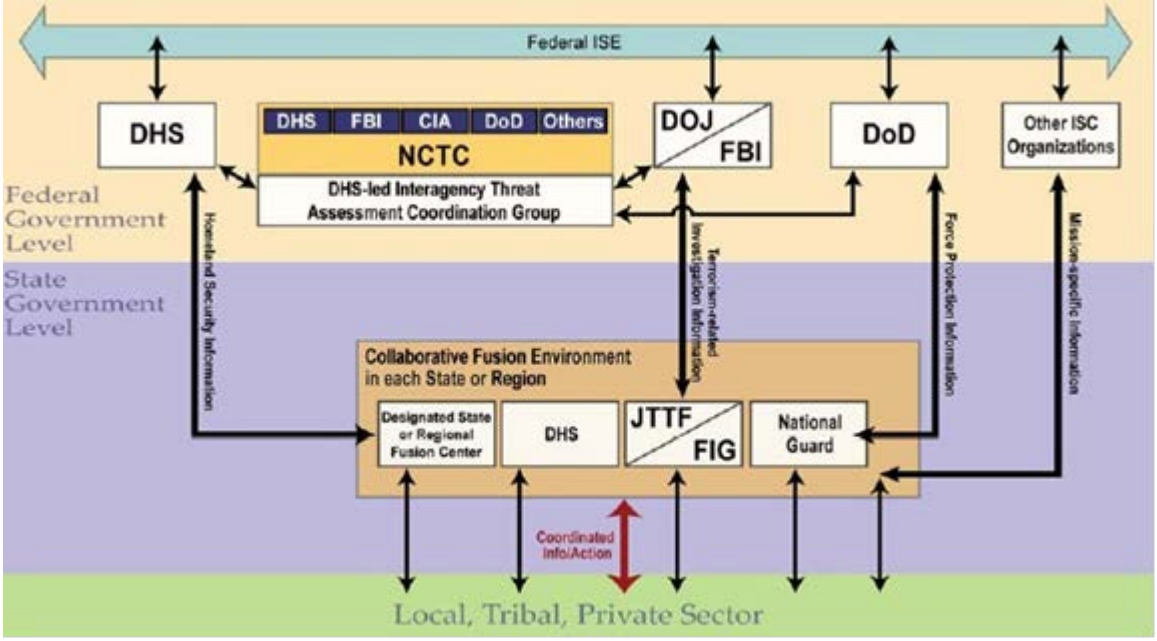


Figure 6. Information-sharing Environment: Framework for Sharing Information with SLTTP Partners.[76]

As stated in the 2007 National Strategy for Information Sharing, the "ITACG supports the efforts of the NCTC to produce 'federally-coordinated' terrorism-related information products intended for dissemination to state, local, and tribal officials and

[74] Commission on the Intelligence Capabilities, *Report to the President of the United States*. Note: The WMD Commission Report recommended that the DNI ensure that effective mechanisms are implemented to prevent conflicts and encourage coordination among U.S. intelligence agencies.

[75] White House, *National Strategy for Information Sharing*, 1.

[76] Program Manager, *Information Sharing Environment Implementation Plan*, 71.

private sector partners."[77] The NCTC, based on its mission mandates, supports no such audience; therefore, the ITACG is intended to assist in mitigating this information-sharing gap. The ITACG's creation was intended to mitigate a three-year gap in intelligence support from the NCTC to state and local governments. Such support requires the unique subject matter expertise of state, local, and tribal officials to advise the federal intelligence analysts working at the NCTC, and, ultimately, the Intelligence Community, regarding what information is useful to those working amongst the local communities in law enforcement, public safety and first responder roles, and the specific language in which intelligence products should be written to reflect their perspective. To accomplish this mission, the *Implementing Recommendations of the 9/11 Commission Act of 2007* (*9/11 Act*) mandated that the ITACG be comprised of two components, an Advisory Council and Detail, to create this required catalyst for the ISE.[78]

2. ITACG Detail

By law, the ITACG Detail—the operational component of the ITACG—is managed by a senior intelligence official from DHS, who serves as the organization's Director and a Deputy from the FBI who is already detailed to the NCTC.[79] The Detail was initially comprised of four full-time state and local law enforcement officials; one part-time tribal law enforcement official; two federal intelligence analysts (from the FBI and DHS); and two contract employees with former Intelligence Community and local law enforcement experience.[80] To enhance the ITACG's efficacy, recommendations were made to expand the Detail's representation to include a state homeland security manager familiar with state and local homeland security operations, a representative from the fire service and emergency response/management community, a public health official, and a state/local law enforcement intelligence analyst.[81] To date, only a few of these

---

[77] White House, *National Strategy for Information Sharing*, 18.

[78] *Implementing Recommendations of the 9/11 Commission Act of 2007*, Public Law 110-53, 110th U.S. Cong., 1st Sess. (August 2007), H.R. 1, Subtitle C, Sec. 521, Sec 210D.

[79] Ibid.

[80] Timothy Connolly (Boston Police Department), interview with author, Boston, MA, March 22, 2008.

[81] Ibid.

recommendations have been met. Currently, the Detail consists of 15 personnel, as it has added additional personnel from state and local law enforcement, fire services, and public health. Furthermore, representation now includes analysts from FBI, NCTC, and the NCTC Directorate of Intelligence.[82]

Those assigned to the ITACG are appointed to the ITACG Detail through federal government (DHS and FBI) fellowship programs for a period of one year. Furthermore, they are deputized as federal employees and do not represent their home agencies; instead, they represent state, local, and tribal agencies as a whole. Each representative is cleared at the top-secret/Sensitive Compartmented Information (TS/SCI) level (with counterintelligence polygraph) and is trained in the procedures for handling, processing, storing, and disseminating classified products. As such, they are afforded access to all information sources within the NCTC.

The ITACG Detail's role is to augment the support that the FBI and DHS give to non-federal partners by advising the Intelligence Community, providing direction to federal analysts regarding what information is necessary, and how products should be tailored and delivered to meet the needs of SLTTP officials as they conduct counterterrorism activities to protect their respective communities.[83] Those assigned to the Detail are tasked with tracking and assessing FBI, DHS, and NCTC intelligence products—both pre-and post-dissemination—to identify ways in which the products can better serve the intelligence requirements of the ITACG's target audience. When necessary, requests are made for language adjustments, as well as the inclusion of additional detail that would be beneficial to first responders. Their goal is to simplify and expedite messages conveyed from the Intelligence Community; make certain that all information necessary to enhance "local" situational awareness, preparedness, prevention, and response capabilities is provided. Moreover, the Detail's goal includes influencing the writing style of those at the federal-level who generate information-products specifically for this community; and, ultimately, to ensure that whenever

[82] Program Manager, Information Sharing Environment, *2010 Report on the Interagency Threat Assessment and Coordination Group* (Washington, D.C.: Office of the Director of National Intelligence, 2010), 17.

[83] *9/11 Commission Act of 2007.*

possible, information is provided at the lowest classification level possible and is approved for broad distribution.[84] To promote this function, the Detail is authorized to request UNCLASSIFIED tear line reports and classification downgrades from the originators of intelligence products and request product transfers between different classification systems (SCI to secret) so that applicable products can reach a more expansive array of consumers outside the federal government (see Figure 7).[85]

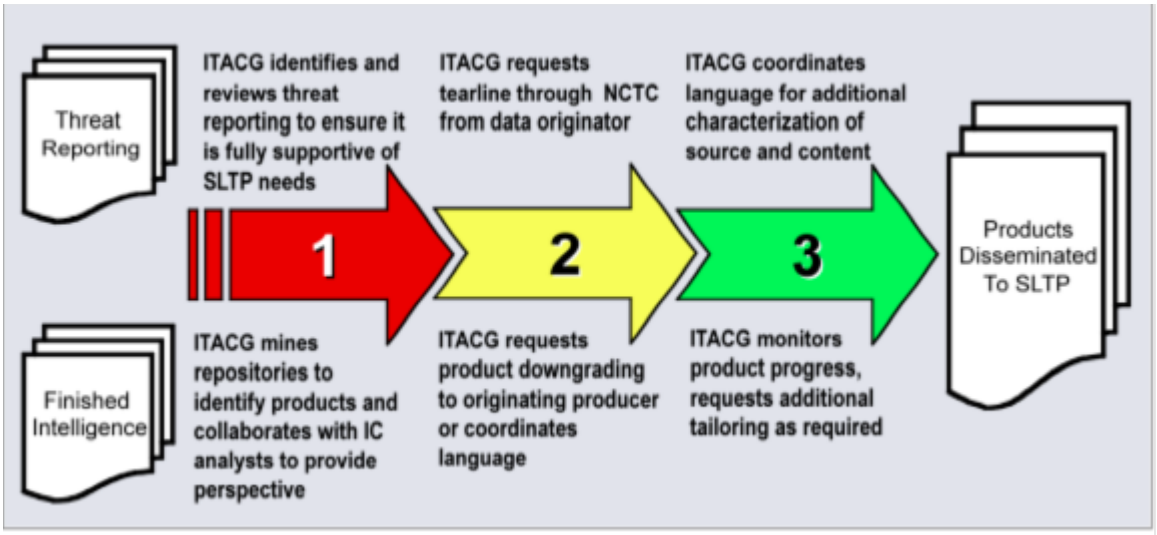


Figure 7. ITACG Intelligence Product Augmentation Methodology[86]

While the ITACG signifies—for the first time—inclusion of the SLTTP perspective in the intelligence activities occurring within the IC, questions remain as to the level of support the ITACG has received to assist it in facilitating its mission; and whether or not its charter competes with the mission and intentions of DHS's Office of Intelligence and Analysis (DHS I&A). Many are skeptical regarding whether or not the ITACG can actually provide value to state and local officials with such a limited number

[84] Connolly, interview with author.

[85] Ibid.

[86] Tim Connolly, "Interagency Threat Assessment and Coordination Group" (Presentation to the International Association of Law Enforcement Intelligence Analysts, Boston, MA, April 8, 2008).

of representatives staffing its operation. The U.S. is currently developing fusion centers within all states and most major urban areas; can the ITACG be used as an intelligence-sharing conduit to each center?

This thesis aims to identify potential solutions to leverage existing intelligence operations that can promote an intelligence-sharing continuum across all tiers of government. The author's research and experience indicates that numerous policy, technological, cultural and political challenges exist, all contributing to the less-than-perfect nature of the United States' existing counterterrorism framework. Over the last four years, policymakers and practitioners have collaborated at a greater pace to carefully navigate the political landscape and operational requirements in their creation of policies and operational practices to ensure that security solutions do not violate the privacy, civil rights, and civil liberties of U.S. citizens or over-tax limited resources. Working together, they must continue to reinforce the required continuum for intelligence sharing and analysis amongst numerous agencies and levels of government to mitigate the inherent risk of terrorist attacks upon our nation. Chapters V and VI provide an analysis of specific, priority issues that require fixing within our nation's counterterrorism apparatus. Chapters VII and VIII provide evidence-based recommendations to improve the capability and value of existing intelligence support structures and further-develop the desired intelligence-sharing continuum.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. METHODOLOGY

A. TRIANGULATION

As previously stated, the events of September 11, 2001, were a major catalyst for intelligence reform in the United States. However, despite the changes that have occurred throughout the U.S. intelligence composition since this date, significant issues still remain that are impeding the creation and flow of useful information and intelligence to support homeland security efforts; this has been identified from research conducted on numerous sources. To fulfill the requirements of this thesis' research question—*identifying what practices and processes should be implemented among state and major urban area fusion centers and the federal Intelligence Community to promote an intelligence-sharing continuum and make fusion centers more effective in meeting the needs of their consumers*—an assortment of organizational structures, policies, practices, and initiatives were analyzed to identify strengths and weaknesses based both against what each is intended to be carrying out and accomplishing, and what each is doing in reality. In the end, a triangulation methodology was administered to test the consistency of findings from several research techniques in order to corroborate the true causes influencing the results. According to social science experts, "Triangulation involves the careful reviewing of data collected through different methods in order to achieve a more accurate and valid estimate of qualitative results for a particular construct."[87]

During the research and analysis process, themes regarding current discrepancies were acknowledged from the author's subject matter expertise and experience, conferences and classes attended, and interviews and discourse with professionals working amongst the intelligence, law enforcement, and public safety communities. Additionally, strengths, weaknesses, and "gaps" were identified from the analysis of academic journals and scholarly articles; documented research conducted by Congressional, federal, and state government oversight groups, and private sector research organizations; Senatorial and Congressional hearings and testimonies; revised

[87] Maria Oliver-Hoyo and DeeDee Allen, "The Use of Triangulation Methods in Qualitative Educational Research," *Journal of College Science Teaching* 35, no. 4 (2006): 42–47.

national strategies, policies, and executive orders; and mandated reports and statements by agency executives regarding specific organizations and initiatives, and their progress since being implemented. Through triangulation, all of the aforementioned interactions, experiences, and literary products influenced the analysis of the issue at hand by contributing information that corroborated the true underlying problems; and furthermore, assisted with the formulation of recommendations to resolve several problems associated with intelligence sharing.

Consequently, a relatively small amount of research is available in academic circles regarding these issues from the practitioners' perspective. While it is common to find documents that describe a sentiment of dissatisfaction regarding the current state of intelligence production and sharing among intelligence consumers involved in homeland security efforts (particularly, from SLTTP officials), it was difficult to determine, exclusively through literature reviews, interviews, and discourse, exactly what issues continue to be problematic—as well as what practical solutions exist—related to the current state of affairs. Therefore, it was necessary to collect and analyze the knowledge of those directly engaged in information and intelligence production and sharing for counterterrorism and homeland security purposes in order to seek explicit insight into these issues from the practitioner's point of view. Ultimately, through triangulation, the author analyzed the common themes acknowledged by practitioners against that of the aforementioned secondary research to identify the underlying issues and formulate policy recommendations.

B. THE DELPHI METHOD

Additional research was necessary to better understand—from the practitioners' perspective—the *causes* of inadequacies in information and intelligence production and sharing between the federal government, fusion centers, and the consumers of fusion center-generated intelligence products, as well as the *practical solutions* considered applicable for fixing the problems. Accordingly, further research was carried out to complement and expand upon the substantial insight provided by organizations such as the Congressional Research Service (CRS), National Governors Association (NGA), U.S.

Government Accountability Office (U.S. GAO), the Manhattan Institute for Policy Research, and the Global Justice Information Sharing Initiative (Global) on the topic of both fusion centers and intelligence sharing.

Traditionally, policy recommendations for complex issues are drafted as an outcome of meetings, committees, and conferences involving professionals with great knowledge in the area in question. [88] Unfortunately, there is a lack of anonymity in this type of setting, and, as a result, the ideas and insights of individuals are often influenced by those of others involved in the process.[89] For instance, one may be reluctant to disagree with the recommendations of a superior or those of an individual who is seen as a top expert in the field; consequently, such situations are highly susceptible to "group think," and individuals refrain from sufficiently voicing their opinions, concerns, or ideas. Additionally, convening a group of experts from a broad geographic area can be difficult to accomplish due to both logistical and financial challenges, and time/scheduling restraints; thus, complicated matters may not be adequately resolved because those best suited to be involved in the policy transformation are unable to participate.

The Delphi method is a structured communication process for collecting and refining knowledge from a group of experts by means of a series of questionnaires and controlled feedback. It is a technique that is often used when there is a complex problem, a lack of knowledge available to answer a research question, and when anonymity is necessary.[90] Because the Delphi method does not require face-to-face contact, it is particularly useful for involving experts, users, resource controllers, or administrators who cannot come together physically.[91] Furthermore, the Delphi method prevents domination by certain individuals and can also be used to aggregate judgments where people are hostile toward one another, or where individual personality styles would be

---

[88] Andre L. Delbecq, Andrew H. Van de Ven, and David H. Gustafson, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes* (Glenview, IL: Scott, Foresman and Co., 1975).

[89] Ibid.

[90] Linstone and Turnoff, *The Delphi Method*, 3–4.

[91] Delbecq, Van de Ven, and Gustafson, *Group Techniques for Program Planning.*

distracting in a face-to-face setting—such as in this case, when collecting expert opinions from individuals of various ranks in law enforcement, intelligence, and public safety agencies.[92] Ultimately, the Delphi method is designed to increase the creative productivity of group action, facilitate group decisions, help stimulate the generation of critical ideas, give guidance in the aggregation of individual judgments, and, in all these endeavors, save human effort and energy and leave participants with a sense of satisfaction.[93] This methodology can be used to serve a broad variety of interests, but was preferred particularly for its strengths in generating a base for evaluation and accommodating policy decisions to diverse points of view and desires.[94]

The Delphi process typically involves three groups:

1. A researcher or research team that works with
2. Policy/decision makers to design questionnaires that focus upon problems, objectives, solutions, or forecasts to elicit the proper discourse (the policy/decision makers will utilize the outcomes of the Delphi method), and
3. A manageable group of respondents/experts whose judgments are being sought.

The first questionnaire asks the participants to respond to a broad question or set of questions; this questionnaire is then returned to the research team, and is analyzed and summarized. Each subsequent questionnaire is built upon the responses to the preceding questionnaire; they contain summary information and may ask participants to disagree or agree with that which has been presented by the others to rank order and/or to indicate strengths and weaknesses. The complete process, depending on availability of staff, is estimated to take between 45 and 90 days to complete; ultimately, it stops when a consensus has been generated among participants or when sufficient information exchange has been obtained—typically after two to six questionnaires have been

[92] Delbecq, Van de Ven, and Gustafson, *Group Techniques for Program Planning.*

[93] Ibid.

[94] Ibid.

disseminated and returned. The questionnaires can be accessed and disseminated via traditional mail, email, personal website, or online survey tools (which were utilized for this thesis).

1. Thesis Intelligence Delphi Panel

In February 2008, a Delphi panel was coordinated to discuss the shortcomings that are leading to deficiencies in counter-terrorism and homeland security intelligence production and flow between the Intelligence Community, fusion centers, and the consumers of fusion center-generated intelligence; this was to serve as a major component of the author's research. In coordinating the Delphi panel, approximately 30 intelligence experts and practitioners were solicited from federal agencies such as DHS and FBI, fusion center administrators and analysts, and fusion center intelligence consumers, such as state and local law enforcement and public safety officials, as well as individuals from private sector organizations. The intention was to generate a relative sample of panelists representative of those agencies and organizations involved in the domestic homeland security information "fusion" process, from agencies and organizations situated throughout the U.S. Panelists were identified, solicited, and selected based on merit, experience, recommendation, relevance to and involvement in the Information Sharing Environment, and their ability and consent to participate.

To fulfill the requirements of the research questions, a total of 22 panelists were enlisted to participate in the Delphi process, representing federal, state, local, and private sector agencies positioned throughout the U.S. Each enlisted panelist was contacted via email to discuss the subject of the research and the procedures required, including the necessary commitment; additionally, an agreement was made that each panelist's identity, as well as his/her answers, would be kept both confidential and anonymous. Each panelist agreed to complete two 15-minute questionnaires and to return them to the author within a "short time frame" (typically, within three days to two weeks of receipt), for a total of one-and-a-half hours over a period of one to three months.

The primary objective of the Delphi method was to disseminate two to three iterations of short answer questionnaires in order to collect a consensus from the

practitioners regarding what is contributing to deficiencies in intelligence production and flow amongst the numerous agencies involved in counterterrorism and homeland security, as well as what they believe could ultimately help promote greater practices and processes to fix the problems. As an additional component of the strategy, the panelists were to be separated into subcategories according to their agency type—federal, fusion center, state and local law enforcement, non-law enforcement public safety, private sector—in order to categorize and analyze the insight of those working at the various levels and positions of government and industry in anticipation of variance in opinions. The use of a Delphi panel to generate this consensus was necessary as there is a lack of heterogeneous information available summarizing these issues from the practitioner's standpoint; additionally, there is a lack of homogeneous information available summarizing these issues from the collective perspective of each tier of government and industry.

The first iteration of questions was intended to generate a brainstorming session for important factors, whereas the second iteration was intended to confine the original list of answers to the most important ones, and to create a final list by rank-ordering the most important factors presented by the panelists. While implementing the Delphi process, guidance was obtained from the Delphi frameworks provided in Okoli and Pawlowski's article, "The Delphi Method as a Research Tool: An example, Design Considerations and Applications," and Delbecq's book, *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes.*[95]

2. Questionnaire 1

In questionnaire 1, each panelist was asked to help identify and explore the principal strengths and weaknesses of the current intelligence production and sharing practices that are in place between the federal Intelligence Community, fusion centers, and the consumers of fusion center-generated intelligence. This questionnaire was

[95] Chitu Okoli, and Suzanne D. Pawlowski, "The Delphi Method as a Research Tool: an Example, Design Considerations and Applications," *Information & Management* 42 (December 2004), 15–29; Delbecq, Van de Ven, and Gustafson, *Group Techniques for Program Planning.*

designed to set the tone for the subsequent questionnaire and the ensuing discourse and analysis. Below are the questions included in the first questionnaire:

1. To the best of your knowledge, are most intelligence and information consumers satisfied with the current standard of products and services provided by state and local fusion centers?[96] Why or Why Not?
2. List the major factors that are affecting information and intelligence production at fusion centers.
3. List significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.
4. List the major factors that currently affect information flow between:
    a. The federal Intelligence Community and fusion centers
    b. Domestic information/intelligence collectors and fusion centers[97]
    c. Fusion centers and the consumers of fusion center-generated products and services
5. List significant factors, practices, and/or processes that would positively influence the flow of information between:
    d. The federal Intelligence Community and fusion centers
    e. Domestic information/intelligence collectors and fusion centers
    f. Fusion centers and the consumers of fusion center-generated products and services
6. Any other factors you care to address:

These questions were drafted to generate themes in the experiences and opinions of a broad sample of the nation's intelligence practitioners. Furthermore, the objective was to begin identifying problems and potential solutions to improve intelligence production and flow and make fusion centers more effective in meeting the needs of their consumers. (The answers to this questionnaire can be found in the Appendix).

---

[96] For the purposes of this Delphi process: federal, state, local, tribal, private and public sector policymakers, managers, agencies and organizations that are supported by the analysis, products and services provided by state and local fusion centers.

[97] For the purposes of this Delphi process: individuals employed by state, municipal and tribal law enforcement agencies; private security agencies; non-traditional intelligence collection agencies such as fire and EMS, municipal and state code inspection agencies, transportation agencies, public health and public service agencies, business organizations, and the public.

3. Questionnaire 2

After collecting and analyzing the responses from questionnaire 1, common themes were identified and prepared for the second round of the Delphi process. The purpose of questionnaire 2 was to develop a greater consensus regarding the most significant issues that are affecting intelligence production and sharing, as well as the most significant practices and processes necessary to improve these issues. Additionally, panelists were asked to rank-order each of the items to differentiate between those that they felt were most important and those that they felt were least important. Finally, the author sought to identify areas of agreement and disagreement, and to discuss items that may need further clarification. (The structure and content of questionnaire 2 can be found in the Appendix).

Ultimately, the Delphi method was an effective research tool that allowed the author to survey and to question a representative sample of senior intelligence, law enforcement, and public safety professionals working and residing in various jurisdictions throughout the nation. It would not have been possible to convene such an exceptional group of individuals for this policy research—especially for the duration of time that the project took—as logistics, funding, and scheduling would have created significant complications, and thus the desired results would not have been achievable. Additionally, some of the dialogue generated from the questions contained controversial themes that might have proven problematic if all of the panelists were together in one room. This was primarily due to the differences in opinion of those working amongst the different tiers of government and industry, as well as a few agencies that appear to be competing. Finally, the insights gained through the Delphi process were significant to the methodological triangulation in verifying the results of prior research and analysis conducted on this topic. Collecting and analyzing the insight from these experts and practitioners was beneficial to the author's final policy recommendations for promoting an intelligence-sharing continuum for homeland security and counterterrorism support.

V. WHAT IS WRONG WITH FUSION CENTERS?

While intelligence production and sharing strategies have improved since the September 11 terrorist attacks, they have not yet reached an adequate level of satisfaction amongst all homeland security stakeholders. During the last 10 years, information sharing has been hampered by a number of impediments that recent legal enhancements and organizational changes have not been able to completely fix. The author's research methodologies were able to corroborate several themes of issues that are affecting the required intelligence-sharing continuum. Some of the most recognized issues are related to the classification of information, inadequate information-sharing channels, low human capital, and a lack of specific, and/or actionable intelligence products provided to state, local, and tribal agencies from both the Intelligence Community and fusion centers. Those dissatisfied include senior executives from numerous U.S. government agencies, organizations, and officials working in various law enforcement, public safety, and security roles at the operational level. Consequently, this has many fearing that our nation's first preventers and first responders may not be adequately prepared if or when the next terrorist attack occurs.

In July of 2007, the Chairman of the House Homeland Security Committee stated:

> The nationwide network of fusion centers intended to gather counterterrorism intelligence is suffering from a lack of direction from the Homeland Security Department. Because of a lack of effective federal leadership, state and local [agencies] have taken it upon themselves to create these centers with varying levels of success.[98]

At the time that the author's research for this thesis began (2007), no minimum standards existed to ensure that fusion centers operated efficiently, were built to interact with other fusion centers as a network, or were meeting the unique needs of each center's

[98] Dizard, "Study: Flaws in Fusion Centers."

respective intelligence consumers.[99] Many had little private sector input, encountered difficulties with the classification of information, and had limited access to relevant information databases.[100]

The aforementioned statement and analysis was verified through methodological triangulation of secondary research, and ultimately, the results from the Delphi panel. The themes identified from the overall triangulation indicate that there are some significant, specific, overarching issues. However, in the end, there were some topics that could not be corroborated through triangulation, as there was great diversity in the individual answers provided amongst the various panelists and sub-groups that participated in the Delphi panel, leading to a lack of consensus. For example, apparent from the concluding analysis of the Delphi process was the following: While a panelist operating from a specific locality identified one issue as particularly important, a panelist working in the same position, but from a different locality, identified the same issue as significantly less important. This, triangulated with the results of the other analytic methodologies administered, has led the author to believe that a lack of overall guidance and oversight may indeed be leading to many of the intelligence production and sharing issues present amongst the nation's homeland security apparatus. Ultimately, the leaders of fusion centers have been left to design, staff, and operate each center on their own with limited guidance, leading to a variance in the effectiveness of different areas of the overall function. For example:

- While some centers indicate that they have strong technological connectivity with partner agencies, other centers do not.
- While some centers indicate that they have established substantial strategic objectives across a diverse group of stakeholders, other centers have not.
- Where some federal agency representatives are successfully integrated into fusion center operations, other federal agency representatives are not.

---

[99] It is important to note, however, that the Department of Justice's Global Justice Information Sharing Initiative has since worked with numerous federal and SLTTP partners to establish "Baseline Capabilities" for state and major urban area fusion centers; a companion document to the *Fusion Center Guidelines*. *Baseline Capabilities for State and Major Urban Area Fusion Centers*; Global Justice Information Sharing Initiative.

[100] Lipowicz, "CRS: Mission Creep at Fusion Centers."

- Where some centers have integrated non-law enforcement public safety officials into the routine operations, other centers lack the presence of non-law enforcement officials.
- Where some centers have adequate connectivity to classified Intelligence Community products through classified computer terminals inside a "secure room" approved for handling secret-level classified information constructed within the confines of their fusion center, other centers lack the same connectivity due to the absence of a secure room.

C. INTELLIGENCE PRODUCTION, SHARING, AND SATISFACTION

Fusion centers appear to be missing the mark when it comes to satisfying their consumers. As indicated in the results of questionnaire 1 from the Delphi process, 68 percent of the respondents reported that from their perspective most intelligence and information consumers are *dissatisfied* with the current standard of products and services provided by state and local fusion centers.[101] Furthermore, the following issues were identified as recurring themes in the responses of the panelists pertaining to the problems associated with consumer satisfaction; thus, those issues related to intelligence production, and intelligence and information sharing:

- Fusion center executives lack leadership skills, strategic focus, and experience with intelligence.
- Fusion centers are not receiving timely, actionable information from federal agencies, which is problematic for subsequent intelligence distribution to key homeland security stakeholders who seek to create effective prevention and response strategies.
- Fusion centers have failed to identify logical, strategically focused intelligence requirements toward which federal agency products and services can be focused.
- Fusion centers are failing to comprehensively respond to the intelligence needs of consumers.
- Consumers have failed to adequately identify clear, concise, realistic intelligence requirements towards which fusion center products and services can be tailored.

[101] See Appendix.

- Fusion centers have struggled to reach an adequate collaborative capacity; they are failing to include representatives from a variety of public safety and private sector agencies in fusion center strategic planning, operations, and other activities.
- Fusion centers are disseminating products that lack analysis, value, and relevance; their products are not always timely or actionable.
- Fusion centers are still working to develop the necessary analytical and operational skills within each center.
- Consumers do not understand the unique capabilities and limitations of their respective fusion center.
- Consumers have not yet been adequately educated in intelligence, analytic lexicons, and the purpose and meaning of many of the products provided.
- Fusion centers have yet to develop adequate feedback and follow-mechanisms to identify the utility of information and intelligence provided to and from consumers.
- The Intelligence Community, fusion centers, and consumers have yet to develop adequate technological solutions to facilitate collaboration, data connectivity, information sharing, knowledge management, and product delivery.[102]

Despite the emphasis on all-source, multi-disciplinary participation, collaboration is a significant issue for many of our nation's fusion centers. Currently, the majority of fusion centers consist primarily of law enforcement entities, as they are predominantly owned and operated by the state police or statewide investigative bureaus. Additionally, the majority of the local police representation is drawn from the larger departments that are able to provide resources to the center, not necessarily the smaller municipal agencies.[103] While many of our nation's fusion centers have some non-law enforcement representation (which in many cases is part-time), there appears to be an absence of full time inclusion in their daily operations, which makes meeting the needs of non-law enforcement public safety partners difficult.[104] Similarly, the majority of fusion centers have yet to include representatives from the various critical infrastructure sectors and have failed to implement practices and processes capable of supporting a broad range of

[102] See Appendix.

[103] Masse, O'Neil, and Rollins, *Fusion Centers*, 35.

[104] Ibid., 36.

private sector partners.[105] Due to this disconnect, it is unclear at this time whether or not those working at fusion centers have in fact adequately identified the most significant risks, threats, and vulnerabilities within their jurisdictions, or are sufficiently fulfilling their missions to mitigate them. Consequently, effective collaboration across diverse agencies and sectors appears to be a rare phenomenon. This is adversely affecting the necessary relationships between fusion centers and their partners and intelligence producers and intelligence consumers, and, thus, fusion centers are unable to meet the needs of their stakeholders.

D. INTELLIGENCE CYCLE

In July of 2007 the Congressional Research Service published a report titled *Fusion Centers: Issues and Options for Congress*, which summarized research conducted on the 43 fusion centers established nationwide at that time.[106] One of the major issues identified from their research was related to the collective, inadequate use of the intelligence cycle at fusion centers. It is, therefore, no coincidence that several of the problematic themes identified from the Delphi panel can be attributed to the absence of a well-administered intelligence cycle, verifying the results of previous analyses. Proper use of the intelligence cycle will ensure that strategic objectives are determined and realized; intelligence gaps are identified; information is gathered, synthesized, analyzed, and disseminated according to the unique needs of decision-makers; proactive and defensive measures are established, and resources are more efficiently allocated due to the provision of valuable insights. While not all fusion centers are experiencing a complete failure in their administration of the intelligence cycle, many are falling short on at least a few of its key components.[107]

1. Planning, Requirements, and Collection

According to the results of the Delphi process, several fusion centers have failed to identify logical, strategically focused intelligence priorities toward which federal

[105] Masse, O'Neil, and Rollins, *Fusion Centers*, 55.

[106] Ibid.

[107] Ibid, 25.

agency products and services can be focused, and they have failed to comprehensively respond to the information and intelligence needs of consumers. This is indicative of a deficiency in their prioritization of the planning, requirements, and collection steps of the intelligence cycle. If fusion center administrators are not routinely meeting and/or communicating with partners and consumers to discuss intelligence requirements and strategic priorities, problems will result from the ensuing lack of focus. Consequently, intelligence producers will risk creating intelligence analytic products based upon what they assume the consumer wants to know, rather than upon what the consumer needs to know. Intelligence requirements are necessary to dictate which issues should receive top priority based upon recognized threats, present trends, the geo-political environment, and perceived risks and vulnerabilities; they are often unique to the needs of each respective intelligence consumer.[108] Furthermore, setting appropriate intelligence requirements and strategically focusing operations and objectives will help ensure that the fusion center is utilizing resources more effectively and efficiently, while making certain that personnel are concentrating efforts—including information collection, analysis, and intelligence production—on that which takes precedence.

The results from the Delphi panel also revealed that several fusion centers have not reached an adequate collaborative capacity, which is ultimately affecting their ability to sufficiently plan, prioritize, and address consumer needs. The indication that consumers have failed to adequately identify relevant intelligence requirements toward which fusion center products and services can be tailored; that consumers do not understand the unique capabilities and limitations of their respective fusion center; and that consumers have not yet been adequately educated in intelligence, as well as the purpose and meaning of intelligence products, is again, a reflection of minimal levels of coordination between fusion center administrators and their partners.

Fusion center personnel must establish trusted, collaborative relationships with their partners and intelligence consumers, educate them of the capabilities and limitations of the center, and determine appropriate intelligence requirements to address and serve.

[108] Krizan, "Intelligence Essentials for Everyone," 13–20.

After all, the absence of collaboration with partner agencies and organizations ultimately contradicts the principle organizational intention behind the development of fusion centers and will have a negative effect on all subsequent, necessary steps of the intelligence cycle for statewide or regional intelligence support purposes. Furthermore, without adequate collection priorities for each respective agency and organization within the state or region, mission-focused data and information, which could have an effect on the security of the area, may not be collected or properly shared. That which is independently gathered and/or observed by outside agencies will stovepipe without well-coordinated relationships between the center and its partners.

2. Synthesis and Analysis, Dissemination, and Feedback

The results of the Delphi process indicated that several fusion centers are disseminating products that lack analysis, value, and relevance. This issue signifies discrepancies in the synthesis and analysis, dissemination, and feedback steps of the intelligence cycle.

Ultimately, fusion centers are at a loss without a sufficient analytic capacity—this is perhaps the most important skill required of centers, and the purpose of their existence. Talented and experienced analysts must be present at each center, employing and exhausting a myriad of analytic methodologies, tools, and resources to extract meaning, develop hypotheses, and draw accurate, objective inferences from data and information that has been targeted for specific purposes. Analysts must be proficient at estimating information for underlying implications—which are often not readily apparent—and be competent in identifying patterns and trends within disparate data sources to determine the "big picture." Another critical skill of the analyst is the ability to express his/her self both orally and in writing.[109]

As many critics and practitioners alike have stated since 9/11, and what has become somewhat of a cliché in terms of today's analytic function, a necessity of the

[109] Lowenthal, Intelligence: From Secrets to Policy, 116.

intelligence analyst is the fundamental skill to "connect the dots." However, in regards to this statement, as well as the complexities of the intelligence analyst's role, Lowenthal has remarked:

> In the aftermath of the September 11 terrorist attacks, the phrase "connect the dots" became prevalent. Connecting the dots depends on all the dots being present to draw the right picture.…The Intelligence Community was accused of not connecting the dots in the run-up to September 11, but was accused of connecting too many dots regarding the alleged Iraqi weapons of mass destruction.[110]
>
> A more useful description is that intelligence analysis is similar to assembling a mosaic, but one in which the desired final picture may not be clear. Not all of the mosaic pieces are available. Further complicating matter, in the course of assembling the mosaic, new pieces appear and some old ones change size, shape, and color.[111]

Additionally, the Delphi panel indicated that adequate technological solutions to facilitate collaboration, data connectivity, information sharing, knowledge management, and product delivery have yet to be developed. This particular issue directly affects the type, quality, and consistency of data and information flowing to the fusion center, as well as the center's ability to effectively synthesize, analyze, coordinate on, and disseminate finalized intelligence to consumers through timely and appropriate means. Ultimately, the results of analyses must be tailored into products that satisfy the consumer's needs in order for the products to be acknowledged, utilized, and become actionable.[112] Once again, this emphasizes the need to adhere to consumer intelligence (production) requirements. However, without the necessary technological solutions to help facilitate the fusion center's communication, collaboration, and information collection and processing requirements (i.e., technological requirements), analysts and other personnel within the center will fall short on efforts to satisfy intelligence consumer expectations and needs.

---

[110] Lowenthal, *Intelligence: From Secrets to Policy*, 127.

[111] Ibid., 127.

[112] Krizan, "Intelligence Essentials for Everyone," 39–47.

Finally, the reception of feedback regarding fusion center products and services was determined to be an additional problem. As specified by the panel, several fusion centers have yet to develop adequate feedback and follow-up mechanisms to identify the utility of information provided to and from consumers. If or when consumers are dissatisfied with the quality of analyses, the format in which products are presented, or the means through which products are delivered, fusion center administrators and analysts must work with the consumers to alter existing production strategies to mirror the content, format, style, and delivery mechanisms desired by each consumer in order to meet their production requirements. Ultimately, this necessitates collaborative relationships between fusion center personnel and their intelligence consumers, as well as the use of various feedback instruments and procedures deemed effective by those working both within and outside the center.

An important fact to consider, which was clearly identified by the Delphi panel and corroborated through secondary research, is that fusion center administrators are still working to develop the necessary analytic and operational skills within the centers. As previously mentioned, fusion centers are a relatively new development within the nation's intelligence apparatus; thus, adequate development will come as time passes and personnel are able to enhance analytic and investigative skill sets. Due to the policies surrounding the allocation of federal funding for personnel, fusion center administrators have experienced difficulty hiring and sustaining analytic and investigative positions within the centers. In many cases, personnel are assigned to fusion centers "on loan" by partner agencies; furthermore, analysts from contract firms are often supplanted using temporary grant funding to enhance the limited, but existing analytic capacity. Greater support is necessary from state and municipal administrations to prioritize and allocate funding to hire qualified personnel, and, ultimately, sustain human capital.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. FEDERAL INTELLIGENCE-SHARING CHALLENGES

A 2006 National Governors Association (NGA) Center for Best Practices Issue Brief indicated that homeland security directors across the nation were displeased with the quality of intelligence provided to state and local officials from the federal government; this survey also marked an increase in dissatisfaction when compared to a similar survey conducted in 2005.[113] Both reports indicated that the information received by state and local officials "lacked specificity and actionable quality."[114] However, the 2007 NGA Survey reflected an improvement in the federal-state intelligence-sharing relationship. According to the report: 56 percent of the state respondents were satisfied with the timeliness of the intelligence received, 47 percent with the specificity, and 50 percent with the actionability. Even so, more than half of the states were dissatisfied with the intelligence-sharing networks established by DHS and other federal agencies, as well as the network-related outreach, training, and participation.[115]

Regardless of the "increase" in intelligence-sharing satisfaction (which is still arguably undesirable as it ranges in the area of 50 percent), the sentiment of dissatisfaction continues to exist. In a September 2007 testimony to the House Homeland Security Committee, a fusion center administrator stated, "One of the chief complaints of state and local officials is the lack of actionable information from the National Intelligence Community [to fusion centers]."[116] Additionally, in a presentation at the March 2008 National Fusion Center Conference, the Chair of the House Homeland Security Subcommittee on Intelligence reprimanded DHS, stating that it is "at risk for losing support for funding because it is not doing a good enough job of sharing

---

[113] Jeff Mitchell, "2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships," *Issue Brief*, April 3, 2006 (Washington, DC: National Governors Association Center for Best Practices), 2.

[114] Ibid.

[115] Chris Logan, "2007 State Homeland Security Directors Survey," *Issue Brief*, December 18, 2007 (Washington, DC: National Governors Association Center for Best Practices), 6–7.

[116] Beasley, "The Way Forward with Fusion Centers," 6.

information with state, local and federal homeland security officials."[117] Furthermore, "DHS' Intelligence and Analysis Office (I&A) needs to improve its relationships with and understanding of the needs of state and local authorities."[118]

The author's research methodologies were able to corroborate numerous factors affecting the continuum of information flowing between the IC and fusion centers. Problems were recognized regarding the lack of quality terrorism-information provided to state and local officials:

- Information "Over-Classification," Difficulty Accessing The Classified Information, And The Inability To Share Classified Information Broadly Amongst The First Responder Community;
- The absence of a standardized framework for categorizing the various tiers of "sensitive but unclassified" (SBU) information; and
- Confusion due to the excessive number, and lack of organization, of electronic information-sharing networks (portals).

For the purposes of this thesis, the author will focus on the verified issues that are specific to the effectiveness of DHS, FBI, NCTC, and the ITACG in providing intelligence to state and local officials.

A. FEDERAL AGENCY SUPPORT TO STATE AND LOCAL OFFICIALS

State and local officials have been dissatisfied with the speed and quality of information that is delivered from federal agencies. Officials have expressed confusion regarding what types of information they should expect from the IC, or how long it will take for information of importance to be delivered. This leaves many desiring a "clearer definition" as to what types of information will be shared, when information will be disseminated, and to whom it will be directed.[119] This was a significant theme triangulated through the author's research, and it was further corroborated by the

---

[117] Ben Bain, "Lawmaker to DHS: Step it up with Fusion Centers," *Federal Computer Week*, March 20, 2008, http://fcw.com/articles/2008/03/20/lawmaker-to-dhs-step-it-up-with-fusion-centers.aspx (accessed June 1, 2008).

[118] Ibid.

[119] Eileen Sullivan, "Intel Centers Losing Anti-terror Focus," *The Associated Press*, November 29, 2007, http://www.usatoday.com/news/topstories/2007-11-28-3174603810_x.htm (accessed December 10, 2007).

responses fielded during the Delphi process. However, the recent expansion of DHS's Intelligence Officer program is beginning to provide value in this regard.

In response to the 9/11 Act, and to assist in carrying out the President's *National Strategy for Information Sharing*, DHS I&A has deployed a total of 73 intelligence officers to state and local fusion centers nationwide to provide support by facilitating the sharing of threat and hazard information between the IC and fusion centers.[120] The implementation of this program is meant to address the intelligence priorities identified by fusion centers (from those that have, in fact, identified their priorities) and to increase the timeliness and quantity of information disseminated "vertically"—both from the IC to fusion center personnel and to the IC from the fusion centers.[121] Those detailed to fusion centers appear to be adding value particularly through their intelligence-related subject matter expertise, and their ability to convey information and provide reach-back to other federal agencies: The DHS officers are facilitating requests for information (RFIs) that must be drawn from resources within the IC; accessing timely federally-produced intelligence and information reports (IIRs); creating homeland information reports (HIRs) from locally derived information that meets federal intelligence requirements, and then sharing this information vertically; and assisting with training, prioritization, and analysis.[122]

Through the Homeland Security Act of 2002, DHS was granted statutory responsibility for coordination with state and local government personnel, agencies, and authorities for terrorism and homeland security-related purposes.[123] Such authority includes the integration of relevant information, intelligence analyses, and vulnerability assessments with state and local governments; as well as the oversight for policies and

---

[120] Bart Johnson, "Status of Efforts to Support Increased Capacity and Sustainment Across the National Network of Fusion Centers" (Briefing to the Criminal Intelligence Coordinating Council, Washington, D.C., May 12, 2011).

[121] Ibid.

[122] Jack Tomachio, "Focus on Fusion Centers: A Progress Report," *Prepared Testimony Before the Senate Committee on Homeland Security and Governmental Affairs Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration*, 110th Congress, 2nd Sess., April 17, 2008, http://www.fas.org/irp/congress/2008_hr/fusion.html (accessed August 14, 2011), 16–75.

[123] *Homeland Security Act of 2002*, Public Law 107-296, 107th Cong., 2nd Sess. (November 2002), H.R. 5005, Title VIII.

procedures governing the sharing of law enforcement, intelligence; and other information relating to homeland security within the federal government and between state and local governments.[124] However, not all terrorism and homeland security-related intelligence created at the federal level of government is coordinated with state and local officials through DHS. For example, in 2008, the FBI had 195 personnel detailed to 48 fusion centers to act as liaisons, investigators and analyst, and to provide subject matter expertise and help facilitate the communication of threat information.[125] According to the Delphi panel and other sources, this duplication of effort often results in confusion; furthermore additional research indicated that this can at times lead to one federal agency intruding into another federal agency's perceived "territory," which has the potential to be disruptive.[126] This duplication and resulting confusion presents the need for a policy to influence coordination amongst the various federal agencies with domestic homeland security and counterterrorism missions—especially those entities from DHS and DOJ that have established direct interactions with state and local officials—to limit duplicative reports, conflicting messages, and interference in investigations.[127] Furthermore, many are requesting that the federal government provide further guidance regarding which federal agency is, in fact, leading domestic homeland security and counterterrorism efforts, as there appear to be conflictions due to the nature of the division of responsibilities. While DHS was granted statutory authority for coordinating terrorism-related information sharing, the *Homeland Security Act of 2002* makes clear, "primary responsibility for investigating and prosecuting acts of terrorism shall be vested not in [DHS], but rather in Federal, State, and local law enforcement agencies with jurisdiction

---

[124] *Homeland Security Act of 2002*.

[125] Wayne M. Murphy, "Making Homeland Security Intelligence Work for State, Local, and Tribal Partners: An Interagency Threat Assessment Coordination Group Progress Report," *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment,* 110th Cong., 2nd Sess., March 13, 2008, http://www.fas.org/irp/congress/2008_hr/hsint.pdf (accessed March 22, 2008), 37.

[126] See appendix.

[127] Sullivan, "Intel Centers Losing Anti-terror Focus."

over the acts in question." Thus, the *Homeland Security Act of 2002* ensures terrorism investigations and prosecutions remain the responsibility of the FBI's Joint Terrorism Task Forces (JTTFs).[128]

The limited number of secure, classified terminals and secure rooms within the national network of fusion centers has been identified as another significant obstacle—corroborated through the author's research. A large amount of the threat information produced by federal agencies is classified and cannot be transmitted to state, local, and tribal agencies through traditional dissemination channels, as there are strict laws and protocols regarding how such information can be handled, stored, and disseminated. While a number of personnel assigned to fusion centers have been granted security clearances—particularly at the secret level—they often encounter difficulties retrieving and handling classified information. Furthermore, because some fusion centers are not certified to house classified documents or data terminals, adequately "cleared" personnel are unable to access, view, or handle classified material within the confines of the facility. Therefore, those centers without a secure, classified computer terminal within a secure room are limited in their ability to routinely access and query classified databases for relevant threat reporting, and monitor and analyze national security information that could have an impact on their state or region.

Initially, the federal government was slow to deploy secure terminals to fusion centers, and most state and local officials had to rely on the FBI field offices to gain access to classified information. In 2008, DHS began deploying their classified network, the "Homeland Secure Data Network" (HSDN), to fusion centers in greater frequency, prioritizing access to their network to those fusion centers with deployed DHS intelligence officers. To date, HSDN has been deployed to 52 fusion centers, granting cleared fusion center personnel access to federal information classified at the secret level.[129]

---

[128] *Homeland Security Act of 2002*, Title I, Sec 101, (b), (2).

[129] Johnson, "Status of Efforts to Support Increased Capacity."

B. NCTC: STATE AND LOCAL SUPPORT?

A study of the NCTC conducted in September 2006 indicated that, "methods for ensuring that homeland security and terrorism information is shared among non-Federal Government entities and the Federal Government remains inadequate."[130] This highlights the perpetual challenge of horizontal and vertical information sharing—still in existence after September 11—amongst the various tiers of U.S. government. Ultimately it has verified existing limitations in regards to the preparedness of our nation's first responders, as information that first responders need at that local level, still may not be reaching them. As stated in the aforementioned report, "Information sharing in support of the nation's counterterrorism objectives 'isn't about flipping a switch;' it involves a diverse landscape of players and technologies, and a myriad of cultural, security, and policy barriers."[131] The complexity of traditional information-sharing practices to and from the NCTC is illustrated in Figure 8.

[130] National Counterterrorism Center, *NCTC and Information Sharing*, 10.

[131] Ibid., 4.

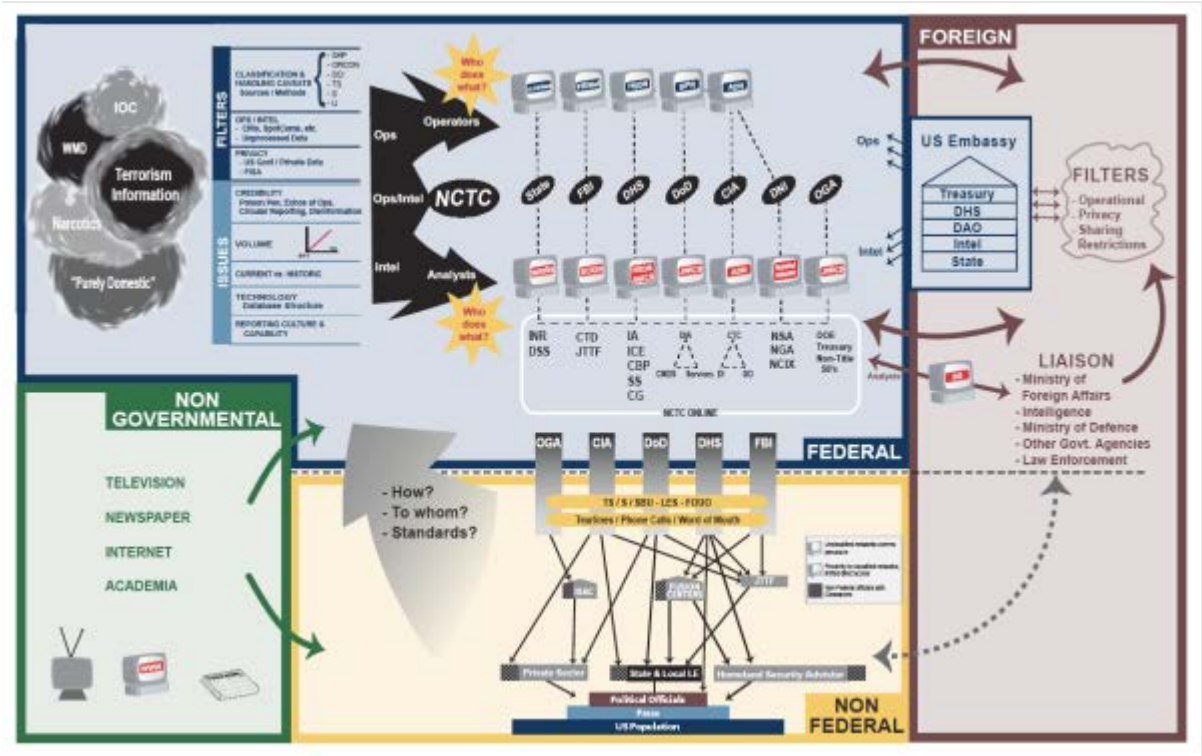


Figure 8. Information Sharing Complexity[132]

Due to the sensitive nature of terrorism-related information, as well as the complexity of the organizations and systems involved, there are, legitimate concerns that must be recognized regarding what sensitive information individuals should be granted access to and how the information should be communicated. According to federal officials, it is imperative that delicate information pertaining to sources and methods is not compromised and that active intelligence and law enforcement operations are not disrupted.[133] This is believed to be much of the reason behind the why information is often classified at such high levels and compartmentalized within agencies for specific, limited audiences. So how does information of significance to state and local first responders get recognized and transferred to such an audience from the complicated systems collecting information at the center?

---

[132] National Counterterrorism Center, *NCTC and Information Sharing*, 4.

[133] Ibid, 3.

Not all of the information and intelligence collected and analyzed within the NCTC is relevant to local agencies for domestic preparedness and response efforts; however, information of potential use by those at the state and local level of government is not easily accessible, as the NCTC's statutory authorities are limited to sharing with federal organizations.[134] As a result, those non-federal public safety officials, best suited to be the eyes and ears for domestic counterterrorism support, can be left uninformed and lacking much-needed guidance regarding current threats and terrorist tactics and techniques, as experienced throughout the world. A 2007 National Intelligence Estimate (NIE) indicated that the U.S. is currently challenged by threats from international terrorist organizations, such as al Qaeda, as well as by the proliferation of homegrown radicalization into Western countries (due to the aggressive propagation of anti-U.S. rhetoric), and the increasing number of violent, clandestine Islamic extremist cells. Therefore, the local law enforcement and first responder communities could benefit from the analysis of trends and patterns from both successful and attempted terrorist attacks, and other terrorist-related activities occurring throughout the world.[135] To quote the NIE, the aforementioned threat environment "require[s] [a] greater understanding of how suspect activities at the local level relate to strategic threat information and how best to identify indicators of terrorist activity in the midst of legitimate interactions."[136] This statement corroborates the aforementioned premise that local agencies must be more intimately involved in the collection and analysis of information related to terrorist activity occurring both inside and outside the U.S.

According to the author's research, among the most prominent issues that have affected the flow of useful terrorism-related information from the IC to the local law enforcement and first responder communities was the absence of state, local, and tribal agency representation at the NCTC. This lack of "local perspective" created a void in the necessary expertise regarding what intelligence is relevant and essential outside the

---

[134] National Counterterrorism Center, *NCTC and Information Sharing*, 1.

[135] Office of the Director of National Intelligence, *National Intelligence Estimate*: *The Terrorist Threat to the U.S. Homeland* (Washington, D.C.: National Intelligence Council, 2007), 6–7.

[136] Ibid., 7.

federal government from the masses of intelligence gathered and analyzed within the center. Accordingly, a "federal-centric" process was created that adequately pushes information of importance up to senior policymakers and amongst the IC, but it fails to provide the same level of support to those working in the front lines of our nation's local communities.[137] Federal agencies, such as the FBI and DHS, are expected to liaison with the NCTC to provide information that they believe would be important for state and local agencies; however, as federal entities themselves, they, too, can lack the experience and expertise necessary—the "local perspective"—to determine what information a specific locality needs to protect itself from, prepare for, and respond to, terrorist activity.

Additionally, the analytic products created at the NCTC—as well as at other federal agencies—are primarily crafted in a manner that is useful to support policy development and decision making amongst the Executive Branch and the various IC components. Consequently, this writing style is often considered vague or "un-actionable" by state and local officials, as they tend to desire information that is of more operational value. This theme was verified by triangulating various sources of research, including the Delphi panel. Unfortunately, while state and local officials have been identified as essential partners in our nation's counterterrorism efforts, for too many years the IC did not consider them primary customers for their intelligence products.[138] The NCTC's Director recognizes that the Center must do a better job tailoring intelligence products to support "'non-traditional partners' such as FBI Joint Terrorism Task forces; [and] state, local, and tribal homeland security officials."[139]

Executive Order 13354 mandated the NCTC's responsibility for supporting DHS, DOJ, and other federal agencies as they fulfill their responsibility to disseminate terrorism-related information to state, local, and tribal officials.[140] While the Center now incorporates representatives from numerous federal organizations, during its first three

---

[137] Leiter, "Looming Challenges in the War on Terror," 3.

[138] Tom Facer, "Interagency Threat Assessment and Coordination Group," (presentation to the 2008 National Fusion Center Conference, San Francisco, CA, March 17–20, 2008).

[139] Leiter, "Looming Challenges in the War on Terror," 3.

[140] *Executive Order 13354.*

years of implementation it included of no state, local, or tribal representation. Consequently, the bulk of the NCTC's terrorism analysis was provided exclusively to the IC and high-ranking government officials; since its inception, little created within the Center has been provided to non-federal agencies, which are outside the Center's original mission space.[141]

C. ITACG: THE MISSING LINK?

1. Past and Present Challenges

The ITACG was passed into law in 2007 to help facilitate the sharing of terrorism-related information amongst federal, state, local, tribal, and private sector officials. The NCTC, based on its mission mandates, directly supports no such audience; therefore, the ITACG is intended to assist in mitigating this information-sharing gap. The initial creation and development of the ITACG was a difficult process, inhibited by bureaucratic roadblocks and disagreements amongst agencies. However, as a new organization within an already complex and evolving environment, it was inevitable that difficulty would be experienced. The author's various research methodologies corroborate a notion that the ITACG was created to resolve the dissatisfaction of Congress and senior leadership from state and local government regarding in the DHS's ability to carry out its statutory responsibilities mandated in the Homeland Security Act of 2002, more specifically, regarding the level and quality of support provided by the Department to state and local first responders. The memorandum of agreement (MOA) for the initial standup of the ITACG was approved on August 29, 2007, and was subsequently signed without delay by all necessary agency representatives, except DHS. According to media sources, the Department was the only organization involved that believed state and local officials should not participate in the organization.[142] DHS officials questioned the MOA's lack of information regarding the ITACG Advisory Council, and they requested that the MOA be clarified "to ensure that the creation of the

---

[141] Wait, "Where the Data Meets the Road."

[142] Siobhan Gorman, "Out of the Loop on Terror Threats: Homeland Security Excludes State, Local Officials from Group that Shares Data," *Baltimore Sun*, February 2, 2007, http://insaonline.org/pdfs/Article%202-Baltimore%20Sun.pdf (accessed June 1, 2008).

ITACG in no way restricts the Office of Intelligence and Analysis (I&A) from either producing or disseminating its own intelligence products."[143] This ultimately led senior lawmakers from Congress to believe that DHS viewed the ITACG as a threat to I&A, rather than an opportunity for greater information sharing.[144] Senior DHS officials indicated that the Department would represent the interests of state and local officials, and that it was not necessary to include them directly.[145] Reports also suggested that DHS officials were opposed to allowing state, local, and tribal officials serve within the ITACG because they believed it would create "unnecessary confusion."[146] Proponents of state and local inclusion suggested that DHS was reluctant to give up the power associated with controlling the flow of information to non-federal entities.[147] Consequently, it took over two months for the Department to finally agree and sign the ITACG's MOA, which ultimately caused delays in the organization's implementation.

The ITACG was eventually implemented in October of 2007, and it gained its initial operating capability in late January 2008 when it was fully accepted under the management of the NCTC. Hearings in late February 2008 indicated that Congress remained dissatisfied with the Department's progress in managing the ITACG, as lawmakers voiced concerns and skepticism related to the extent in which DHS would fully embrace the ITACG's intended purpose to break down information-sharing walls.[148] However, the author's professional experience indicates that those involved in

---

[143] Thompson, Bennie G., Peter T. King, Harman, Jane, Riechert, David G. (Subcommittee on intelligence, Information Sharing, and Terrorism Risk Assessment), "Committee Leaders Write Secretary Chertoff Regarding ITACG," to Michael Chertoff (Secretary, U.S. Department of Homeland Security), September 26, 2007, http://chsdemocrats.house.gov/SiteDocuments/20070927104243-98852.pdf (accessed December 10, 2007).

[144] "Committee Leaders Urge Secretary Chertoff to Move Forward with Information Sharing," in *United States House of Representative Committee on Homeland Security*, September 27, 2007, http://chsdemocrats.house.gov/press/index.asp?ID=275&SubSection=3&Issue=0&DocumentType=0&PublishDate=0 (accessed December 10, 2007).

[145] Gorman, "Out of the Loop on Terror Threats."

[146] Ibid.

[147] Ibid.

[148] Jason Miller, "Better Information Sharing on the Horizon," *Federal Computer Week*, November 15, 2007, http://fcw.com/articles/2007/11/15/better-information-sharing-on-the-horizon.aspx (accessed December 19, 2007); Ben Bain, "Lawmakers Blast DHS' Efforts to Share Intel with State, Local Partners," *Federal Computer Week*, February 28, 2008, http://fcw.com/articles/2008/02/28/lawmakers-blast-dhs-efforts-to-share-intell-with-state-local-partners.aspx (accessed March 22, 2008).

its development—including DHS—have since worked to overcome bureaucratic obstacles and many of the cultural issues that have impeded information sharing for decades, while advocating on behalf of our nation's "first preventers/responders," who operate outside the IC's traditional federal realm.

The ITACG's collocation at the NCTC is designed to afford state, local, and tribal representatives unprecedented access to counterterrorism subject matter experts, direct interaction with those producing intelligence for both federal and non-federal consumption, and access to numerous classified and unclassified information systems and sources contained within the confines of the Center. However, this access is only granted to those assigned to the Detail; and due to the high-classification of the information, the vast majority of the information reviewed remains just as compartmentalized after the ITACG's review, as it did previously. While, the daily NCTC-Intelligence Community briefings and teleconferences afford the ITACG access to highly classified terrorism-related information, this information is rarely shared outside the Center due to its classification. Some may argue that such access is unprecedented and represents a remarkable cultural shift, as well as a significant change in information-sharing policies and practices and trusted relationships amongst disparate levels of government. However, how much value does this model of information sharing provide to state and local first responders when the sharing typically ends with those detailed to the ITACG? After all, the NCTC does not have the ITACG Detail representatives acting in their official capacities; rather, they are deputized federal employees and have no authority to report information back to their home agency. State and local agencies with personnel assigned to the ITACG find comfort knowing that their personnel are contributing to the national intelligence cycle for counterterrorism but find it difficult knowing that their personnel cannot share the vast majority of the information they are privy to outside the NCTC.[149] The ITACG is not meant to be a point-of-contact for state and local agencies, or a conduit to received information from the NCTC. Due to the limited number of personnel

[149] Unnamed law enforcement source, interview with author, Boston, MA, August 21, 2010.

operating at the Center, opening the door to such communication exchange would quickly overwhelm the Detail and would take it away from its daily review and coordination responsibilities.[150]

Ultimately, challenges have been identified from conflicting visions related to the size and role of the ITACG—particularly, regarding whether or not the organization should be a stand-alone intelligence analysis and production entity.[151] Some advise that this should not be the end result of this organization, as it would lose the information connectivity it has acquired from its current arrangement disrupt its collaboration with other agencies collocated within the NCTC. Furthermore, a modification such as this has the potential to create an additional information stovepipe, which would undermine the efforts and successes that have already been experienced from the organization's current orientation. As our government continues to develop the Information Sharing Environment, bridging together disparate agencies that seek to protect our nation from terrorism, it is increasingly necessary to integrate expertise from all disciplines and levels of government to enhance intelligence production and analysis efforts. Creating a "stand alone" entity to fulfill the mission set forth in the ITACG charter would prove counterproductive.

Administrative issues related to sustaining ITACG operations remain a significant challenge, as officials have experienced complications recruiting personnel to fulfill the requirements of the Detail, and Congressionally appropriated funding for its operation has not been secured beyond FY2012.[152] Due to the nature of the staffing requirements and the deteriorating condition of the nation's economy, state and local public safety agencies are hesitant to give up their best and brightest to a year-long detail outside their

---

[150] Timothy Connolly (Boston Police Department), interview with author, New Orleans, LA, February 25, 2010.

[151] Michael Leiter, "Making Homeland Security Intelligence Work for State, Local, and Tribal Partners: An Interagency Threat Assessment Coordination Group Progress Report," *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, Washington, D.C., 110th Congress, 2nd Sess., March 13, 2008, http://www.gpo.gov/fdsys/pkg/CHRG-110hhrg43955/html/CHRG-110hhrg43955.htm (accessed March 22, 2008), 13.

[152] Program Manager, *2010 Report on the Interagency Threat*, 15

jurisdictions when little measurable benefit is reciprocated directly to the host agency.[153] Many of our nation's public safety agencies are currently operating at or below minimum staffing levels, and thus it is difficult justifying the loss of additional positions from daily operations. There has been significant focus on the amount of time individuals are assigned to the ITACG, incentives for the assignments, and how ones relocation to the Washington, D.C. area can be made easier. Furthermore, it is unknown whether or not Congress has seen enough benefit from the ITACG's operation to warrant sustaining its operation.

According to one local official:

> Some feel that it is unclear what role state, tribal and local law enforcement will actually play within the ITACG, as the [ISE Implementation] Plan appears to limit participation to representatives from DHS, FBI, DOD, and other 'relevant Federal (emphasis added) organizations.' Further, the Plan emphasizes that, although it is going to be co-located with the NCTC, the ITACG 'will not be a part of the NCTC,' and it 'is not intended to duplicate, impede, or otherwise interfere with the existing and established counterterrorism roles and responsibilities.' Consequently, on several levels, the ITACG does not appear to address fully the concern that the NCTC is lacking in non-federal representation. Indeed, the Plan's language refers to producing 'federally coordinated' information instead of 'jointly coordinated,' or more ideally, 'collaboratively produced intelligence.'[154]

According to a local official currently assigned to the Detail:

> The ITACG efforts are intended to complement and supplement existing analytic, production, and dissemination efforts by Federal entities. The ITACG does not create, transfer, or deliver intelligence products; rather, it helps to facilitate these processes through established DHS and FBI mechanisms [see Figure 9].[155]

Internal to the NCTC, the provision of appropriate security clearances for those detailed to the ITACG and coordinating disparate fellowship programs to fund the

---

[153] Michael Quick (Las Vegas Metropolitan Police Department), interview with author, Monterey, CA, June 24, 2010.

[154] Ron Leavell, "Evolution of Regional Counterterrorism Centers Within a National Counterterrorism Network: Is It Time to Fuse More Than Information?" (master's thesis, Naval Postgraduate School, 2007), 74–75.

[155] Connolly, interview with author.

organization has proven difficult. Challenges also remain in "bottom-up" information sharing from state and local officials and the fact that the establishment of feedback mechanisms—outside the existing informal communication chains—has yet to be determined.[156]

Figure 9. ITACG Facilitated Dissemination Procedure[157]

It is, however, important to note the many successes of the ITACG since its implementation. The ITACG signifies a new and enhanced relationship between the IC and non-federal public safety officials. Most significantly, it involves for the first time, inclusion of the "state, local, and tribal perspective" in the intelligence activities occurring at the national level. During the first months of the ITACG's development, those assigned to the organization focused a significant amount of time reviewing previously published intelligence products for information of value, requesting

[156] Quick, interview with author.

[157] Connolly, "Interagency Threat Assessment and Coordination Group."

classification downgrades, and assisting with product tailoring efforts.[158] Between October 23, 2007 and April 7, 2008, over 40,000 previously published intelligence products were reviewed, resulting in the identification of 25 "valuable" products that had not been disseminated—16 of which were subsequently downgraded and re-disseminated.[159] Additionally, over 2,588 threat reports were reviewed—97 of which were related to the U.S. and identified for state, local, and tribal use.[160] Ultimately, existing reports that were not downgraded or released for state and local consumption during the course of the ITACG's comprehensive review were verified by those detailed to the ITACG as outside the needs of state and local officials and, thus, irrelevant to their operational requirements.

More recently, however, the ITACG's subject matter expertise has been leveraged in order to shape products by providing substantive input as they are published or prior to their dissemination.[161] Currently, all the intelligence products that leave the NCTC and are intended for state and local consumption are reviewed by the ITACG prior to their release. Such measures have involved efforts to put intelligence sources, as well as the threats portrayed, into proper context to assist state and local officials in their efforts to increase awareness and establish defensive postures, while avoiding "over-reaction" and unnecessary resource deployment and expenditures. For the same reason, equally sufficient measures have been taken to provide greater detail in finished intelligence products distributed to state and local partners. For example, according to an ITACG representative:

> The ITACG assisted NCTC analysts in the tailoring of an intelligence product regarding Ricin toxicity and use, precipitated by the discovery of the rare, yet toxic substance in a Las Vegas motel room in late February 2008. Accordingly, those detailed to the ITACG recommended specific modifications to make the product more useful to state, local, and tribal law enforcement and first responders, as the product in its original state lacked critical information necessary for safe response and mitigation

---

[158] Connolly, "Interagency Threat Assessment and Coordination Group."

[159] Ibid.

[160] Ibid.

[161] Ibid.

> protocols. The detailees requested an enhanced description regarding what constituted a lethal dose of Ricin, as well as additional descriptors—such as what it looks and smells like in various forms—so that law enforcement and other first responders could be more prepared if or when they encountered the substance. The original product recommended 'wearing personal protective equipment (PPE)' when Ricin is suspected; the ITACG requested the minimum safe level of protective equipment be identified in the final product, so that law enforcement officials could decide if they are properly equipped to respond, or if they should request the assistance of specially trained HAZMAT personnel.[162]

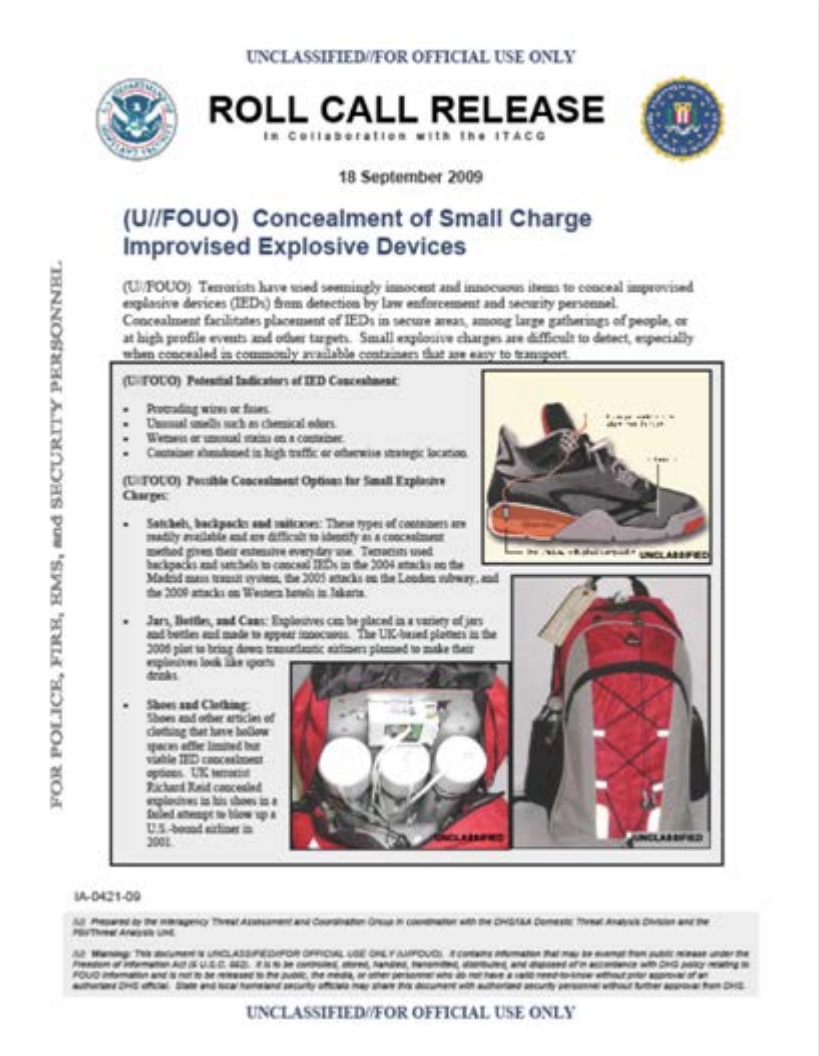
One of the most broadly recognized outputs of the ITACG is the *Roll Call Release* (see Figure 10). The *Roll Call Release* is a joint DHS-FBI publication, produced at the Unclassified For Official Use Only release-classification, which includes significant input from the ITACG Detail for state and local relevance. The contents of the product are kept very brief and include photos, illustrations, and short information summaries focused on indicators, tactics, techniques, procedures, and trends related to terrorism, homeland security, and weapons of mass destruction.[163] Additionally, most products provide directions for the reader to find additional information relative to the topics discussed, so that more research can be conducted if desired. Research verified that this is a first-of-its-kind production designed exclusively for release to non-federal, "street level" first responders. The reaction to this product from state and local officials has been mixed: research indicates that to some, the information provided is "elementary" and bears little value, while others that traditionally have less exposure to the information provided through this publication find it highly valuable.[164] Overall, the *Roll Call Release* productions can be evaluated as successful considering that their contents are often derived from intelligence gleaned from both past and recent terrorism investigations, and thus fills an intelligence gap for many with public safety responsibilities.

---

[162] Connolly, "Interagency Threat Assessment and Coordination Group."

[163] Connolly, interview with author.

[164] Michael Quick, "Production, Dissemination, and Feedback" (presentation to the Fusion Center Leaders Program, U.S. Naval Postgraduate School, Monterey, CA, June 24, 2010).



UNCLASSIFIED//FOR OFFICIAL USE ONLY

ROLL CALL RELEASE

In Collaboration with the ITACG

18 September 2009

(U//FOUO) Concealment of Small Charge Improvised Explosive Devices

FOR POLICE, FIRE, EMS, and SECURITY PERSONNEL

(U//FOUO) Terrorists have used seemingly innocent and innocuous items to conceal improvised explosive devices (IEDs) from detection by law enforcement and security personnel. Concealment facilitates placement of IEDs in secure areas, among large gatherings of people, or at high profile events and other targets. Small explosive charges are difficult to detect, especially when concealed in commonly available containers that are easy to transport.

(U//FOUO) **Potential Indicators of IED Concealment:**

- Protruding wires or fuses.
- Unusual smells such as chemical odors.
- Wetness or unusual stains on a container.
- Container abandoned in high traffic or otherwise strategic location.

(U//FOUO) **Possible Concealment Options for Small Explosive Charges:**

- **Satchels, backpacks and suitcases:** These types of containers are readily available and are difficult to identify as a concealment method given their extensive everyday use. Terrorists used backpacks and satchels to conceal IEDs in the 2004 attacks on the Madrid mass transit system, the 2005 attacks on the London subway, and the 2009 attacks on Western hotels in Jakarta.
- **Jars, Bottles, and Cans:** Explosives can be placed in a variety of jars and bottles and made to appear innocuous. The UK-based plotters in the 2006 plot to bring down transatlantic airliners planned to make their explosives look like sports drinks.
- **Shoes and Clothing:** Shoes and other articles of clothing that have hollow spaces offer limited but viable IED concealment options. UK terrorist Richard Reid concealed explosives in his shoes in a failed attempt to blow up a U.S.-bound airliner in 2001.

UNCLASSIFIED

IA-0421-09

UNCLASSIFIED//FOR OFFICIAL USE ONLY

Figure 10. Example of Roll Call Release[165]

Additionally, the ITACG's expertise has been harnessed to publish the *Intelligence Guide for First Responders*, a joint production by state, local, and federal partners engaged through the activities of the ITACG (see Figure 11). The guide was designed to assist state, local, and tribal first responders in accessing and understanding federal counterterrorism, homeland security, and weapons of mass destruction reporting.[166] It provides first responders that work outside the federal government with an overview of intelligence and the IC; what reporting is available to state, local, tribal,

[165] "(U//FOUO) Concealment of Small Charge Improvised Explosive Devices," *Roll Call Release* (Washington, D.C.: Interagency Threat Assessment and Coordination Group, September 18, 2009).

[166] Connolly, interview with author.

and private sector officials and how to access it; understanding threat information; and IC terminology and acronyms. Mass quantities of the guide were provided to fusion centers for release to their homeland security partners and to over 48,000 state, local, and tribal police and fire departments across the nation. Additionally, PDF versions of the guide have been posted to several secure portals and are available for computer download and re-posting purposes.[167]

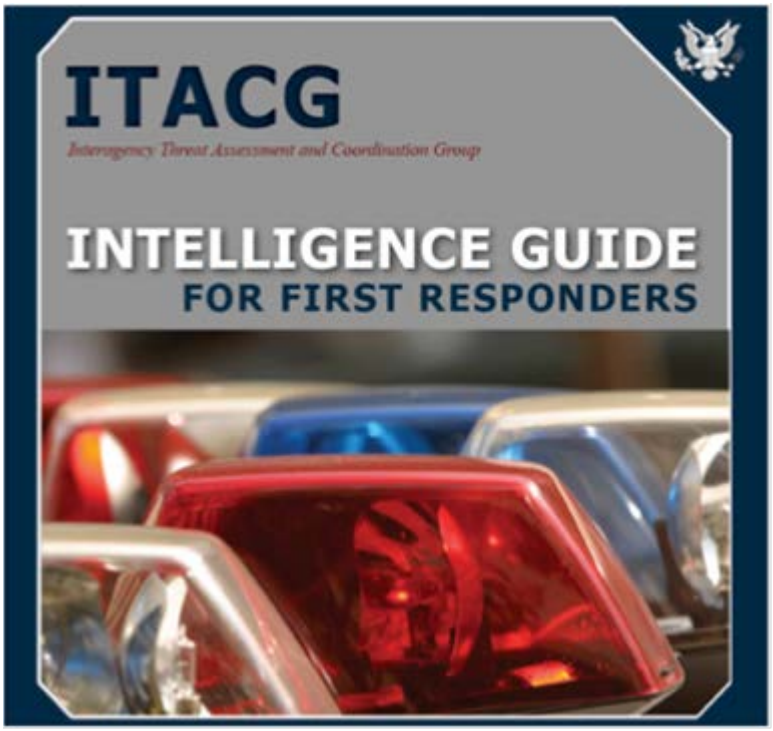


Figure 11. ITACG Intelligence Guide for First Responders[168]

Efforts are being made to educate state, local, and tribal officials of the role of the ITACG and to assist them in accessing the information it coordinates. The ITACG interacts with state and local partners during a weekly threat teleconference and bi-weekly video teleconference hosted by DHS.[169] In addition, the Detail also delivers its

[167] Program Manager, Information Sharing Environment, *2010 Annual Report to Congress* (Washington, D.C.: Program Manager, Information Sharing Environment, 2010), 25.

[168] Interagency Threat Assessment and Coordination Group, *ITACG: Intelligence Guide for First Responders* (Washington, D.C.: Interagency Threat Assessment and Coordination Group, 2009).

[169] Connolly, interview with author.

information-sharing message during national conferences, ad hoc meetings, and formal training events. These presentations include analyst training through the Defense Intelligence Agency's Advanced Counterterrorist Analyst Course, the DHS Basic and Mid-level Intelligence Terrorism Analysis Course, and the FBI Basic Analyst Course. Additionally, and perhaps most importantly, the ITACG is working to define the most effective means of integrating with state and local fusion centers.[170]

According to the *July 2010 Information Sharing Environment Annual Report to Congress:*

> Over the last year the ITACG:
>
> - Contributed to the publication of approximately 34 *Roll Call Releases* relating to terrorism, homeland security, and WMD threats;
> - Reviewed, provided comments, or proposed language to 403 Intelligence Community products prior to publication by the originating agencies; and
> - Requested downgrading of 78 classified Intelligence Community products.[171]

D. CONCLUSION

As our government continues to develop the Information Sharing Environment, bridging together disparate agencies that seek to protect our nation from terrorism, it is increasingly necessary to integrate expertise from all disciplines and levels of government to enhance intelligence production, analysis and sharing efforts. The federal government's model of facilitating the ISE must be further refined to incorporate greater collaboration with state and local officials to ensure relevant intelligence is both developed for and provided to those in positions to protect the homeland, beyond their traditional IC customers. The ITACG is a relatively new development within the federal government that, if integrated appropriately within both the NCTC and national network of fusion centers, has the potential to mature and become the much-needed conduit of the desired intelligence-sharing continuum. To date, considering the ITACG's capabilities

---

[170] Murphy, "Making Homeland Security Intelligence Work," 4.

[171] Program Manager, *2010 Annual Report to Congress*, 25.

and limitations, it has gained considerable ground integrating with the IC and advocating for first responders. The following chapters aim to provide recommendations to enhance this much-needed continuum.

THIS PAGE INTENTIONALLY LEFT BLANK

VII. RECOMMENDATIONS: MAKING FUSION CENTERS WORK

A fusion center's effectiveness is dependent on its ability to analyze disparate streams of information and consistently share timely, accurate, and relevant intelligence that augments the decision-making abilities of a broad group of stakeholders, thereby increasing public safety and homeland security. As corroborated from the previous analyses, fusion centers are experiencing difficulty satisfying this objective, which is the very purpose of their existence. If working properly, fusion centers will improve the overall safety of a state or region by influencing the establishment of proactive, resource-efficient security strategies in response to threat scenarios. Ultimately, this requires that leadership at fusion centers develop broad-reaching, trusted partnerships for gathering information and sharing relevant intelligence; as well as policies and procedures to ensure that the processes and guidelines that govern a well-functioning intelligence-sharing enterprise become doctrine. Through the creation of a "megacommunity," the author provides several policy options, triangulated through research, to make fusion centers work properly.

A. THE PUBLIC SAFETY "MEGACOMMUNITY"

1. Collaboration

Among the most significant themes corroborated in the analysis of fusion centers is their limited collaborative capacity. Collaboration is essential, as highlighted in the tenets of the *Fusion Center Guidelines*:

> The ultimate goal [of a fusion center] is to provide a mechanism through which government, law enforcement, public safety, and the private sector can come together with a common purpose and improve the ability to safeguard our homeland and prevent criminal activity.…Fusion centers embody the core of collaboration, and as demands increase and resources decrease, fusion centers will become an effective tool to maximize available resources and build trusted relationships.[172]

[172] Global Justice Information Sharing Initiative, *Fusion Center Guidelines*, 4.

However, as was apparent from the analyses presented in Chapter V, fostering a unified, "team" approach amongst numerous, disparate organizations, and generating the capacity to execute a comprehensive strategy is no simple task. Ultimately, collaboration involves more than just two-way communications and having partners on the receiving end of an information product. Rather, collaboration requires shared, mutual involvement in planning, coordination, decision-making, and operational activities, which for statewide or regional purposes, necessitate a more intimate involvement of diverse agencies in contributing to the fusion center mission. Most notably, collaboration promotes trust, which is essential for effective intelligence production and sharing—a requirement verified through the author's research. The success of a fusion center demands collaboration with a diverse group of government, law enforcement, public safety, and private sector agencies to fulfill strategic planning, prioritization, information sharing, analysis and intelligence production, as well as threat detection and mitigation requirements. As such, a practicable strategy for each respective center should be the initiation and sustainment of a megacommunity. Executives from Booz Allen Hamilton have defined the term megacommunity as "a collaborative socioeconomic environment in which business, government, and civil society interact according to their common interests, while maintaining their unique priorities."[173]

A common interest among business, government, and civil society is public safety. Therefore, the mission of the recommended megacommunity, for example, is to provide security to the state or region through the early identification threats, effective communication, reduction of vulnerabilities, implementation of effective incident-response strategies, and the mitigation of risk to ensure overall public safety. Such a mission would be in the best interests of all area businesses and organizations, as each requires the aforementioned security attributes for continuity of operations, the promotion of a healthy economic environment, and the preservation of a desirable quality of life for all citizens. Accordingly, the fusion center would be the primary intelligence coordination component within the megacommunity, successfully integrated with all law

[173] Mark Gerencser, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together* (New York: Palgrave MacMillan, 2008), 232.

enforcement, public safety, intelligence, and security entities operating within the area, as well as all organizations within the state or region that have a vested interest in security and public safety. Thus, the success of the megacommunity requires a tremendous amount of agency/organization buy-in, all must contribute to, understand, and agree to the overarching mission and related strategies. Moreover, each organization must conform to their individual roles within the megacommunity and be willing to work together collaboratively towards common goals. For fusion center purposes, this equates to the identification of individual megacommunity member intelligence needs; the routine delivery of information to the center by all megacommunity entities; megacommunity collaboration on information collection strategies and subsequent analyses; and the fusion center's timely delivery of relevant, actionable intelligence to each respective megacommunity partner to help support public safety and fulfill the overarching mission. Each of the aforementioned requirements was recognized as strongly correlating variables in the author's research triangulation.

In the initial development of a megacommunity, a core group of existing fusion center executives must be selected to serve as ambassadors of the center for outreach and marketing purposes. This group's primary responsibility should be to execute the role of "initiators," and, thus, move the fusion center—and the megacommunity—from the latent stage—where overlapping issues have been recognized, but multi-agency, multi-discipline collaboration is nonexistent—to the active state of a cross-sector collaborative environment.[174] This philosophy blends well with suggestions in both the *Fusion Center Guidelines* and the *Baseline Capabilities for State and Major Urban Area Fusion Centers* in that it recommends the establishment of a governance board or advisory group to guide the strategic planning of the center.[175]

Expanding upon the center's existing partnerships, the initiators must promote greater outreach to create a diverse enterprise that focuses on both the overarching and unique needs of a broad group of public, private, and government stakeholders within the respective state or region. It is, therefore, recommended that fusion center executives

[174] Gerencser, Van Lee, Napolitano, and Kelly, *Megacommunities*, 139.

[175] Global Justice Information Sharing Initiative, *Baseline Capabilities*, 23.

carefully map out the desired megacommunity with a matrix that includes a list of potential stakeholders and a description of their interests, objectives, and relationships (see Figure 12).[176] The resulting matrix can then be used as a guide for all subsequent recruiting efforts conducted by the initiation team and, subsequently, to identify and document sector- and agency-specific intelligence requirements that enable the center in creating niche analysis and reporting for its product line. The identification of consumer-specific intelligence requirements was corroborated by the author's research methodologies as a requirement for successful fusion center operations.

[176] Gerencser, Van Lee, Napolitano, and Kelly, *Megacommunities*, 127.

Public Safety Megacommunity Stakeholder Matrix			
Sector	**Agency/Organization**	**ILO**	**Requirements**
Agriculture/Food/ Water/Environment	Boston Water & Sewer	YES	Quarterly briefing; Weekly report…
	MA Dept. of Agriculture	YES	Weekly report…
	Food & Drug Administration	NO	Annual summary…
	Environmental Protection Agency	YES	Weekly report…
Banking & Finance	John Hancock	NO	Quarterly briefing; Threat Advisory…
	Fidelity Investments	YES	Quarterly briefing; Threat Advisory…
	State Street Bank	YES	Quarterly briefing; Threat Advisory…
Chemical Industry & Hazardous Material	Dow Chemical	NO	Annual summary; Bi-weekly Conf Call…
	Accenture	NO	Annual summary; Bi-weekly Conf Call…
	Ironwood Pharm	NO	Quarterly briefing; Weekly report…
Criminal Justice	…	…	…
Education	Boston Public Schools	YES	Bi-weekly Conf Call; Daily report…
	Boston University	YES	Bi-weekly Conf Call; Daily report…
	Mass Institute of Technology	YES	Bi-weekly Conf Call; Daily report…
	Harvard University	YES	Daily Report; Quarterly briefing…
Emergency Services	…	…	…
Energy	Nstar	YES	Quarterly briefing; Threat Advisory…
	National Grid	YES	Quarterly briefing; Threat Advisory…
	GDF SUEZ/Distrigas of MA	YES	Quarterly briefing; Threat Advisory…
Government	…	…	…
Health & Public Health Services	BU Medical Center	YES	Quarterly briefing; Threat Advisory…
	Partners Healthcare	NO	Annual summary; Bi-weekly Conf Call…
	Beth Israel Deaconess	YES	Annual summary; Bi-weekly Conf Call…
	Mass General Hospital	YES	Quarterly briefing; Threat Advisory…
	Brigham & Woman's Hospital	YES	Annual summary; Bi-weekly Conf Call…
	Dana Farber	NO	Quarterly briefing; Threat Advisory…
Hospitality & Lodging	Hilton	YES	Weekly report; Quarterly briefing…
	Marriott	YES	Weekly report; Quarterly briefing…
	Hyatt	YES	Weekly report; Quarterly briefing…
Information & Telecommunications	Verizon	NO	Annual summary; Bi-weekly Conf Call…
	Comcast	YES	Annual summary; Bi-weekly Conf Call…
Military Facilities and Defense Industrial Base	Fort Devins	NO	Weekly report; Quarterly briefing…
	Otis Air Force Base	YES	Weekly report; Quarterly briefing…
	Army Recruitment Facility	YES	Threat Advisories; Quarterly briefing…
Postal & Shipping	FedEx	NO	Quarterly briefing; Annual summary…
	USPS	YES	Weekly report; Quarterly briefing…
	UPS	NO	Quarterly briefing; Annual summary…
Private Security	Ameriguard	NO	Weekly report; Quarterly briefing…
	Securitas	YES	Weekly report; Quarterly briefing…
	Paragon	NO	Weekly report; Quarterly briefing…
Public Works	Boston Public Works	YES	Quarterly briefing; Annual summary…
Real Estate	Boston Properties	YES	Weekly report; Quarterly briefing…
	Copley Real-estate	YES	Weekly report; Quarterly briefing…
Retail	Newbury Street Business League	NO	Weekly report; Quarterly briefing…
	Dorchester Business Assoc.	NO	Weekly report; Quarterly briefing…
Social Services	Boston Public Health	YES	Bi-weekly Conf Call; Daily report…
Transportation	MA Bay Transportation Authority	YES	Daily Report; Threat Advisories…
	Boston Coach	NO	Quarterly briefing; Annual summary…
	Metro Cab	NO	Quarterly briefing; Annual summary…

Figure 12. Public Safety Megacommunity Stakeholder Matrix

It is critical that communication during outreach, strategic planning, and all ensuing efforts focus on the overlapping vital interests of the prospective

megacommunity agencies and organizations; thus, connections must be made between their intelligence needs to maintain public safety, security, and operational continuity, and the events transpiring locally, nationally, and internationally.[177] Accordingly, linking local security issues with global trends (such as existing and emerging criminal activity trends, natural disasters, and domestic and international terrorist threats) will help to stimulate the interests of the identified stakeholders to augment buy-in and participation, and enhance their understanding of the underlying mission of the megacommunity, the current threat picture, and their application to the state or region.

This approach will also aid in marketing the fusion center and identifying how it can work to satisfy each community member's intelligence needs. Furthermore, routine, coordinated strategy meetings are necessary to introduce and provide an orientation for new participants; maintain trusted relationships and commitments to established objectives; collect and discuss feedback from both prior and current engagements; address problems, concerns, successes, and lessons learned; and refocus strategies according to evolving issues and priorities. This will provide the collaborate capacity required for successful fusion activities.

2. Capabilities and Limitations

The author's research corroborated that fusion center leaders must also work to educate their stakeholders of the capabilities and limitations of the center on an ongoing basis and provide relevant updates as the center's human capital grows and additional skills sets, technology, and resources are attained.[178] Nationally, fusion centers are at various stages of development; not all currently have the analytic capabilities, technology, or degree of subject-matter expertise available to meet all of the needs of

[177] Gerencser, Van Lee, Napolitano, and Kelly, *Megacommunities*, 139.

[178] See appendix.

consumers.[179] Furthermore, what some consumers may expect from their fusion center may not be possible; thus, it is important that consumers not base their expectations on unreasonable standards.

A common misconception about intelligence is that personnel at fusion centers should know everything about everything, oftentimes before an event occurs. This is completely false and a misunderstanding of what capabilities truly exist within the confines and reach of a fusion center. Intelligence analysts at fusion centers will rarely beat the media to a high-profile incident or event; this is not necessarily what intelligence is meant to do, and all stakeholders must be educated of this. However, the by-products of intelligence analysis should assist fusion center consumers in avoiding strategic surprise and ensure that they are adequately prepared for potential incidents related to current threat streams. Ultimately, the capabilities and limitations of the fusion center must be clearly articulated during the initial and subsequent meetings with partner agencies and organizations. As capabilities change, partners and consumers must be informed and adjustments must be made to existing intelligence priorities, products, and processes.

Additionally, routine meetings with consumers can be used as bilateral educational forums to learn the purpose and significance of the various products and services that each agency (including the fusion center) can provide, the different analytic and industry writing styles and lexicons, and the integral functions of the intelligence, law enforcement, public safety, and private and public sector organizations involved in the fusion efforts, joined together in the megacommunity. It is necessary that members of the megacommunity work towards the goal of communicating with a common language eliminating the opportunity for inconsistencies that contribute to misunderstandings, confusion, and improper guidance. This will ultimately lead to a greater understanding of each representative's perspective and objectives, as well as the capabilities and

[179] CENTRA Technology, *Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps* (Burlington, MA: February 2008), 12.

limitations of participants.[180] Understanding each other's needs is important for sustaining a collaborative environment and maintaining focus on the overlapping requirements of the participants. Most importantly, this will also help foster trust and help facilitate the desired continuum of information flowing to and from the fusion center and all of its partner agencies and organizations.

3. Development of Intelligence Liaison Officer Programs

The author's research triangulation has verified that the race to collocate representatives from numerous agencies within the confines of a fusion center may be losing momentum and understandably so. The traditional fusion center design emphasizes multi-agency collocation, as placing operational personnel together in the same room has been found to accelerate the development of trusted relationships and facilitate collaboration.[181] However, many agencies and organizations find difficulty dedicating limited resources to initiatives that withdraw personnel from their traditional assignments. For example, after 9/11 the resources of local law enforcement agencies were stretched thin as they attempted to adapt and manage both traditional anti-crime efforts and new anti-terrorism priorities.[182] Making matters more difficult, over the course of several years, the majority of cities across the U.S. have experienced increasing violent crime rates, coupled with decreasing law enforcement staffing capacities.[183] As a result, agency leaders have expressed concerns regarding the fact that if officers are guarding critical infrastructure during heightened security alerts, essential resources may not be available to police the streets.[184] Continuity of "normal" business operations is a fundamental requirement for any organization's success; therefore, it is critical that those resources considered necessary for addressing standard agency needs are able to contribute to fusion center priorities without disrupting their normal duties. Nevertheless,

---

[180] Gerencser, Van Lee, Napolitano, and Kelly, *Megacommunities*, 171–172.

[181] Global Justice Information Sharing Initiative, *Fusion Center Guidelines*, 29.

[182] Rosen, *Chief Concerns*, 1. In 2005, the Unified Crime Reports indicated the largest single year violent crime increase in 14 years; this trend of increasing violence continued through 2008.

[183] Ibid.

[184] Ibid.

while agencies are encouraged to collocate key resources within fusion center facilities to meet desired staffing requirements, those that cannot afford to dedicate resources to the facility on a full-time basis should not be discouraged from participating in a fusion center's operations.

It should also be noted that there are logistical challenges that affect collocation. It has been realized that many of the fusion center facilities are not large enough to house representatives from all agencies, organizations, and sectors that exist within a given state or region, nor would this be necessary for the purposes of everyday operations. Moreover, providing each representative the required network connectivity to access their agency's data, records management systems, and communications networks can be extremely costly and challenging. Furthermore, due to the sensitivity of the information that is routinely handled within each facility (i.e., law enforcement, terrorism, homeland security), legal issues exist that put into question the presence of some public and private sector personnel within fusion centers, as they cannot legally view certain sensitive or personal identifiable information included in most law enforcement information.[185] As previously indicated, all entities participating in the collaborative environment must continue to satisfy their respective agency's routine priorities. Thus, it is important that each representative maintain the ability to continue functioning in their normal capacity while providing value to the fusion center and, ultimately, the megacommunity. Solutions must be identified that are capable of addressing the aforementioned collaboration challenges.

A means of fulfilling the fusion center–megacommunity concept at the ground level is through the implementation of community, interagency, and sector-specific liaison officer programs. Such programs have proved to be effective in several states and regions, and the author's research corroborates that great success can be realized through

[185] Global Justice Information Sharing Initiative, *Privacy and Civil Liberties Policy Development Guide and Implementation Templates* (Washington, D.C.: Global Justice Information Sharing Initiative, Department of Justice, 2008), 2-1. Fusion centers must satisfy a legal obligation to uphold the U.S. Constitution and protect the privacy rights of U.S. citizens by safeguarding both sensitive and personally identifiable information.

their implementation.[186] Liaison officer programs enhance interagency partnerships, collaboration, outreach, and "reach-back" capabilities by sponsoring qualified representatives from the various agencies and disciplines present within each fusion center's respective state or region, and empowering them to serve as dedicated and vetted liaisons between the center, their host agency, and the megacommunity. Each liaison committed to the program should be trained in matters of intelligence, criminology, counterterrorism, critical infrastructure, and emergency response and management; routinely briefed on current threat streams, as well as the high-risk characteristics of the megacommunity's area; become part of the fusion center's operations and information collection and analysis efforts; and gain access to valuable fusion center resources. Each liaison will ultimately serve as a subject matter expert according to the matters of their respective home organization and will develop valuable expertise and a level of connectivity that is advantageous to the needs of both the fusion center and the organization in which he/she represents.

In theory, each organization involved in the megacommunity should have at least one primary representative to serve in this capacity, depending on the size and characteristics of the organization. Their role will be to ensure connectivity and communication to and from the fusion center while engaged in operational activities—whether directed by the fusion center's priorities or in fulfilling the duties required by their home agency. Accordingly, the liaison will have "both 'outside-in' and 'inside-out' functions," and the liaison's agency will benefit from the development of formal and informal networks established through participation in the fusion center, as well as the larger megacommunity.[187] The Department of Homeland Security and Department of Justice currently fund training programs, based on agency best practices, to provide the liaison officers with the necessary knowledge, skills, and abilities to help fulfill the mission of the fusion center and, ultimately, to help enhance the security and mission

[186] Norman Beasley, Douglas Johnson, Mike Sena, and Rick Salyers, "Liaison Officer Programs" (presentation at the 2008 National Fusion Center Conference, San Francisco, CA, March 18–20, 2008).

[187] Gerencser, Van Lee, Napolitano, and Kelly, *Megacommunities*, 159.

requirements of the megacommunity.[188] Fusion centers should host introductory training events for new liaison officers and convene additional trainings and briefings on a routine basis (such as quarterly or bi-annually) to reinforce the strength of the network, forge stronger interagency relationships, and to educate on the latest threats, information systems, and tools available to assist them in facilitating their role.

The centralization of key assets within the fusion center's facility, combined with the centers connectivity to numerous decentralized hubs established around each individual liaison officer, will create a highly effective hybrid network that is conducive to the overarching intelligence needs of each organization within the megacommunity.[189] The hybrid network structure will help to eliminate issues related to information "stovepiping", as well as communication "bottlenecks" within the network. While the fusion center will be the main conduit for intelligence coordination and analytic resources, the numerous external entities that contribute to the fusion center's operations, acting as force multipliers, will be interlinked to support the megacommunity and, ultimately, provide various degrees of support.

As the fusion center develops intelligence products, the intelligence liaison officers within each respective organization will serve as recipients of the product disseminations. Based on liaison officers' training and understanding of their respective organizations, they will determine who within their organization is best suited to be a direct recipient of specific intelligence released from the center. This accomplishes two important objectives: first, it ensures that the fusion center is not overloading public safety and security personnel with information that is not relative to their operational role, ensuring the fusion center remains relevant. Second, the model streamlines product flow to those in the best position to act upon the intelligence provided, as the liaison officers will know the inner-workings of their respective agencies better than personnel working within the fusion center (see Figure 13).

---

[188] U.S. Department of Homeland Security and Global Justice Information Sharing Initiative, *DHS/DOJ Fusion Process Technical Assistance Program*, 5th ed. (Washington, D.C.: U.S. Department of Homeland Security and Global Justice Information Sharing Initiative, Department of Justice, 2010), 17–18.

[189] Ori Brafman and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations* (New York: Penguin Group, 2006), 159–178.

Reversing the information flow of this model proves just as effective because it ensures that information collected at the "ground-level" by operational personnel is coordinated through the liaison officer and up to the fusion center. After all, it would be counterproductive for information to by-pass the liaison officer to reach the fusion center, as this would circumvent the significant need to keep the liaison officer informed of relevant events occurring within his or her area of responsibility. Liaison officers should be kept privy of all information of significance and, most importantly, related to the intelligence/information requirements and collection priorities identified by the megacommunity leadership. Ultimately, an intelligence-sharing continuum will develop throughout the megacommunity network.

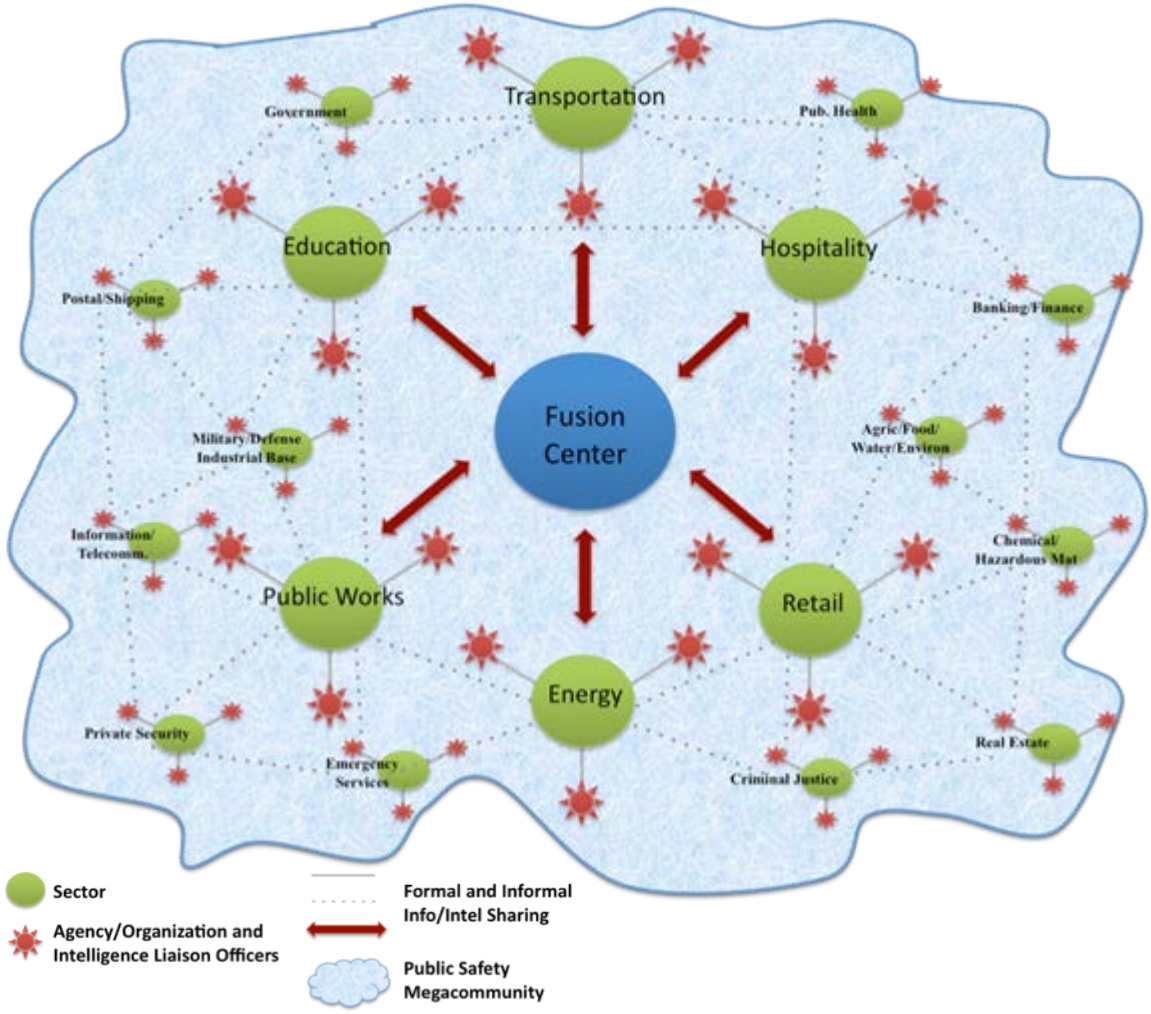


Figure 13. Public Safety Megacommunity[190]

B. CONCLUSION

If fusion centers choose to continue operating in the status quo, there is a significant chance that opportunities to identify activity that could affect the safety and security of the homeland will be missed. Therefore, significant focus must be placed on building a highly collaborative environment—one that embraces the design of a hybrid network and focuses the fusion center's analysis toward the state or region's high-risk

[190] David Carabin, *Public Safety Megacommunity* illustration, August 2011.

assets and the needs of its stakeholders. The recommendations provided in this chapter were verified through triangulation as appropriate solutions to promote a desired intelligence-sharing continuum. Each recommendation presents an opportunity for significant increases in productivity and efficiency throughout all fusion center operations—this will ultimately increase the fusion center's information and intelligence sharing capabilities.

The "Public Safety Megacommunity" model, coupled with a fusion center's comprehensive use of the intelligence cycle, will ensure that intelligence gaps are identified, resources are more effectively and efficiently allocated, all stakeholders' needs are met, and preventive/protective measures are established throughout the state or region. The aforementioned model provides a framework to enable information sharing and increase a community's knowledge of its local environment and how it relates to an international, geopolitical threat environment; furthermore, it promotes an intelligence-sharing continuum amongst all entities within the megacommunity.

While the recommendations provided in this chapter serve to improve fusion center operations and make "actionable" the intelligence produced and shared through fusion centers to a state and local audience, they are only part of the solution this thesis aims to address. The federal government plays a critical role in ensuring the security of the homeland and is a major component of the required intelligence-sharing continuum—via the NCTC, ITACG, DHS and FBI. The following chapter will provide recommendations to improve these components' effectiveness based on the (federal government's) intelligence-sharing issues identified in Chapter VI.

VIII. IMPROVING THE FEDERAL MODEL: ADVANCING THE INTELLIGENCE-SHARING CONTINUUM BY HARNESSING THE ITACG

In today's asymmetric threat environment, it is imperative that an intelligence-sharing continuum exists to facilitate a standardized means for handling, analyzing, and coordinating terrorism-related information, so that actionable intelligence can be provided to empower the decision making of those on the front lines—both domestically and abroad.

The ITACG was created to ensure that relevant intelligence collected at the NCTC is shared beyond the Center's traditional IC consumer base, via DHS and FBI, to meet the needs of non-federal public safety officials (via fusion centers). Arguably, the ITACG was established to begin implementing the required intelligence-sharing continuum. The NCTC, ITACG, DHS, and FBI are currently working together to provide intelligence to fusion centers in a manner that meets their intelligence needs. However, the question remains as to whether or not the current model employed by these organizations to share, interact, and coordinate with state and local public safety officials is working well enough. Was the implementation of the ITACG into the pre-existing model enough to facilitate the required intelligence-sharing continuum?

Measuring the ITACG's level of success or failure is relative to ones expectations. The Detail was established in response to a significant gap identified in the frequency, quality, timeliness, and relevance of information shared by the IC with state and local first responders. During its initial years, the Detail consisted of no more than nine personnel—four of whom were assigned from federal, not local, agencies—each tasked with reviewing thousands of highly classified reports for applicability to a state and local audience. In many ways, they served an auditing roll, which left them in a position where the state and local community would notice little of their tedious work. After a considerable amount of time, the Detail slowly arrived in a position to begin contributing to federal intelligence production and developing new resources and product lines to meet the needs of state and locals.

"The primary mission of the ITACG is to facilitate the production and timely issuance of terrorism-related interagency products for distribution to State, Local, Tribal, Territorial, and Private Sector [SLTTP] partners, as well as other agencies responsible when appropriate," which relies on the performance of the personnel assigned to the Detail, the authority of its leadership, and both cooperation and collaboration of IC professionals.[191] Currently, the Detail consists of 14 people, which is still a small number of personnel to ensure such an important responsibility is fulfilled. Taking into account the fact that there are more than 400 federal officials assigned to the NCTC for terrorism analysis purposes, how significant of an impact can be expected from such a small group of state and local personnel—a group with no authority over the information they are reviewing and even less authority to ensure that it is released at a lesser classification? What "results" should be expected from a group that cannot communicate the information and analysis it is privy to because of significant—and often justified—classification and compartmentalization restrictions, as well as protocols restricting the Detail from serving as a dissemination mechanism?

A recent report of the ITACG's progress states, "Over the last year the ITACG contributed to the publication of approximately 250 intelligence products and 37 Roll Call Releases relating to terrorism, homeland security, and WMD threats. With the [new] development of a performance management framework, the ITACG Advisory Council has set the foundation to create the appropriate performance measures to fully assess the ITACG's progress."[192] For the three and a half years that the Detail has been operating, a significant amount of time has been allocated to defining its existence and developing the processes that justify its relevance. Considering the significant challenges to its operation, the positive differences the ITACG has made thus far should result in significant acknowledgements to those assigned to its operation. Unfortunately, the organization—on its own—will unlikely satisfy the overarching mission requirements for which it was intended, due to limitations in its size, authority, and permissible

[191] National Counterterrorism Center, "ITACG Roles and Responsibilities," http://www.nctc.gov/itacg/itacg_roles_and_responsibilities.html (accessed July 16, 2011).

[192] Program Manager, *2010 Report on the Interagency Threat*, v.

connectivity with state and local officials. And without greater coordination between the ITACG, DHS, and FBI locally (i.e., outside Washington, D.C.), all three entities will continue to fail as enablers of the Information Sharing Environment.

The author provides several recommendations below—each corroborated through the applied research methodologies—that may prove effective in establishing the required intelligence-sharing continuum between the intelligence community and fusion centers by harnessing the ITACG. The recommendations are intended to:

1. Facilitate organizational change through empowered leadership;
2. Foster greater collaboration between intelligence community and fusion center personnel;
3. Link federally-generated intelligence and locally-generated intelligence to the requirements of both communities; and
4. Leverage expertise and vetted resources to streamline a consistent, timely, bi-directional delivery of information between the NCTC and fusion centers.

A. MULTI-LEVEL LEADERSHIP

The author's research has verified that successful organizational change often requires a strategic placement of carefully selected personnel into new leadership positions. If selected internally, the new leaders must be capable of deflecting pressures applied by peers that are in opposition to the required organizational change.[193] If selected externally, they must quickly gain an understanding of the institutional dynamics of the organization they will lead in order to deflect these same pressures. Regardless of internal or external selection, new leaders must earn and sustain organizational buy-in to ensure a successful transition and provide a clear definition of where the organization is intended to go. As stated by Michael Watkins, a prominent business transition expert, "Far too many new leaders…do a poor job of diagnosing their situations and tailoring their strategies accordingly"; which can result in bad decisions leading to organization transition failures.[194]

---

[193] Michael Watkins, *The First 90 Days: Critical Success Strategies for New Leaders at all Levels* (Boston, MA: Harvard Business School Press, 2003), 60–62.

[194] Ibid., 60.

In the world of private enterprise, the ITACG's creation would be considered a hybrid of a "startup" and a "sustaining-success situation." In a start-up, new leaders are "charged with assembling the people, funding, and technology to get a new business, product, or project off the ground;" while in a sustaining-success situation, they are "shouldering responsibility for preserving the vitality of a successful organization and taking it to the next level."[195] Considering the NCTC had been operating with various degrees of success for three years, the creation of the ITACG at the NCTC called for a careful diagnosis to ensure that the Detail's implementation strategy fit the existing organizational and cultural dynamics of both the NCTC and the IC as a whole. For the first time in U.S. history, the ITACG would bring "outsiders" to a functioning IC operation, charged with evaluating and changing existing practices and cultural norms that were deeply institutionalized. Leading such change would not be easy.

Analysis indicates that since the ITACG's inception, advocating for the needs of state and local agencies within the federally dominated NCTC has proven to be challenging. As stated by an experienced law enforcement practitioner, formerly detailed to the ITACG:

> In its current state, the ITACG presents its self as a 'feel-good' organization that allows state and locals the ability to interact with federal information, but does not necessarily provide the organization the appropriate means for true collaboration on solutions that advocate for state and local interest. Much of this is due to the current leadership structure.[196]

This is not due to uncooperative personalities or lack of competence but rather the culture of the institutions these leaders come from.

The ITACG Detail's daily operational leadership consists of a director, who is appointed from DHS and a Deputy Director from FBI; there is no leadership position representing a state/local organization. While both DHS and FBI have worked hard to create strong alliances to support the needs of state and local governments, the current

---

[195] Watkins, *The First 90 Days*, 61–62.

[196] Anonymous source (Seattle Police Department), phone interview with author, Boston, MA, June 8, 2010.

operational model presents a questionable structure to non-federal stakeholders.[197] Expecting the ITACG Detail's federal leadership to "go to battle" against their own agencies in support of the state and local first responder community is an unrealistic expectation, as such actions could result in negative repercussions to their careers. After all, the mere concept of the ITACG was seen as controversial to both DHS and FBI to begin with, as it was forced upon them by Congressional leaders due to both agencies' perceived incompetence. As presented in Chapter III, the roles and responsibilities of ITACG are focused on complementing and supplementing the existing analytic, production, and dissemination efforts by federal entities by:

- Working with federal analysts to create products for SLTP partners,
- Providing SLTP perspective to draft intelligence products,
- Requesting classification downgrades for terrorism-related products suitable for first responders,
- Helping get appropriately classified information to SLTP boots on the ground, and
- Facilitating briefing opportunities for analysts to interact with SLT partners.[198]

One might argue that DHS Office of Intelligence & Analysis was originally charged with performing the duties that the ITACG would now be implemented to perform, and the FBI had been competing with DHS as a result of the Department's creation—through the Homeland Security Act of 2002—taking some of these same responsibilities away from them. As such, one should not expect the leaders of the Detail to push against their home agency in its power struggle while advocating for the ITACG's mission, or lead in a manner that may be seen as competitive or threatening to DHS' or FBI's perceived "territory." The implementation of the ITACG required monumental changes in the way that the IC incorporated state and local public safety interests as it crafted, compartmentalized, and shared intelligence. Thus, the assignment

[197] Anonymous source (Seattle Police Department), phone interview with author, Boston, MA, June 8, 2010.

[198] National Counterterrorism Center, "ITACG Roles and Responsibilities," http://www.nctc.gov/itacg/itacg_roles_and_responsibilities.html (accessed July 16, 2011).

of federal officials to lead the ITACG without a state/local official in an equivalent position left the operation in a disadvantaged position from the beginning.

While the ITACG Advisory Council provides the overall strategic direction for the organization's operation, it presents the only state and local perspective to the Detail's leadership. Fifty percent of the Council's membership consists of organizations that represent state, local, and tribal interests. Furthermore, those formerly assigned to the Detail report that this group is not in touch with the ITACG's daily operation, as they meet semi-annually and function solely as a governance body.[199] Those assigned to the Detail are afforded opportunities to interact with members of the Council, but without a daily presence in the operation, many of the issues the Detail routinely faced went unnoticed.

To improve the ITACG's potential for success and thereby balance leadership decisions with the equities of state and local public safety officials, it is recommended that the Detail's Deputy Director be an appointed state or local official, not a representative of the federal government. This recommendation will provide the necessary degree of expertise and perspective at the executive level to better influence the roles and responsibilities of the Detail's daily operation at the NCTC. Candidates should be selected by the Advisory Council and may include former state homeland security advisors, chiefs, and commissioners from law enforcement and public safety agencies, intelligence and investigative commanders, and fusion center directors. Ultimately, the ITACG Detail's leaders will then include the perspective of an official with significant "local" experience working in community the Detail is intended to represent, while ensuring they have considerable knowledge of the IC, national security policy, and goals/objectives of the Information Sharing Environment. Perhaps most important, unpopular lobbying and decision making against controversial interests of DHS and FBI will be far less risky for those in this position, ensuring that politics do not interfere with what is required to accomplish the ITACG's intended mission objectives.

[199] Quick, interview by author, June 24, 2010.

As another means to advise leadership decisions, those that have served on the ITACG Detail should be provided the opportunity to operate in an advisory capacity to the ITACG Advisory Council upon their deployment back to their home agency. Those that have served on the Detail can provide great insight regarding the opportunities and challenges faced by the Detail in implementing the ITACG mission. While it would be difficult justifying that those formerly assigned to the Detail hold an official position on the Advisory Council, it will prove beneficial for them to serve on a working group that continues to provide insight to members of the Advisory Council to ensure the ITACG's success.

B. OVERHAULING THE DIGITAL BACKBONE OF THE CONTINUUM

Nearly 10 years after 9/11, analysts working at fusion centers are still frustrated by the large number of information-sharing systems connecting the intelligence reporting produced by the Intelligence Community to that of the national network of fusion centers; this issue was corroborated through numerous sources. Efforts to overhaul DHS' Homeland Security Information Network (HSIN) for unclassified report sharing have been slow and arduous. In addition, the deployment of DHS' classified HSDN terminals, while necessary, has proven expensive and risky, while demonstrating various levels of success. Ultimately, more is required to streamline the digital backbone of the required intelligence-sharing continuum.

For matters related to this technological solution, the ITACG is in a valuable, strategic position to implement change due to its knowledge of both communities' requirements. It is, therefore, recommended that the ITACG coordinate with both federal and non-federal homeland security partners to finally reduce the number of existing information-sharing systems and develop a unified platform for sharing information with fusion centers; this will ultimately provide greater efficiency in the reporting of, and access to, terrorism-related information.[200] Furthermore, the ITACG should work with

[200] Eileen R. Larence, "Focus on Fusion Centers: A Progress Report," in *Prepared Testimony Before the Senate Committee on Homeland Security and Governmental Affairs Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration*, 110th Cong., 2nd Sess., http://www.fas.org/irp/congress/2008_hr/fusion.pdf (accessed August 14, 2011), 15.

the IC to develop a robust, consistent, and timely process to deliver information of value to these systems; a similar process should be applied by each fusion center. "Real-time" linkages, as well as consistent procedures and security policies for information sharing, are essential to provide connectivity between those operating within the local communities of the U.S. and the IC.[201] For counterterrorism purposes, the establishment of such a link between fusion centers and the NCTC seems most appropriate. Accordingly, the ITACG should be harnessed to ensure such connectivity and coordination becomes a reality.

The ITACG Detail should lead an initiative to provide classified terrorism-related information to authorized state and local officials through the NCTC Online secret (NOL-S) classified, secure Web-portal. NOL-S has been designed to mirror NCTC Online, which is the top-secret information-sharing system that the NCTC uses to share highly-classified information collected from 28 government networks with federal IC partners operating worldwide.[202] To avoid further duplication of information-sharing systems deployed for state and local use, and, as recommended by those assigned to the Detail, DHS, FBI and NCTC should endorse NOL-S as the primary and central repository for classified terrorism-related intelligence materials intended for state and local consumption.[203] While NOL-S is available through existing DHS, FBI, and DOD secret-level classified information networks, not all fusion centers possess these systems, and, therefore, access to this information is not consistently distributed.[204]

It is recommended that DHS continue working to expedite the delivery of HSDN to all 72 fusion centers to ensure that classified information provided by the ITACG is accessible and properly coordinated with state and local officials. Although it should be noted that the reception of classified information presents a challenge that is greater than just acquiring special equipment, it necessitates strict policy implementation and training

---

[201] Beasley, "The Way Forward with Fusion Centers," 6.

[202] Leiter, "Making Homeland Security Intelligence Work", 10.

[203] Allen, "Making Homeland Security Intelligence Work," 5.

[204] Johnson, "Status of Efforts to Support Increased Capacity." In 2010, HSDN existed in only 33 fusion centers, in May of 2011, there were 52.

on appropriate procedures for the system's use and subsequent information handling. To date, this has been a significant frustration of fusion center personnel, as those with secure terminals and access to HSDN have yet to receive procedural guidance, training for the system's use, or direction on what information exists where within the system and how to access it.[205] Fusion centers have essentially been left on their own to figure this out. One fusion center director recently stated, "This dilemma is like a waiter at a restaurant asking the patrons what they would like to order for dinner, while refusing to show them the menu or explain the 'specials.'"[206] Not only should DHS prioritize the deployment of HSDN, but also training must be provided to ensure that the equipment is used both in accordance with the law and through a means that is most efficient for the center (yet another recommendation corroborated through research). This will provide state and local personnel with the ability to receive and work with classified information at their fusion center, while ensuring that such access does not interfere with active investigations or intelligence collection operations.

Still, however, more must be accomplished to meet the information needs of the majority—those state and local officials *without* secret-level security clearances. Unclassified documents produced by the NCTC are routinely posted to top secret systems.[207] Consequently, this practice renders the products inaccessible by those without a security clearance and, ultimately, "over-classifies" the information. As previously mentioned, unclassified information distribution by the IC has historically been an unorganized process that has resulted in the formation of redundant systems and confusion and frustration by those on the receiving end.

It is recommended that the ITACG coordinate with DHS and FBI on the distribution of all unclassified terrorism-related information to one secure portal: the Homeland Security—State and Local Intelligence Community (HS-SLIC). This will ensure that the information is easily accessible by fusion center personnel for integration

---

[205] Rudy Zupanc, "Northeast Region Breakout Session," (presented at 2011 National Fusion Center Conference, Denver, CO, March 15–17, 2011).

[206] Ibid.

[207] Tim Connolly, interview with author.

into threat and risk assessments, analyses, and for prompt disseminated to appropriate partners. Fusion center directors, via the National Fusion Center Association, have been working to establish policies and procedures to govern a secure and confident exchange of information through this portal.[208] Furthermore, the directors have indicated that they would like this to be *the* primary portal used for these purposes.[209] The author's research has corroborated that incorporating the ITACG's contributions to the Information Sharing Environment via HS-SLIC will further-enable the intelligence-sharing continuum between the federal government and fusion centers (see Figure 14).

Figure 14. ITACG Coordinated Dissemination[210]

[208] Zupanc, "Northeast Region Breakout Session.

[209] Ibid.

[210] Quick, "Production, Dissemination, and Feedback."

The ITACG's federal and non-federal partners should guide and support the Detail in initiatives to overhaul the content and design of NOL-S and HSIN-SLIC to help make certain that both sites work to the likings of federal, state, and local officials. The ITACG should conduct outreach and awareness campaigns to promote the use of these systems, gain feedback for their design, and provide direction in their use. Furthermore, it is recommended that the ITACG work with DHS and FBI to ensure that their headquarters, field offices, and deployed personnel are trained accordingly, abide by new coordination policy, and post relevant products to NOL-S and HS-SLIC accordingly, thus ensuring consistency and preventing information "stove piping" within disparate systems. The ITACG should continue to work with state and local officials to gain an even greater understanding of their individual intelligence requirements and experiences working with federal agencies to ensure that the organization's efforts to overhaul the digital backbone of the continuum will fulfill the needs of the community that they are advocating for.[211]

C. ENHANCING HUMAN CAPITAL: PHASE 2, POST-DETAIL DEPLOYMENT

From a strategic perspective, our government has failed to sustain the expertise gained by those that complete their ITACG detail at the NCTC. Research indicates that the current model sends those that have completed their assignment at the ITACG Detail back to their home agency without agreements for future roles and responsibilities that include them in national security positions.[212] While assigned to the Detail, state and local officials are engaged in an environment that raises their knowledge of national security policies and procedures and provides first-hand experience in the U.S. government's international counterterrorism operations. This experience should be leveraged to improve local coordination of counterterrorism efforts and, ultimately, to increase the national security human capital at fusion centers.

---

[211] Program Manger, Information Sharing Environment, *Establishing the Interagency Threat Assessment and Coordination Group: Report for the Congress of the United States* (Washington, D.C.: 2008), 8–11.

[212] Quick, interview by author, June 24, 2010.

As "Phase 2" of the ITACG's deployment, it is recommended that upon completion of individuals' one-year assignments to the NCTC, they return to the home agency as a local representative of the ITACG and a liaison to the NCTC. During their Phase 2 deployment, local ITACG representatives should serve as both terrorism and Intelligence Community subject-matter experts, which will prove to be an invaluable resource to fusion centers, considering that most centers are lead and staffed by state and local officials with limited exposure to the IC. The local ITACG representatives will be strategically prepared to drive collection efforts, train intelligence liaison officers, and advocate for the information needs of both the IC and the local public safety community.

As of May 2011, 73 intelligence officers from DHS have been deployed to fusion centers to support their respective missions.[213] One of their main assignments is drafting Homeland Information Reports (HIRs), which are based on information derived locally that supports DHS' intelligence collection requirements. HIRs are most frequently generated from patterns of criminal activity identified in police reports, intelligence cases and investigations. Concurrently, FBI analysts working in the local field office's Field Intelligence Groups (FIGs) are tasked with analyzing and reporting on their "domain," or area of responsibility according to both jurisdiction and threat analysis, to drive intelligence collection and support active investigations. Presently, little coordination occurs between DHS and FBI personnel while they report on their respective agency's intelligence requirements, which are, more often than not, interrelated.

To remedy this issue, it is recommended that local ITACG representatives are tasked to work in close collaboration with both DHS and FBI personnel to ensure that information collected domestically that meets national security requirements is identified, articulated, and coordinated between both agencies *and the fusion center* and, ultimately, the ITACG Detail. Collaboration with the local FBI field office is a strict requirement, as this will ensure that sensitive investigative case information is not improperly released. Using consistently applied protocols, information should be delivered to the ITACG for further integration with IC reporting; hence, harnessing the ITACG to *push information*

[213] Johnson, "Status of Efforts to Support Increased Capacity."

to the IC, instead of just to pull information from it. Local ITACG representatives should leverage NOL-S via the fusion center's HSDN system and HS-SLIC to move locally generated information of relevance to the attention of the ITACG, which, in turn, can correlate the information with locally-generated information from other fusion centers and inform the NCTC of patterns and trends in local activity (see Figure 15). This positive organizational change to a bi-directional give-and-take methodology—rather than the existing one-way take methodology—will help the IC better understand the value of the state and local community in support of global counterterrorism efforts and, eventually, lead to greater collaboration.

Figure 15. ITACG Local Collection and IC Integration Model[214]

[214] Quick, "Production, Dissemination, and Feedback."

1. Extending Joint-Duty: Integrating Elements from Both Sides of the Continuum to Enhance Knowledge, Skills and Abilities

Leaders within the IC tend to be skilled in their respective fields of expertise; however, their ability to provide the best solutions is often blocked by the boundaries of their institutional culture and prerogatives.[215] Senior IC leaders require a broad, enterprise-wide focus that provides a deep understanding of how each agency and element of the IC contributes to the overall counterterrorism mission.[216] In an effort to promote better teamwork among IC agencies and to develop leaders with the ability to integrate all of the IC assets to accomplish this mission, the Joint Duty Program was passed into law fulfilling one of the key elements of the 2004 IRTPA. In short, Joint Duty requires intelligence officials to spend time working at another intelligence agency before they can be considered for senior-level promotions, providing leadership with knowledge and experience outside the institutional boundaries of their home agency.[217] According to former DNI Dennis Blair, "When the next generation of intelligence leaders moves into the top jobs, their experience will make them better joint leaders….They will instinctively pool their skills and capabilities."[218]

Joint Duty is currently limited to the Intelligence Community's personnel; meanwhile, the national network of fusion centers has emerged, requiring consistent interaction with several elements of the IC. Fusion center personnel have begun short term "joint duty" engagements of their own to learn about the operations of other fusion centers and share best practices and experiences; this has been administered through the DOJ/DHS *Fusion Center Exchange Program.* The author's research has corroborated that this program has become a highly sought after as a rich learning experience for front-line personnel and executives alike. Unfortunately, few programs are available allowing

---

[215] Dennis Blair, "Luncheon Keynote Address" (presented to State of Intelligence Reform Conference, Bipartisan Policy Center, Washington, D.C., April 6, 2010), http://www.bipartisanpolicy.org/news/multimedia/2010/04/07/videos-447 (accessed August 14, 2011).

[216] Mike McConnell, "Intelligence Community Civilian Joint Duty Program Implementing Instructions," in *Intelligence Community Policy Guidance Number 601.01* (Washington, D.C.: Office of the Director of National Intelligence, 2007).

[217] *Intelligence Reform and Terrorism Prevention Act of 2004.*

[218] Blair, "Luncheon Keynote Address."

such an exchange between fusion center and IC personnel. While fusion centers may never be considered a node of the IC, their relevance in regards to the U.S. national security mission and the Information Sharing Environment, demands a seamless, coordinated partnership with the IC. Thus, consideration should be given to the inclusion of fusion center personnel in the IC's Joint Duty Program (see Figure 16). The ITACG's creation may be considered a positive step forward in seeing that this becomes a reality, as it currently facilitates a similar role.

Figure 16. Intelligence Community with SLTT Joint Duty Participation[219]

Research has verified the need for training and education within the IC to raise awareness of the counterterrorism operations developing within state and local governments and to determine how the IC and fusion centers can augment each other's mission requirements. The ITACG's creation was intended to help IC personnel think differently when conducting analysis and writing products, mostly due to the IC's historic inability to write intelligence to a state and local audience. IC agencies have traditionally written intelligence at the highest classification level; there has never existed a requirement or incentive to write at the Unclassified-level.[220] ITACG personnel have worked closely with federal analysts assigned to the Detail to cross-train and augment their writing styles and educate on what information is of most value to the local public

[219] Graphic adapted from Pile, "Overview of the Office of the Director of National Intelligence."

[220] Quick, interview with author, June 24, 2010.

safety community. To help promote this level of cross training beyond the Detail, and to begin promoting a greater awareness of fusion centers, the ITACG should develop a training program for personnel at IC training academies. The training program should focus on the relationship between the operations of state and local law enforcement and public safety officials and that of the IC. Significant emphasis should be applied toward writing intelligence products at multiple tiers of classification and to the needs of various stakeholders to ensure that elements of their intelligence reporting can reach the local audience. Additionally, participants should be educated on the operations of fusion centers, their capabilities and limitations, and how they fit into their counterterrorism mission.

IC analysts with relevant national security responsibilities should rotate in and out of both the ITACG Detail and fusion centers as part of the IC's joint duty program. This should be an element for consideration in an IC analyst's career track and an additional reinforcement for one's promotion. The experience gained will provide IC personnel opportunities to learn the requirements of state and local officials by actively participating in a fusion center operation. Ultimately, this provides an environment where both state and local officials and IC personnel can learn tradecraft from each other that is beneficial to the broad range of national security requirements.

5. Joint Duty Case Study: Boston ODNI RASER Team

In 2007 and 2008, ODNI deployed small groups of IC personnel on joint duty training assignments at various national security and law enforcement organizations as part of its Rapid Analytic Support and Expeditionary Response program (known as "RASER Teams"). According to the ODNI, "RASER [was] a program to create multidisciplinary teams of Intelligence Community (IC) analysts trained and equipped with the leadership skills, analytic tools, tradecraft, and mission processes to meet complex analytic challenges. The teams test innovative analytic training, tools, and tradecraft that can be applied to improve and bolster existing processes and tools."[221]

[221] Office of the Deputy Director of National Intelligence for Analysis, *Analytic Transformation: Unleashing the Potential of a Community of Analysts* (Washington, D.C.: Office of the Director of National Intelligence, 2008), 14.

The RASER program was an experiment to test a hypothesis that special joint training and development can compress the learning that normally requires many years for analysts to accomplish via traditional training and assignments into a single year.[222] The Boston Regional Intelligence Center (BRIC), the Metro-Boston Region's fusion center, was one of the locations in which teams were deployed. From a fusion center perspective, this program provided a positive experience for IC and fusion center personnel alike: 1.) It offered an opportunity for cross-discipline training that was otherwise absent from fusion center operations, and otherwise unavailable to fusion center personnel. The RASER Team provided personnel training in intelligence analysis and collection tradecraft; intelligence cycle implementation and procedural guidance; and worked hand-in-hand with fusion center analysts assessing emerging threats and producing intelligence on risks within the BRIC's area of responsibility.[223] 2.) In return, the IC personnel from the RASER Team were afforded an opportunity to assist a non-Federal, criminal intelligence and investigative operation; they experienced firsthand how the information collected by the IC applies to fusion center operations and helps to inform state and local government risk mitigation strategies; and they learned how a lack of coordination amongst IC agencies interacting with fusion centers can negatively affect analyses and investigations.[224]

The extension of the Joint Duty Program should provide inter-agency exchange opportunities for both IC and fusion center personnel alike. It is recommended that fellowship opportunities become available for fusion center personnel to work not only at the ITACG, but also within agencies of the IC to gain a broader perspective of international counterterrorism operations. The fellowships model should allow time for analytic tradecraft development, education, and collaboration on projects that enhance both communities' understanding of each other's mission requirements. This will expose fusion center personnel to new analytic methodologies and subject matter, making them stronger analysts upon their return to the fusion center.

---

[222] Office of the Deputy Director, *Analytic Transformation*, 14.

[223] Experience of author.

[224] Experience of author.

In 2008, the Ash Institute for Democratic Governance and Innovation at the Harvard Kennedy School selected the IC's Joint Duty Program as a winner of the 2008 Innovations in American Government Awards. The program was recognized for promoting cross collaboration and knowledge transfer across the entire Intelligence Community. As one of six winners, the program received $100,000 toward dissemination and replication across the country.[225] Opportunities such this should be leveraged to supplement the funding required to extend this program to fusion centers. Furthermore, the Technical Assistance Program offered through DHS and DOJ may provide an additional resource for sponsorship, providing the financial and logistical assistance needed to execute this recommendation.

Implementation of this recommendation may resolve a significant issue that has obstructed the ITACG's ability to succeed, as fusion center personnel deployed to the IC through the Joint Duty Program will serve as force-multipliers to the ITACG Detail. Where the Detail has been limited is size and reach, fusion center personnel participating in joint duty will mitigate this issue by extending elements of the ITACG's operation deeper into the IC, while providing a unique, local analytical perspective. Moreover, the knowledge and experience gained through this infusion of local personnel into the IC will subsequently contribute additional, qualified personnel to fulfill the responsibilities of the recommended ITACG Phase 2 deployments at fusion centers. Ultimately, a sustainable cycle of subject-matter expertise will emerge and proliferate the intelligence-sharing continuum (see Figure 17).

[225] "Intelligence Community Civilian Joint Duty Program Honored as Innovations in American Government Award Winner," Office of the Director of National Intelligence Public Affairs Office, September 9, 2008, www.dni.gov/press_releases/20080910_release.pdf (accessed April 15, 2011).

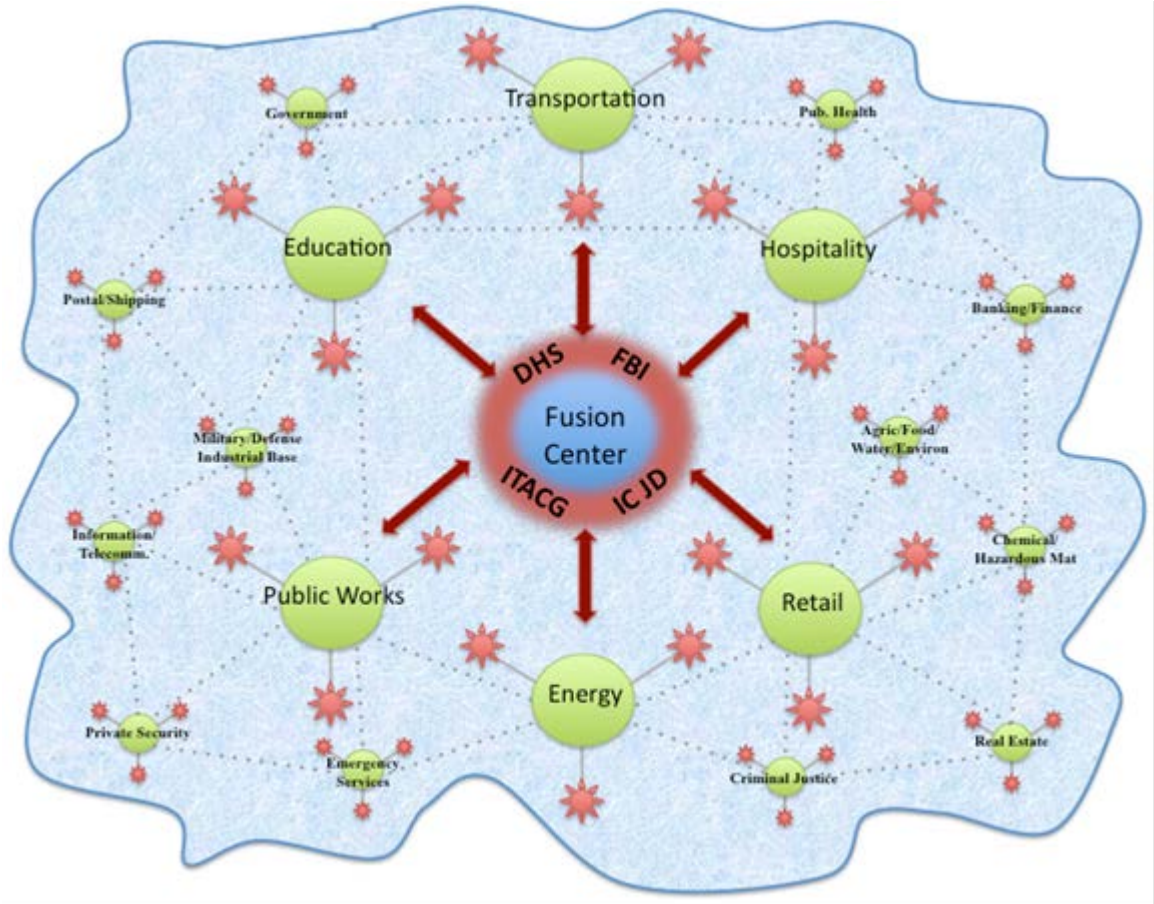


Figure 17. Public Safety Megacommunity with Enhanced Fusion Center[226]

D. CONCLUSION

Nearly 10 years after 9/11, the federal government still requires a more effective means to ensure that terrorism-related information generated globally is analyzed and shared with the National Network of Fusion Centers and the local public safety communities they serve in order to assist in the formulation of risk mitigation strategies. Furthermore, better inter-agency coordination is required between DHS' and FBI's domestic operations to reduce duplicative efforts and foster collaborative relationships; and more efficient protocols are required to streamline the flow of locally generated intelligence, collected at fusion centers, with members of the IC. Triangulating the

226 "Enhanced Fusion Center" includes greater federal agency coordination via ITACG Post-Detail Deployment, Intelligence Community Joint Duty Detailee, DHS I&A, and FBI FIG.

results of several research methodologies corroborated these requirements. Furthermore, through the application of this research methodology, the author has provided the following recommendations to promote the required intelligence-sharing continuum by harnessing the ITACG:

- Recommendation: Appoint a state or local government representative to the position of Deputy Director of the ITACG Detail.
- Outcome: Provide a representative leadership structure and thereby ensure that politics related to DHS and FBI do not interfere with what is required to accomplish the ITACG's intended mission objectives.
- Recommendation: Recruit those that previously served on the ITACG Detail to serve and report in an advisory capacity to the ITACG Advisory Council.
- Outcome: Provide greater insight regarding the frequent challenges and opportunities for the Detail's operation.
- Recommendation: Leverage the experiences, perspectives and mission of the ITACG to reduce, overhaul, and streamline the existing electronic systems used to share classified and unclassified information with state and local partners.
- Outcome: Consistent, reliable, and faster access to relevant federally-generated intelligence.
- Recommendation: Expedite the delivery of DHS' Homeland Security Data Network to all 72 fusion centers and provide training to *all* system users on site contents, portal navigation, and appropriate use procedures.
- Outcomes:
    - Establish capability to receive secret-level classified intelligence consistently at all fusion centers;
    - Support effective use of classified systems by state and local intelligence practitioners; and
    - Provide reliable, faster access to relevant classified federal intelligence.
- Recommendation: Continue working towards a greater frequency of tear line, unclassified intelligence reporting.
- Outcomes:
    - Provide a consistent, timely, actionable stream of intelligence to state and local law enforcement and public safety officials; and

    - Ensure current trends related to terrorist activity remain relative to the first responder community.

- Recommendation: Implement a "Phase 2" ITACG Detail deployment strategy to institutionalize specific Detail operational requirements at fusion centers.

- Outcomes:

    - Appropriately coordinate locally derived information with fusion center personnel, locally deployed DHS assets, and FBI field offices;

    - Establish local counterterrorism and IC experts and liaisons to the NCTC; and

    - Facilitate the delivery of relative fusion center generated intelligence to the Intelligence Community via the ITACG Detail and the NCTC.

- Recommendation: Institute processes and procedures that harness the ITACG Detail to better coordinate to reception of fusion center generated intelligence at the NCTC.

- Outcome: Provide a means to facilitate the collection, collation, and analysis of locally-derived intelligence, in coordination with the NCTC, to identify regional, national, and international patterns of emerging activity.

- Recommendation: Expand the Intelligence Community's Civilian Joint Duty Program to fusion centers.

- Outcomes:

    - Promote short-term detail opportunities for IC professionals at fusion centers;

    - Provide short-term detail opportunities for fusion center personnel at IC agencies;

    - Develop cross-disciplinary and cross-governmental training; and

    - Improve IC knowledge of fusion center requirements and fusion center awareness of IC requirements.

The desired continuum requires support from the top levels of leadership capable of defying boundaries created by Cold War mentalities and organizational culture. Our nation's 72 fusion centers are at a loss without the aid of a national intelligence support structure capable of providing timely and actionable terrorism-related intelligence that includes the IC's international perspective. However, the mere delivery of generic intelligence is not enough. Similar to the model presented in Chapter VII, the Federal

government must harness the requirements of its newest stakeholders—the National Network of Fusion Centers—through greater interaction and collaboration. The ITACG is in a unique position to provide expertise and continue coordination efforts beyond the confines of the NCTC, extending their services to fusion centers. Leveraging technology as a means to facilitate intelligence-sharing, and personnel from the ITACG Detail to provide the voice of state and local officials, the desired intelligence-sharing continuum will emerge, capable of facilitating the flow of timely, actionable intelligence with all parties participating in counter terrorism endeavors (see Figure 18).

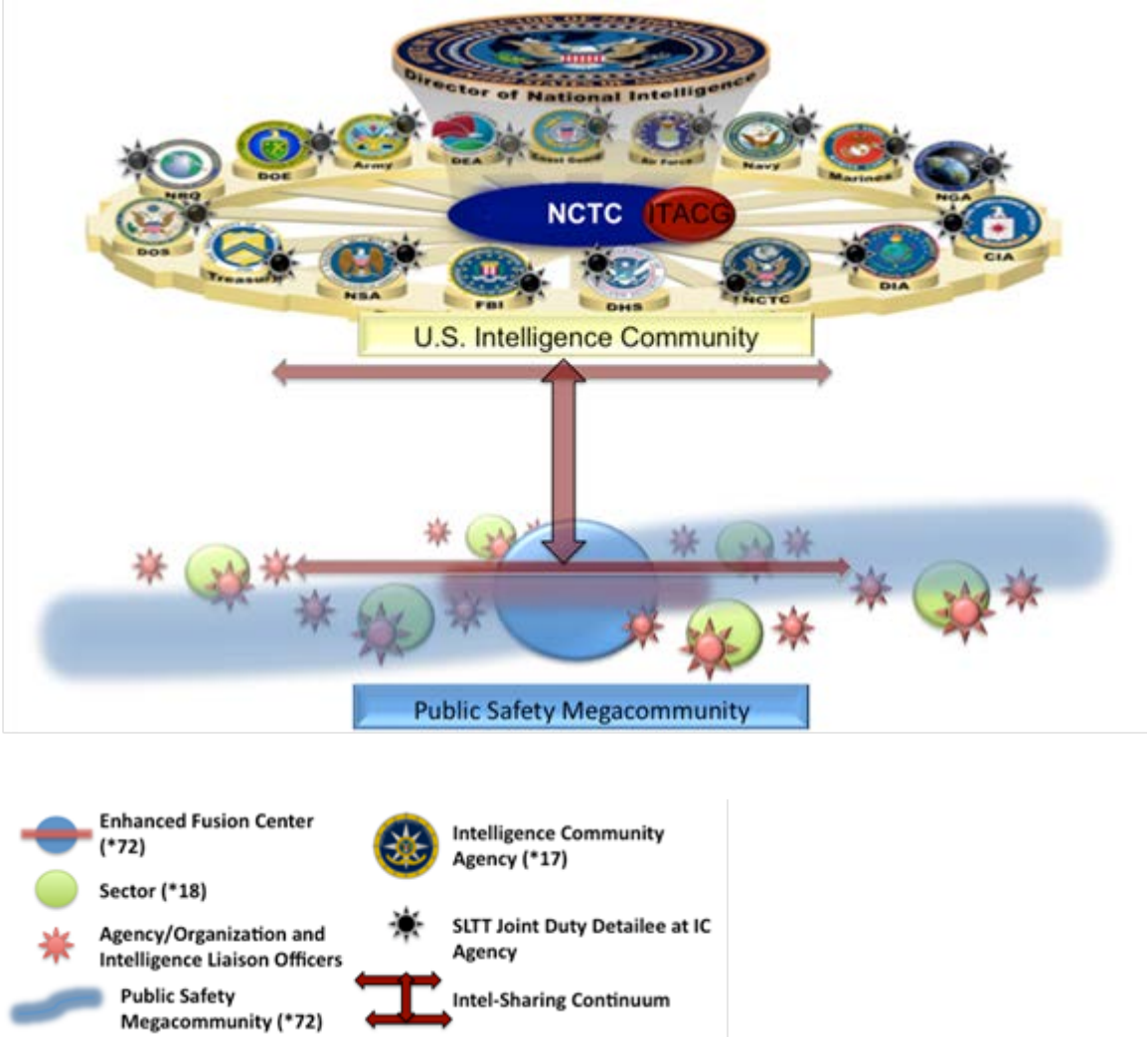


Figure 18. Recommended Model with Intelligence-Sharing Continuum[227]

[227] Intelligence Community graphic adapted from Pile, "Overview of the Office of the Director of National Intelligence."

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX DELPHI PANEL

A. DELPHI PANEL: QUESTIONNAIRE 1 FEBRUARY 13, 2008

For the questions below, list as many factors as you feel necessary, providing a brief explanation of the importance of each factor. Your insights regarding "best practices" and/or negative factors will be important to this survey.

1. To the best of your knowledge, are most intelligence and information consumers[228] satisfied with the current standard of products and services provided by state and local fusion centers? Why or Why Not?
2. List the major factors that are affecting information and intelligence production at fusion centers *(e.g., leadership, collaboration, subject matter expertise, human capital, relevance of analysis).*
3. List significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and service *(e.g., Is the intelligence received making a difference? Your intelligence requirements, feedback, success stories.).*
4. List the major factors that currently affect information flow between:
   a. The Federal Intelligence Community and fusion centers
   b. Domestic information/intelligence collectors[229] and fusion centers
   c. Fusion centers and the consumers of fusion center-generated products and services

   (e.g., Who do you think is in charge of domestic intelligence? Is the intelligence making it to the street? Classification of information, effectiveness of "write for release" practices, classification network domains; need for HSINT doctrine, definitions of HSINT).
5. List significant factors, practices, and/or processes that would positively influence the flow of information between:
   a. The Federal Intelligence Community and fusion centers
   b. Domestic information/intelligence collectors and fusion centers
   c. Fusion centers and the consumers of fusion center-generated products and services

---

[228] **Information/Intelligence Consumers:** Federal, state, local, tribal, private, and public sector policy makers, managers, agencies and organizations that are supported by the analysis, products and services provided by state and local fusion centers.

[229] **Domestic Information/Intelligence Collectors:** Individuals employed by state, municipal and tribal law enforcement agencies; private security agencies; non-traditional intelligence collection agencies such as fire and EMS, municipal and state code inspection agencies, transportation agencies, public health and public service agencies; business organizations; and the public.

(e.g., unify the federal HSINT product through one agency or group, increase constructive dialogue with federal intelligence providers, ensure state/local fusion center intelligence is provided to federal stakeholders, success stories).

6. Any other factors you care to address:

B. DELPHI PANEL: SUMMARY OF RESPONSES PROVIDED FOR QUESTIONNAIRE 1 MARCH 16, 2008

1. To the best of your knowledge, are most intelligence and information consumers satisfied with the current standard of products and services provided by state and local fusion centers? Why or Why Not?

15 respondents stated that consumers are not satisfied:

- Lack of analysis and value added in products (substandard products)
  - Low value added affects consumer views of SLFC
  - Too much cutting and pasting
  - Circular reporting
  - Publishing products to show they are doing something
  - Most of what is disseminated can be found in the news/media
  - Information not properly sourced
  - Receiving one-size-fits-all products
- Not meeting consumer requirements
  - Consumers are not defining requirements
  - Lack requisite info, Intel, sources to meet consumers' needs
- Information delivery lacks timeliness
  - Ad hoc delivery/dissemination chains
- Consumers don't know how to interpret the products
- Little private sector participation
- Fusion centers are not identifying priorities and developing collection plans
  - Lack of planning in development of SLFCs
- Producers are still developing necessary skills and processes for production
- LE sensitive reports are not reaching non-LE partners
- Disconnect between IC and LE communities

- Consumers not aware of what SLFCs can provide
- SLFCs still trying to figure out their roles

5 stated that consumers are satisfied:

- However, consumers would like to see more products with local relevance
- However, consumers would like to see increased efforts for collocation to increase participation
- Agencies happy to be assisting SLFCs on terrorism related issues

2 stated that they were not sure why.

2. List the major factors that are affecting information and intelligence production at fusion centers.

Lack of subject matter expertise:

- Lack of human capital in analysts
    - Can't retain the highly trained
- Lack of experience
- Lack of analytic experience
- Over-tasking w/ different assignments and roles leads to jack of all trades, rather than an expert in a particular area
- Lack of analytic training and skill development

Lack of leadership/leadership issues:

- Lack of knowledge re: Intelligence
- Lack of understanding regarding the value of analysis
- Lack modern organizational vision
- Lack leadership training
- Lack of political commitment help build and sustain FCs
- Ineffective leadership

Shortage in personnel depth:

- Can't hire enough personnel to meet expectations/demands
- Staffing restraints
- Inadequate funding

Problems with Collaboration:

- Turf wars
- Issues with co-location
- Lack of partnerships through personal contact
- Lack of sharing of resources, personnel, decision making, accountability

Tactical vs. Strategic analysis emphasis:

- Lack of strategic focus
- Conflicting intelligence focus areas
- Operational support has overtaken strategic analysis

Problems w/ technology:

- Database capabilities
- Information sharing capabilities
- Lack of tools

Lack of information sharing:

- Within State and amongst state, local, and federal partners
- *Classified materials*
    - Lack of knowledge regarding how to handle classified materials
    - Lack of declassification—too much over-classification
    - Affecting joint-production

3. List significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.

Leadership must:

- Develop strong, active, lasting relationships with partner agencies from all levels of government, as well as the private and public sectors.
- Clearly articulate to consumers the capacity of the fusion center and ensure that consumer expectations do not exceed the fusion center's capabilities.
- Partake in greater marketing and outreach programs by publicizing their mission, and sharing success stories and best practices.
- Set strategic priorities, planning and direction, and ensure that all processes and practices are in accordance with the intelligence cycle.

- Obtain a greater balance between tactical and strategic product development/priorities, etc.
- Collaborate nationally to develop baseline capabilities for fusion centers (operational standards).

Intelligence Requirements—Fusion Centers must:

- Set clear, concise intelligence requirements, and develop effective means' of adjusting requirements according to their evolving needs.
- Fusion centers must focus collection priorities according to the intelligence requirements of their consumers.
- Develop better product/service evaluation and feedback mechanisms must be developed so that fusion center product development can stay on point with the evolving needs of consumers.

Training and Education:

- Fusion centers must develop career intelligence professionals.
- Personnel must be properly trained and educated, and given the time to gain experience and develop greater analytic skill.
- Leadership must be properly trained, strategically focused, and experienced with the intelligence profession.

Miscellaneous:

- Fusion centers must enhance partnerships and outreach capabilities through community, interagency, and sector-specific liaison officer programs.
- Fusion center personnel need access to timely and relevant unclassified information from the IC that can be applied to their analysis and products.
- Fusion centers need better technology to help facilitate collection, analysis, dissemination, and knowledge management.

4. List the major factors that currently affect information flow between the Federal Intelligence Community and fusion centers; domestic information/intelligence collectors and fusion centers; and fusion centers and the consumers of fusion center-generated products and services.

Information Classification:

- Information is being over-classified.
- Affects ability of analysts to use information provided by feds.
- Access to classified materials is useless—information cannot be shared with front line personnel.

- Challenges accessing classified systems (fusion centers).
- Issues with the laws and policies that regulate the handling and dissemination of SBU information.

Trust/Collaboration:

- Lack of trust has led to insufficient collaboration between the IC and fusion centers.
- Fusion centers are not comprehensively included in the national intelligence system.
- Lack of collaboration between DHS and FBI creates an obstacle for information flow.
- A competitive atmosphere, territoriality, and interagency rivalries are inhibiting information sharing between agencies and fusion centers.
- No clear model for how disparate agencies can work together collaboratively on intelligence operational endeavors.
- Absence of routine meetings between fusion center leadership and consumers for strategic planning; to enhanced relationships and collaboration.
- The private and public sectors are not adequately engaged in fusion center efforts.

Information Network Efficacy:

- Too many information-sharing networks at the national/federal level.
- Absence of standardized, formal reporting mechanisms for the timely exchange of information between the IC and fusion centers.
- Insufficient technology for knowledge management and the sharing of data, information, and intelligence.

Intelligence Requirements:

- Strategic priorities at fusion centers are not adequately focused, leading to collection efforts that are dissimilar to consumer requirements.
- Limited outreach and marketing of fusion center intelligence requirements and production capabilities.
- Lack of focused, efficient collection efforts at the state and local level
- Fusion centers have not identified and shared their intelligence requirements with the IC.

Miscellaneous:

- Products created at the federal level lack relevance to state and local needs.
- There is a lack of education, training, and experience with intelligence outside the federal echelon.
- Unclear as to who is leading fusion center and domestic intelligence endeavors.
- Limited personnel available at fusion centers to provide outreach and marketing of priorities and capabilities.
- Inadequate feedback and follow-up mechanisms to identify the usefulness of information provided to fusion centers.

5. List significant factors, practices, and/or processes that would positively influence the flow of information between the Federal Intelligence Community and fusion centers; domestic information/intelligence collectors and fusion centers; and fusion centers and the consumers of fusion center-generated products and services.

Create National Strategy for Fusion Centers:

- Create a national strategy for fusion centers that articulates their role and position amongst law enforcement and intelligence agencies at all levels of government.
- Define the role of DHS representatives within the fusion centers, and then identify how this role, as well as fusion center access to classified material, is an asset beyond the confines of the fusion center.
- The federal government must provide a clear vision of how fusion centers fit into the intelligence community, and then fund it accordingly.
- Implement policy change and promote cultural change that facilitates and encourages information sharing across all agencies, disciplines, and sectors.

Focus on Intelligence Requirements:

- Fusion centers must articulate clear, concise, relevant intelligence requirements, and the IC must meet those requirements with products tailored to meet their needs.
- Prioritize intelligence requirements and lead strategically focused collection efforts that meet the needs of consumers; limit general requirements
- Fusion center consumers must articulate clear, concise, relevant intelligence requirements.

Enhance Collaboration:

- Unification in the messages sent from the IC to fusion centers.
- DHS and FBI (as well as other agencies) must collaborate on join-products to close gaps and provide "one federal voice".
- Stronger partnerships, collaborations, and trust amongst IC and fusion center agencies; no more "us" vs. "them."
- Develop stronger interagency relationships through greater partnerships, collaborations, trust, and the ability to collocate to establish personal contact.
- Implement more liaison officer programs to facilitate communication and collaboration amongst agencies, disciplines, and sectors.

Fusion Center Management and Marketing:

- Develop efficient feedback and follow-up mechanisms to identify the usefulness of information provided to both fusion centers and consumers.
- Share success stories and best practices to build trust and confidence.
- Greater outreach and marketing of fusion center mission, intelligence requirements; explain what the fusion center does, capabilities, limitations, and what the consumer can provide the fusion center.
- Establish standardized, formal reporting mechanisms and dissemination protocols for the timely, efficient exchange of information between fusion centers, agencies, and front line personnel.

Enhance and Streamline Information Systems/Networks:

- Consolidate the federal information sharing systems and create a single location for gathering federal information and posting RFIs, IIRs, etc.
- Better technology for information sharing: systems/portals where data, crime bulletins, IIRs, RFIs, etc. can be posted and shared with all partner agencies within a state or region
- Standardize the technology so that systems can be interlinked to facilitate exchange nationally.

Prioritize Training and Education:

- Proper training amongst federal, state, and local agencies regarding each agencies mission space, how to work together more effectively, and the relevance of certain topics at each level of government.
- Train and educate fusion center personnel in leadership and intelligence matters.

Fix Information Classification Issues:

- More de-classification, write-for-release, and tear line reporting that information can be shared beyond the fusion center.
- Create standards for "Sensitive but Unclassified" information so that it can be easily shared, yet adequately protected.

C. DELPHI PANEL: QUESTIONNAIRE 2 MARCH 27, 2008

NPS Intelligence Delphi Panel: Questionnaire #2

1. NPS Intelligence Delphi Panel: Questionnaire #2

This is the second Delphi questionnaire aimed at exploring and assessing the principle strengths and weaknesses of the current intelligence production and sharing practices that are in place between the Federal Intelligence Community, fusion centers, and the consumers of fusion center-generated intelligence. As you will see, this questionnaire is based on the responses obtained from the first questionnaire.

In this Delphi questionnaire, participants are asked to do three things in each question:

1. Review all items on the questionnaire and comment on any items you wish. Feel free to ask questions, make clarifications, argue in favor of or against items. Brevity and clarity will facilitate my analysis.

2. Select the items you feel are most important. Depending on the total number of items listed in each question, use the following logic to rank-order the items: Assign a value of "10" to the most important item. Assign a value of "9" to the next most important, and so on, until the item you feel is comparatively the least important is assigned a value of "1".

3. Complete this survey by April 11, 2008.

Each of the following questions relates to the six questions presented in Questionnaire #1; additionally, the items that you will find listed for commenting and ranking represent the most common themes identified by the panelists in their answers to questions 1-6 in the first questionnaire.

Thank you very much for your participation in this study; your insight is very much appreciated.

2. Consumer Satisfaction

The first question in Questionnaire #1 asked panelists if they believed most intelligence and information consumers were satisfied with the current standard of products and services provided by state and local fusion centers (Why or Why Not?).

68% of the panelists stated that consumers are NOT satisfied with the products and services provided by state and local fusion centers; 23% of the panelists stated that most consumers are satisfied, while 9% were unsure of consumer satisfaction.

Below are the most common themes identified in the answers of the panelists. Please rank-order the six most important items as you perceive them at this time (assign a value of "6" to the most important, "5" to the next most important, and so on until least important item is assigned a value of "1"). If you wish to add comments expressing agreement, disagreement, or clarification concerning the items, please do so in the space provided below.

***1. Please review each of the following items identified in Questionnaire #1 as important factors that are affecting fusion center consumer satisfaction.**

	Least Important 1	2	3	4	5	Most Important 6
Fusion centers are still attempting to determine their role and develop the skills necessary to satisfy their consumers.	○	○	○	○	○	○
Consumers do not know how to interpret the products, rendering them useless or counterproductive.	○	○	○	○	○	○
Consumers are unaware of the products, services, and benefits fusion centers can provide.	○	○	○	○	○	○
The private sector is not adequately represented or included in the fusion center processes or consumer group.	○	○	○	○	○	○
Both consumers and fusion centers are failing to identify their intelligence requirements/priorities/needs.	○	○	○	○	○	○
Fusion centers are disseminating products that lack analysis, value, relevance, and timeliness; the information disseminated can usually be found in the media, and is often a contribution to the routine "circular reporting".	○	○	○	○	○	○

3. Fusion Center Productivity

The second and third questions in Questionnaire #1 asked panelists to:
- List the major factors that are affecting information and intelligence production at fusion centers; and,
- List significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.

Below are the most common themes identified in the answers of the panelists. For Question #2, please rank-order the eight most important items as you perceive them at this time (assign a value of "8" to the most important, "7" to the next most important, and so on until the least important item is assigned a value of "1"). For Question #3, please rank-order the ten most important items following the same logic. If you wish to add comments expressing agreement, disagreement, or clarification concerning the items, please do so in the space provided below.

***2. Please review each of the following items identified in Questionnaire #1 as important factors that are affecting information and intelligence production at fusion centers.**

	Least Important 1	2	3	4	5	6	7	Most Important 8
Fusion center personnel lack the necessary subject-matter expertise required to provide relevance and quality analysis to their products and services; more training and education in intelligence, analysis, information technology, and other essential skills is necessary.	○	○	○	○	○	○	○	○
There has been an absence of political support and funding to build and sustain fusion centers that can operate at the necessary capacity; as a result, they are suffering from a shortage of personnel and resources, making it difficult to meet expectations and demands.	○	○	○	○	○	○	○	○
Information sharing deficiencies exist between the federal government and fusion centers.	○	○	○	○	○	○	○	○
Information/intelligence "classification" is affecting the quality, quantity, and timeliness of information that can be released to fusion center consumers; information provided from federal agencies is often over-classified, and there is a shortage of tear line and "write-for-release" reports available for product development and dissemination.	○	○	○	○	○	○	○	○
Fusion centers lack a strategic focus; too much effort has been placed on tactical and operational support, rather than strategic analysis.	○	○	○	○	○	○	○	○
Fusion center leadership has been ineffective.	○	○	○	○	○	○	○	○
Fusion centers lack adequate technological solutions to aid analysis, access relevant databases, and facilitate information sharing and product delivery.	○	○	○	○	○	○	○	○
Fusion Centers have struggled to reach an adequate collaborative capacity; there have been issues with collocation, partnerships, and the sharing of personnel, resources, decision-making, and accountability.	○	○	○	○	○	○	○	○

***3. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.**

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10
Fusion center personnel need access to timely and relevant unclassified information from the Federal Intelligence Community that can be applied to their products and analysis.	○	○	○	○	○	○	○	○	○	○
Fusion center leadership must participate in greater marketing and outreach programs by publicizing their mission, success stories, and best practices; furthermore, leadership must develop strong, active, lasting relationships with agencies from all disciplines, levels of government, and the private and public sectors.	○	○	○	○	○	○	○	○	○	○
Fusion centers need better technology to help facilitate collection, analysis, dissemination, and knowledge management.	○	○	○	○	○	○	○	○	○	○
Leadership must clearly articulate to consumers the capacity of the fusion center, and ensure that consumer expectations do not exceed the fusion center's capabilities.	○	○	○	○	○	○	○	○	○	○
Fusion center leadership must work with individual consumers to set clear, concise intelligence requirements, and develop an effective means of adjusting requirements according to their evolving needs.	○	○	○	○	○	○	○	○	○	○
Fusion centers must enhance partnerships, collaborations, outreach, and reach-back capabilities through the implementation of community, interagency, and sector-specific liaison officer programs.	○	○	○	○	○	○	○	○	○	○
Fusion centers must develop better evaluation, feedback, and follow-mechanisms to identify the usefulness of information provided to and from consumers.	○	○	○	○	○	○	○	○	○	○
Fusion center leadership must be properly trained, strategically focused, and experienced with the intelligence profession; set and regulate strategic priorities, planning and direction; focus collection efforts according to consumer requirements; ensure that all processes and practices conform to the intelligence cycle.	○	○	○	○	○	○	○	○	○	○
Fusion centers must develop career intelligence professionals; personnel must be properly trained and educated, and given the time to gain experience and develop greater analytic skill.	○	○	○	○	○	○	○	○	○	○
Fusion centers must obtain a greater balance between tactical and strategic product development and operational priorities.	○	○	○	○	○	○	○	○	○	○

4. Information/Intelligence Sharing Deficiencies

The fourth question in Questionnaire #1 asked panelists to list the major factors that currently affect information flow between:
(a) The Federal Intelligence Community and fusion centers;
(b) Domestic information/intelligence collectors and fusion centers; and,
(c) Fusion centers and the consumers of fusion center-generated products and services.

Below are the most common themes identified in the answers of the panelists. For Question #4, please rank-order the ten most important items as you perceive them at this time (assign a value of "10" to the most important, "9" to the next most important, and so on until the least important item is assigned a value of "1"). For Question #5, please rank-order the twelve most important items following the same logic. If you wish to add comments expressing agreement, disagreement, or clarification concerning the items, please do so in the space provided below.

***4. Please review each of the following items identified in Questionnaire #1 as important factors that are currently affecting information flow between the Federal Intelligence Community and fusion centers.**

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10
There are issues with the laws and policies that regulate the handling and dissemination of Sensitive But Unclassified information.	○	○	○	○	○	○	○	○	○	○
It is unclear as to who is leading both fusion center and domestic intelligence endeavors	○	○	○	○	○	○	○	○	○	○
A lack of trust has led to insufficient collaboration between the IC and fusion centers, and fusion centers are not comprehensively included in the national intelligence system.	○	○	○	○	○	○	○	○	○	○
There are too many information-sharing networks at the national/federal level.	○	○	○	○	○	○	○	○	○	○
Products created at the federal level lack relevance to state and local needs.	○	○	○	○	○	○	○	○	○	○
There is an absence of robust, standardized, formal mechanisms for the timely exchange of information between the IC and fusion centers.	○	○	○	○	○	○	○	○	○	○
Fusion centers have not adequately identified and shared their intelligence requirements with the Federal Intelligence Community.	○	○	○	○	○	○	○	○	○	○
Over-classification of information inhibits information sharing between federal agencies/personnel and cleared and non-cleared fusion center personnel.	○	○	○	○	○	○	○	○	○	○
The lack of collaboration between DHS and FBI creates an obstacle for information flow.	○	○	○	○	○	○	○	○	○	○
Fusion centers have encountered challenges with accessibility to classified systems.	○	○	○	○	○	○	○	○	○	○

***5. Please review each of the following items identified in Questionnaire #1 as important factors that are currently affecting information flow between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.**

	Least Important 1	2	3	4	5	6	7	8	9	10	11	Most Important 12
The private and public sectors are not adequately engaged in fusion center efforts.	○	○	○	○	○	○	○	○	○	○	○	○
There is an absence of standardized, formal reporting mechanisms and protocols for the timely exchange of information between fusion centers, agencies, and front-line personnel.	○	○	○	○	○	○	○	○	○	○	○	○
A competitive atmosphere, territoriality, interagency rivalries, and a reluctance to share case-specific materials are inhibiting information sharing between agencies and fusion centers.	○	○	○	○	○	○	○	○	○	○	○	○
Consumers are failing to provide clear, concise, relevant intelligence requirements.	○	○	○	○	○	○	○	○	○	○	○	○
Fusion centers have provided limited outreach and marketing efforts regarding their intelligence requirements and production capabilities.	○	○	○	○	○	○	○	○	○	○	○	○
Collection efforts have not been led by intelligence priorities, resulting in disparities between what is collected and consumer requirements.	○	○	○	○	○	○	○	○	○	○	○	○
Current standards of technology are insufficient for knowledge management and the sharing of data, information, and intelligence across agencies, disciplines, and jurisdictions.	○	○	○	○	○	○	○	○	○	○	○	○

No clear models or methods exist to show how disparate agencies can collaborate and/or share information for intelligence endeavors.	○	○	○	○	○	○	○	○	○	○	○
Classification issues affect the ability of fusion center personnel to release information to consumers: over-classification and the lack of tear line reports are keeping information from reaching the streets; additionally, there are issues with the laws and policies that regulate the handling and dissemination of "Sensitive But Unclassified" information.	○	○	○	○	○	○	○	○	○	○	○
Fusion center leadership is not communicating and meeting with consumers to discuss customer satisfaction, intelligence requirements, and strategies to enhanced relationships and collaboration.	○	○	○	○	○	○	○	○	○	○	○
There is a lack of education, training, and experience with intelligence outside the federal level of government.	○	○	○	○	○	○	○	○	○	○	○
There is a lack of adequate feedback and follow-up mechanisms to identify the usefulness of information provided to and from fusion centers.	○	○	○	○	○	○	○	○	○	○	○

5. Information/Intelligence Sharing Enablers

The fifth question in Questionnaire #1 asked panelists to list significant factors, practices, and/or processes that would positively influence the flow of information between:
(a) The Federal Intelligence Community and fusion centers;
(b) Domestic information/intelligence collectors and fusion centers; and,
(c) Fusion centers and the consumers of fusion center-generated products and services.

Below are the most common themes identified in the answers of the panelists. For Question #6, please rank-order the eight most important items as you perceive them at this time (assign a value of "8" to the most important, "7" to the next most important, and so on until the least important item is assigned a value of "1"). For Question #7, please rank-order the ten most important items following the same logic. If you wish to add comments expressing agreement, disagreement, or clarification concerning the items, please do so in the space provided below.

***6. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would positively influence the flow of information between the Federal Intelligence Community and fusion centers.**

	Least Important 1	2	3	4	5	6	7	Most Important 8
The Intelligence Community must (better) define the role of DHS representatives within the fusion centers, and then identify how this role, as well as fusion center access to classified material, is an asset beyond the confines of the fusion center (due to the limited ability to share classified material).	○	○	○	○	○	○	○	○
The Federal government must provide a clear vision of how fusion centers fit into the intelligence community, and then fund it accordingly; create a national strategy for fusion centers that articulates their role and position amongst law enforcement and intelligence agencies at all levels of government.	○	○	○	○	○	○	○	○
The Intelligence Community must consolidate the numerous federal information sharing systems and create a single location for gathering and disseminating information and posting SARs, RFIs, IIRs, etc.	○	○	○	○	○	○	○	○
More training must be conducted amongst federal, state, and local agencies regarding each agencies mission space, how to work together more effectively, and the relevance of specific topics at each level of government.	○	○	○	○	○	○	○	○
More unification in the messages sent from the Intelligence Community to fusion centers; DHS and FBI (as well as other agencies) must collaborate more on join-products to close gaps and provide "one federal voice".	○	○	○	○	○	○	○	○
Federal agencies must declassify more information and produce more write-for-release, and tear line reports that can be shared with (and beyond) the fusion center; standards must be developed for "Sensitive But Unclassified" information so that it can be easily shared and adequately protected.	○	○	○	○	○	○	○	○
Fusion centers must articulate clear, concise, relevant intelligence requirements, and the Intelligence Community must meet those requirements with products tailored to meet their needs.	○	○	○	○	○	○	○	○
Stronger partnerships, collaborations, and trust must be developed amongst Intelligence Community and fusion center agencies; no more "us" vs. "them".	○	○	○	○	○	○	○	○

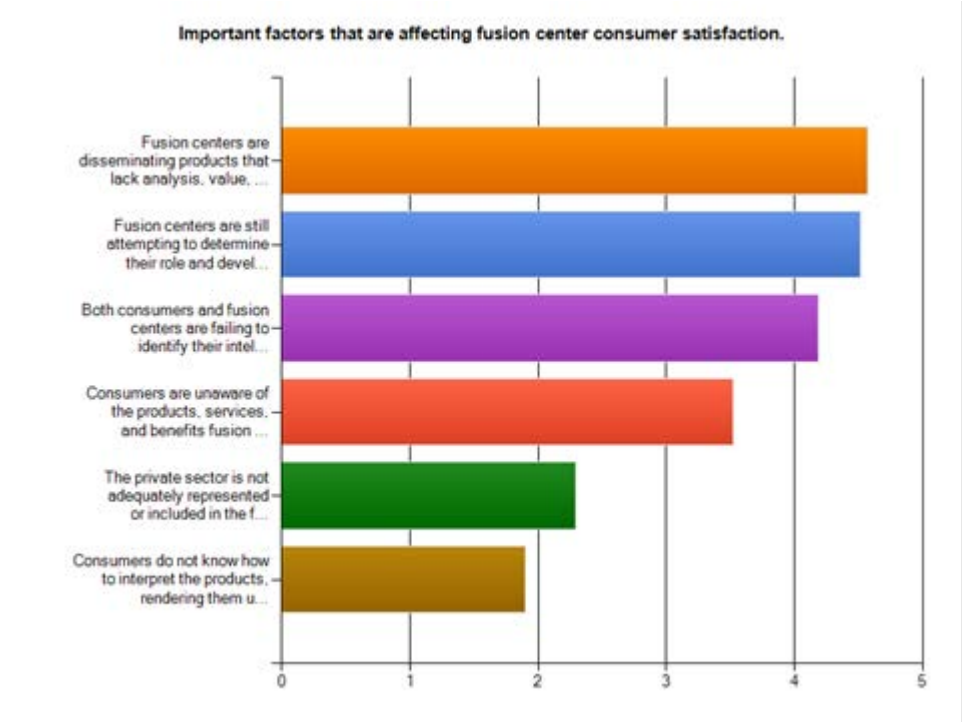
***7. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would positively influence the flow of information between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.**

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10
Fusion centers must harness/develop better technology for information sharing: systems/portals where data, crime bulletins, SARs, IIRs, RFIs, etc. can be posted and shared with all partner agencies within a state or region; standardize the technology so that systems can be interlinked to facilitate this exchange nationally.	○	○	○	○	○	○	○	○	○	○
Fusion center leadership must partake in greater outreach and marketing of the fusion center mission and intelligence requirements; explain what the fusion center does, capabilities, limitations, and what the consumer can provide the fusion center; share success stories and best practices to build trust and confidence.	○	○	○	○	○	○	○	○	○	○
Federal agencies must declassify more information and produce more write-for-release and tear line reports that can be shared beyond the fusion center; standards must be developed for "Sensitive But Unclassified" information so that it can be easily shared and adequately protected.	○	○	○	○	○	○	○	○	○	○
Fusion center personnel must be better trained and educated in leadership, analysis, and intelligence.	○	○	○	○	○	○	○	○	○	○
Fusion centers must develop better evaluation, feedback and follow-up mechanisms to identify the usefulness of information provided to and from consumers.	○	○	○	○	○	○	○	○	○	○
Fusion centers must enhance interagency partnerships, collaborations, communication, outreach, and reach-back capabilities through collocation and the implementation of community, interagency, and sector-specific liaison officer programs.	○	○	○	○	○	○	○	○	○	○
Fusion centers must prioritize intelligence requirements and lead strategically focused collection efforts that meet the needs of consumers.	○	○	○	○	○	○	○	○	○	○
All agencies must promote policy change and cultural change in order to better facilitate information sharing across agencies, disciplines, and sectors.	○	○	○	○	○	○	○	○	○	○
Consumers must articulate clear, concise, relevant intelligence requirements; general requirements must be limited.	○	○	○	○	○	○	○	○	○	○
Fusion centers must establish standardized, formal reporting mechanisms and dissemination protocols for the timely, efficient exchange of information between fusion centers, agencies, and front line personnel.	○	○	○	○	○	○	○	○	○	○

D. DELPHI PANEL: SUMMARY OF RESPONSES PROVIDED FOR QUESTIONNAIRE 2 MAY 7, 2008

1. Please review each of the following items identified in Questionnaire #1 as important factors that are affecting fusion center consumer satisfaction.

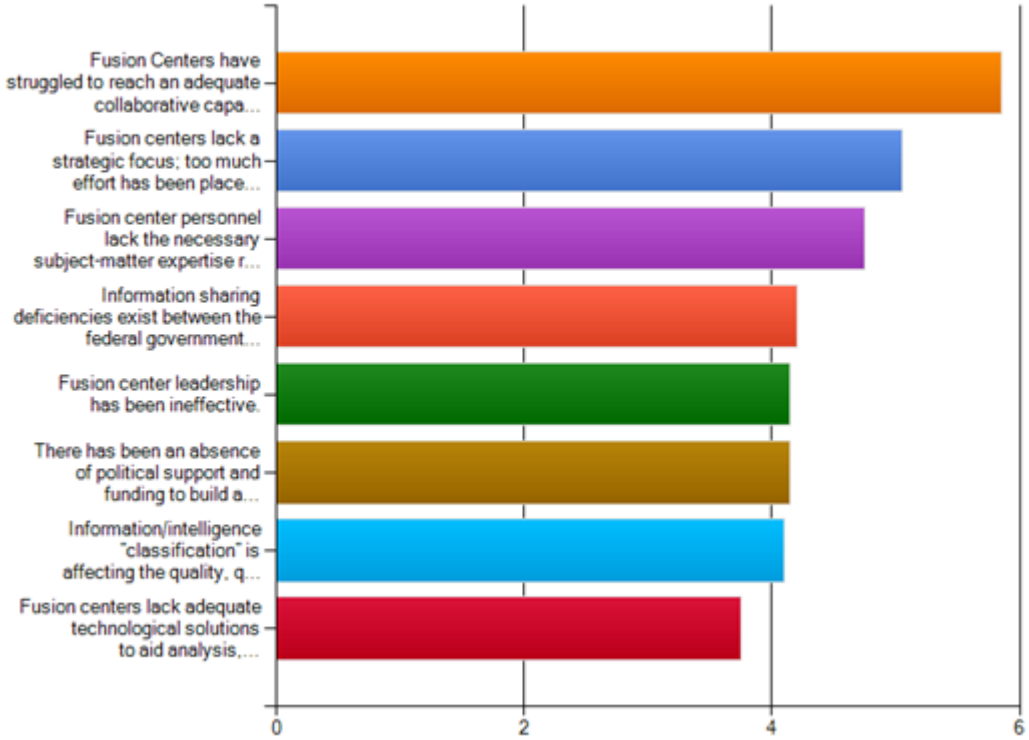
	Least Important 1	2	3	4	5	Most Important 6	Rating Average	Response Count
Both consumers and fusion centers are failing to identify their intelligence requirements/priorities/needs.	14.3% (3)	0.0% (0)	4.8% (1)	**33.3% (7)**	28.6% (6)	19.0% (4)	4.19	21
Fusion centers are disseminating products that lack analysis, value, relevance, and timeliness; the information disseminated can usually be found in the media, and is often a contribution to the routine "circular reporting".	0.0% (0)	9.5% (2)	19.0% (4)	9.5% (2)	28.6% (6)	**33.3% (7)**	4.57	21
Consumers do not know how to interpret the products, rendering them useless or counterproductive.	**38.1% (8)**	**38.1% (8)**	19.0% (4)	4.8% (1)	0.0% (0)	0.0% (0)	1.90	21
The private sector is not adequately represented or included in the fusion center processes or consumer group.	**38.1% (8)**	33.3% (7)	9.5% (2)	4.8% (1)	9.5% (2)	4.8% (1)	2.29	21
Consumers are unaware of the products, services, and benefits fusion centers can provide.	9.5% (2)	9.5% (2)	**28.6% (6)**	**28.6% (6)**	19.0% (4)	4.8% (1)	3.52	21
Fusion centers are still attempting to determine their role and develop the skills necessary to satisfy their consumers.	0.0% (0)	9.5% (2)	19.0% (4)	19.0% (4)	14.3% (3)	**38.1% (8)**	4.52	21



2. Please review each of the following items identified in Questionnaire #1 as important factors that are affecting information and intelligence production at fusion centers.

	Least Important 1	2	3	4	5	6	7	Most Important 8	Rating Average	Response Count
Fusion center personnel lack the necessary subject-matter expertise required to provide relevance and quality analysis to their products and services; more training and education in intelligence, analysis, information technology, and other essential skills is necessary.	5.0% (1)	15.0% (3)	10.0% (2)	**25.0% (5)**	5.0% (1)	10.0% (2)	15.0% (3)	15.0% (3)	4.75	20
Fusion center leadership has been ineffective.	**25.0% (5)**	5.0% (1)	10.0% (2)	10.0% (2)	15.0% (3)	15.0% (3)	15.0% (3)	5.0% (1)	4.15	20
There has been an absence of political support and funding to build and sustain fusion centers that can operate at the necessary capacity; as a result, they are suffering from a shortage of personnel and resources, making it difficult to meet expectations and demands.	15.0% (3)	**30.0% (6)**	10.0% (2)	5.0% (1)	5.0% (1)	5.0% (1)	5.0% (1)	25.0% (5)	4.15	20
Fusion Centers have struggled to reach an adequate collaborative capacity; there have been issues with collocation, partnerships, and the sharing of personnel, resources, decision-making, and accountability.	5.0% (1)	0.0% (0)	5.0% (1)	10.0% (2)	15.0% (3)	**25.0% (5)**	20.0% (4)	20.0% (4)	5.85	20
Fusion centers lack a strategic focus; too much effort has been placed on tactical and operational support, rather than strategic analysis.	10.0% (2)	5.0% (1)	5.0% (1)	10.0% (2)	**25.0% (5)**	20.0% (4)	15.0% (3)	10.0% (2)	5.05	20
Information sharing deficiencies exist between the federal government and fusion centers.	15.0% (3)	10.0% (2)	**25.0% (5)**	0.0% (0)	20.0% (4)	10.0% (2)	10.0% (2)	10.0% (2)	4.20	20
Information/intelligence "classification" is affecting the quality, quantity, and timeliness of information that can be released to fusion center consumers; information provided from federal agencies is often over-classified, and there is a shortage of tear line and "write-for-release" reports available for product development and dissemination.	15.0% (3)	**20.0% (4)**	15.0% (3)	15.0% (3)	5.0% (1)	0.0% (0)	15.0% (3)	15.0% (3)	4.10	20
Fusion centers lack adequate technological solutions to aid analysis, access relevant databases, and facilitate information sharing and product delivery.	10.0% (2)	15.0% (3)	20.0% (4)	**25.0% (5)**	10.0% (2)	15.0% (3)	5.0% (1)	0.0% (0)	3.75	20

Important factors that are affecting information and intelligence production at fusion centers.

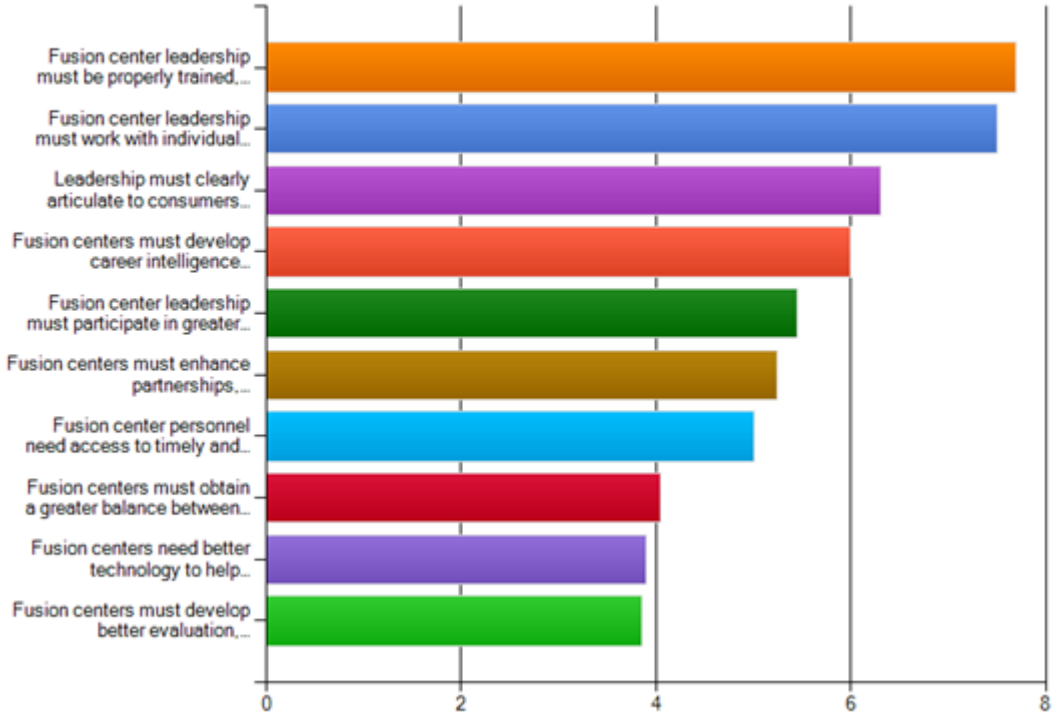


3. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10	Rating Average	Response Count
Fusion center leadership must participate in greater marketing and outreach programs by publicizing their mission, success stories, and best practices; furthermore, leadership must develop strong, active, lasting relationships with agencies from all disciplines, levels of government, and the private and public sectors.	15.0% (3)	15.0% (3)	10.0% (2)	10.0% (2)	5.0% (1)	5.0% (1)	5.0% (1)	0.0% (0)	10.0% (2)	**25.0% (5)**	5.45	20
Fusion centers must enhance partnerships, collaborations, outreach, and reach-back capabilities through the implementation of community, interagency, and sector-specific liaison officer programs.	10.0% (2)	**25.0% (5)**	10.0% (2)	5.0% (1)	0.0% (0)	5.0% (1)	5.0% (1)	15.0% (3)	20.0% (4)	5.0% (1)	5.25	20

Fusion center leadership must work with individual consumers to set clear, concise intelligence requirements, and develop an effective means of adjusting requirements according to their evolving needs.	0.0% (0)	5.0% (1)	0.0% (0)	5.0% (1)	15.0% (3)	5.0% (1)	10.0% (2)	20.0% (4)	15.0% (3)	**25.0% (5)**	7.50	20
Leadership must clearly articulate to consumers the capacity of the fusion center, and ensure that consumer expectations do not exceed the fusion center's capabilities.	0.0% (0)	0.0% (0)	10.0% (2)	10.0% (2)	10.0% (2)	**25.0% (5)**	20.0% (4)	15.0% (3)	0.0% (0)	10.0% (2)	6.30	20
Fusion centers must develop better evaluation, feedback, and follow-mechanisms to identify the usefulness of information provided to and from consumers.	10.0% (2)	15.0% (3)	**25.0% (5)**	15.0% (3)	15.0% (3)	10.0% (2)	5.0% (1)	5.0% (1)	0.0% (0)	0.0% (0)	3.85	20
Fusion center leadership must be properly trained, strategically focused, and experienced with the intelligence profession; set and regulate strategic priorities, planning and direction; focus collection efforts according to consumer requirements; ensure that all processes and practices conform to the intelligence cycle.	0.0% (0)	0.0% (0)	0.0% (0)	10.0% (2)	10.0% (2)	5.0% (1)	10.0% (2)	**25.0% (5)**	20.0% (4)	20.0% (4)	7.70	20
Fusion centers must develop career intelligence professionals; personnel must be properly trained and educated, and given the time to gain experience and develop greater analytic skill.	10.0% (2)	5.0% (1)	10.0% (2)	10.0% (2)	5.0% (1)	5.0% (1)	**20.0% (4)**	10.0% (2)	15.0% (3)	10.0% (2)	6.00	20
Fusion center personnel need access to timely and relevant unclassified information from the Federal Intelligence Community that can be applied to their products and analysis.	10.0% (2)	10.0% (2)	5.0% (1)	10.0% (2)	15.0% (3)	**25.0% (5)**	15.0% (3)	5.0% (1)	5.0% (1)	0.0% (0)	5.00	20
Fusion centers need better technology to help facilitate collection, analysis, dissemination, and knowledge management.	**25.0% (5)**	10.0% (2)	20.0% (4)	10.0% (2)	10.0% (2)	5.0% (1)	5.0% (1)	5.0% (1)	10.0% (2)	0.0% (0)	3.90	20
Fusion centers must obtain a greater balance between tactical and strategic product development and operational priorities.	**20.0% (4)**	15.0% (3)	10.0% (2)	15.0% (3)	15.0% (3)	10.0% (2)	5.0% (1)	0.0% (0)	5.0% (1)	5.0% (1)	4.05	20

Significant factors, practices, and/or processes that would help fusion centers generate relevant information/intelligence products and services.

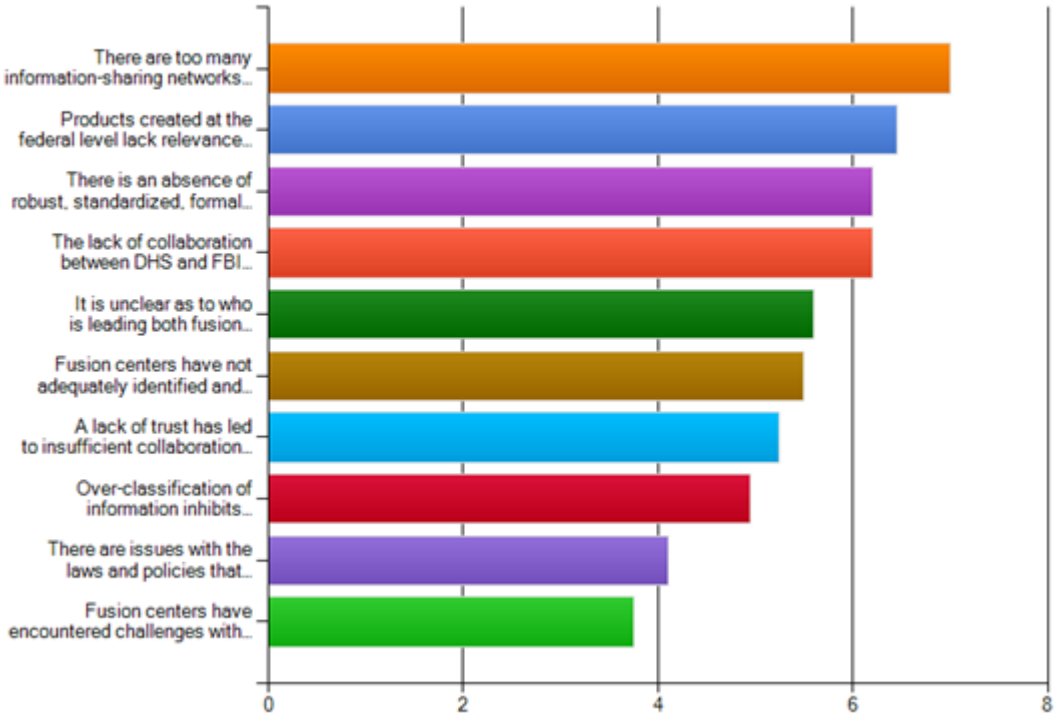


4. Please review each of the following items identified in Questionnaire #1 as important factors that are currently affecting information flow between the Federal Intelligence Community and fusion centers.

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10	Rating Average	Response Count
Over-classification of information inhibits information sharing between federal agencies/personnel and cleared and non-cleared fusion center personnel.	10.0% (2)	15.0% (3)	10.0% (2)	0.0% (0)	**20.0% (4)**	15.0% (3)	15.0% (3)	5.0% (1)	10.0% (2)	0.0% (0)	4.95	20
There is an absence of robust, standardized, formal mechanisms for the timely exchange of information between the IC and fusion centers.	0.0% (0)	10.0% (2)	0.0% (0)	**20.0% (4)**	10.0% (2)	10.0% (2)	15.0% (3)	15.0% (3)	15.0% (3)	5.0% (1)	6.20	20
There are too many information-sharing networks at the national/federal level.	15.0% (3)	0.0% (0)	5.0% (1)	0.0% (0)	0.0% (0)	15.0% (3)	10.0% (2)	10.0% (2)	20.0% (4)	**25.0% (5)**	7.00	20
Fusion centers have not adequately identified and shared their intelligence requirements with the Federal Intelligence Community.	10.0% (2)	5.0% (1)	10.0% (2)	**20.0% (4)**	0.0% (0)	15.0% (3)	10.0% (2)	15.0% (3)	10.0% (2)	5.0% (1)	5.50	20
Fusion centers have encountered challenges with accessibility to classified systems.	10.0% (2)	**25.0% (5)**	**25.0% (5)**	5.0% (1)	15.0% (3)	10.0% (2)	5.0% (1)	0.0% (0)	0.0% (0)	5.0% (1)	3.75	20

A lack of trust has led to insufficient collaboration between the IC and fusion centers, and fusion centers are not comprehensively included in the national intelligence system.	**15.0% (3)**	10.0% (2)	10.0% (2)	**15.0% (3)**	5.0% (1)	10.0% (2)	0.0% (0)	**15.0% (3)**	5.0% (1)	**15.0% (3)**	5.25	20
It is unclear as to who is leading both fusion center and domestic intelligence endeavors	5.0% (1)	0.0% (0)	20.0% (4)	0.0% (0)	**30.0% (6)**	10.0% (2)	10.0% (2)	15.0% (3)	5.0% (1)	5.0% (1)	5.60	20
The lack of collaboration between DHS and FBI creates an obstacle for information flow.	5.0% (1)	10.0% (2)	10.0% (2)	15.0% (3)	10.0% (2)	5.0% (1)	0.0% (0)	5.0% (1)	15.0% (3)	**25.0% (5)**	6.20	20
There are issues with the laws and policies that regulate the handling and dissemination of Sensitive But Unclassified information.	**30.0% (6)**	15.0% (3)	5.0% (1)	15.0% (3)	0.0% (0)	5.0% (1)	10.0% (2)	10.0% (2)	5.0% (1)	5.0% (1)	4.10	20

Important factors that are currently affecting information flow between the Federal Intelligence Community and fusion centers.

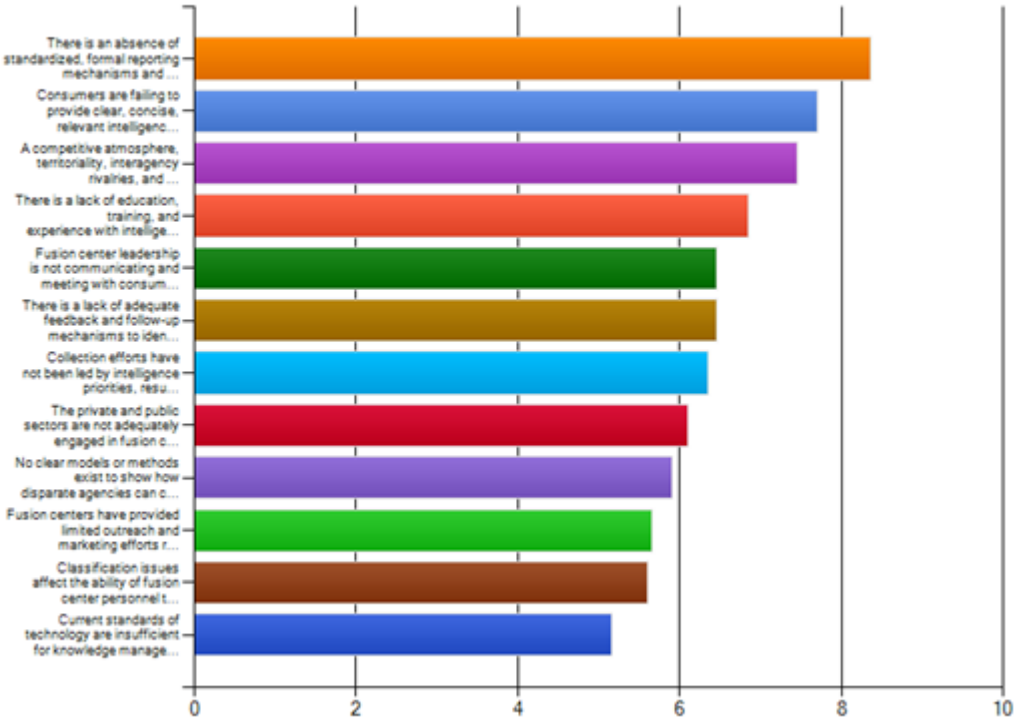


5. Please review each of the following items identified in Questionnaire #1 as important factors that are currently affecting information flow between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.

	Least Important 1	2	3	4	5	6	7	8	9	10	11	Most Important 12	Rating Average
The private and public sectors are not adequately engaged in fusion center efforts.	0.0% (0)	15.0% (3)	10.0% (2)	5.0% (1)	15.0% (3)	10.0% (2)	10.0% (2)	**20.0% (4)**	0.0% (0)	5.0% (1)	5.0% (1)	5.0% (1)	6.10
Classification issues affect the ability of fusion center personnel to release information to consumers: over-classification and the lack of tear line reports are keeping information from reaching the streets; additionally, there are issues with the laws and policies that regulate the handling and dissemination of "Sensitive But Unclassified" information.	10.0% (2)	10.0% (2)	15.0% (3)	**20.0% (4)**	0.0% (0)	5.0% (1)	10.0% (2)	5.0% (1)	10.0% (2)	0.0% (0)	5.0% (1)	10.0% (2)	5.60
There is a lack of education, training, and experience with intelligence outside the federal level of government.	0.0% (0)	10.0% (2)	10.0% (2)	0.0% (0)	15.0% (3)	10.0% (2)	5.0% (1)	15.0% (3)	**20.0% (4)**	5.0% (1)	5.0% (1)	5.0% (1)	6.85
There is a lack of education, training, and experience with intelligence outside the federal level of government.	0.0% (0)	10.0% (2)	10.0% (2)	0.0% (0)	15.0% (3)	10.0% (2)	5.0% (1)	15.0% (3)	**20.0% (4)**	5.0% (1)	5.0% (1)	5.0% (1)	6.85
Consumers are failing to provide clear, concise, relevant intelligence requirements.	5.0% (1)	0.0% (0)	5.0% (1)	15.0% (3)	5.0% (1)	10.0% (2)	5.0% (1)	5.0% (1)	15.0% (3)	0.0% (0)	**25.0% (5)**	10.0% (2)	7.70
Fusion center leadership is not communicating and meeting with consumers to discuss customer satisfaction, intelligence requirements, and strategies to enhanced relationships and collaboration.	5.0% (1)	5.0% (1)	10.0% (2)	15.0% (3)	**20.0% (4)**	5.0% (1)	0.0% (0)	5.0% (1)	0.0% (0)	**20.0% (4)**	10.0% (2)	5.0% (1)	6.45
Collection efforts have not been led by intelligence priorities, resulting in disparities between what is collected and consumer requirements.	15.0% (3)	5.0% (1)	0.0% (0)	**20.0% (4)**	5.0% (1)	0.0% (0)	15.0% (3)	5.0% (1)	10.0% (2)	10.0% (2)	10.0% (2)	5.0% (1)	6.35
No clear models or methods exist to show how disparate agencies can collaborate and/or share information for intelligence endeavors.	10.0% (2)	15.0% (3)	5.0% (1)	5.0% (1)	**20.0% (4)**	5.0% (1)	0.0% (0)	5.0% (1)	15.0% (3)	15.0% (3)	0.0% (0)	5.0% (1)	5.90
Current standards of technology are insufficient for knowledge management and the sharing of data, information, and intelligence across agencies, disciplines, and jurisdictions.	15.0% (3)	20.0% (4)	10.0% (2)	0.0% (0)	5.0% (1)	**25.0% (5)**	5.0% (1)	5.0% (1)	0.0% (0)	0.0% (0)	0.0% (0)	15.0% (3)	5.15
There is an absence of standardized, formal reporting mechanisms and protocols for the timely exchange of information between fusion centers, agencies, and front-line personnel.	0.0% (0)	0.0% (0)	5.0% (1)	10.0% (2)	0.0% (0)	10.0% (2)	**20.0% (4)**	5.0% (1)	5.0% (1)	15.0% (3)	15.0% (3)	15.0% (3)	8.35

Fusion centers have provided limited outreach and marketing efforts regarding their intelligence requirements and production capabilities.	**20.0% (4)**	10.0% (2)	10.0% (2)	5.0% (1)	0.0% (0)	10.0% (2)	10.0% (2)	5.0% (1)	5.0% (1)	15.0% (3)	10.0% (2)	0.0% (0)	5.65
A competitive atmosphere, territoriality, interagency rivalries, and a reluctance to share case-specific materials are inhibiting information sharing between agencies and fusion centers.	10.0% (2)	10.0% (2)	5.0% (1)	0.0% (0)	5.0% (1)	5.0% (1)	5.0% (1)	**20.0% (4)**	0.0% (0)	10.0% (2)	10.0% (2)	**20.0% (4)**	7.45
There is a lack of adequate feedback and follow-up mechanisms to identify the usefulness of information provided to and from fusion centers.	10.0% (2)	0.0% (0)	15.0% (3)	5.0% (1)	10.0% (2)	5.0% (1)	15.0% (3)	5.0% (1)	**20.0% (4)**	5.0% (1)	5.0% (1)	5.0% (1)	6.45

Important factors that are currently affecting information flow between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.

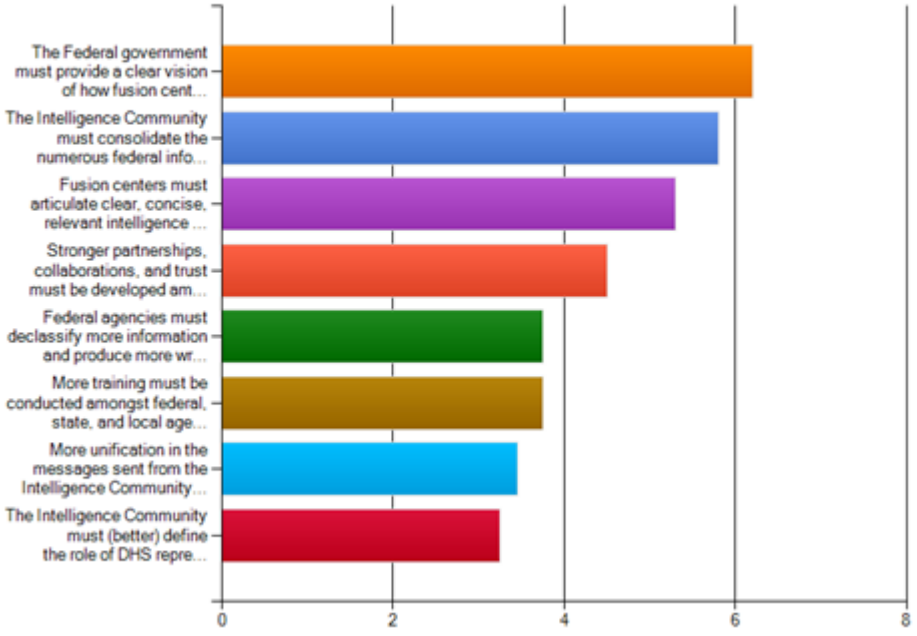


6. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would positively influence the flow of information between the Federal Intelligence Community and fusion centers.

	Least Important 1	2	3	4	5	6	7	Most Important 8	Rating Average	Response Count
More unification in the messages sent from the Intelligence Community to fusion centers; DHS and FBI (as well as other agencies) must collaborate more on join-products to close gaps and provide "one federal voice".	15.0% (3)	**25.0% (5)**	15.0% (3)	10.0% (2)	15.0% (3)	20.0% (4)	0.0% (0)	0.0% (0)	3.45	20
The Intelligence Community must consolidate the numerous federal information sharing systems and create a single location for gathering and disseminating information and posting SARs, RFIs, IIRs, etc.	5.0% (1)	5.0% (1)	15.0% (3)	0.0% (0)	5.0% (1)	10.0% (2)	**45.0% (9)**	15.0% (3)	5.80	20
Federal agencies must declassify more information and produce more write-for-release, and tear line reports that can be shared with (and beyond) the fusion center; standards must be developed for "Sensitive But Unclassified" information so that it can be easily shared and adequately protected.	20.0% (4)	0.0% (0)	10.0% (2)	**40.0% (8)**	20.0% (4)	5.0% (1)	5.0% (1)	0.0% (0)	3.75	20
More training must be conducted amongst federal, state, and local agencies regarding each agencies mission space, how to work together more effectively, and the relevance of specific topics at each level of government.	**25.0% (5)**	15.0% (3)	15.0% (3)	5.0% (1)	5.0% (1)	20.0% (4)	10.0% (2)	5.0% (1)	3.75	20
Fusion centers must articulate clear, concise, relevant intelligence requirements, and the Intelligence Community must meet those requirements with products tailored to meet their needs.	0.0% (0)	5.0% (1)	15.0% (3)	**25.0% (5)**	15.0% (3)	0.0% (0)	20.0% (4)	20.0% (4)	5.30	20
The Federal government must provide a clear vision of how fusion centers fit into the intelligence community, and then fund it accordingly; create a national strategy for fusion centers that articulates their role and position amongst law enforcement and intelligence agencies at all levels of government.	5.0% (1)	5.0% (1)	0.0% (0)	0.0% (0)	25.0% (5)	15.0% (3)	10.0% (2)	**40.0% (8)**	6.20	20

The Intelligence Community must (better) define the role of DHS representatives within the fusion centers, and then identify how this role, as well as fusion center access to classified material, is an asset beyond the confines of the fusion center (due to the limited ability to share classified material).	20.0% (4)	**35.0% (7)**	10.0% (2)	10.0% (2)	5.0% (1)	10.0% (2)	0.0% (0)	10.0% (2)	3.25	20
Stronger partnerships, collaborations, and trust must be developed amongst Intelligence Community and fusion center agencies; no more "us" vs. "them".	10.0% (2)	10.0% (2)	**20.0% (4)**	10.0% (2)	10.0% (2)	**20.0% (4)**	10.0% (2)	10.0% (2)	4.50	20

Significant factors, practices, and/or processes that would positively influence the flow of information between the Federal Intelligence Community and fusion centers.

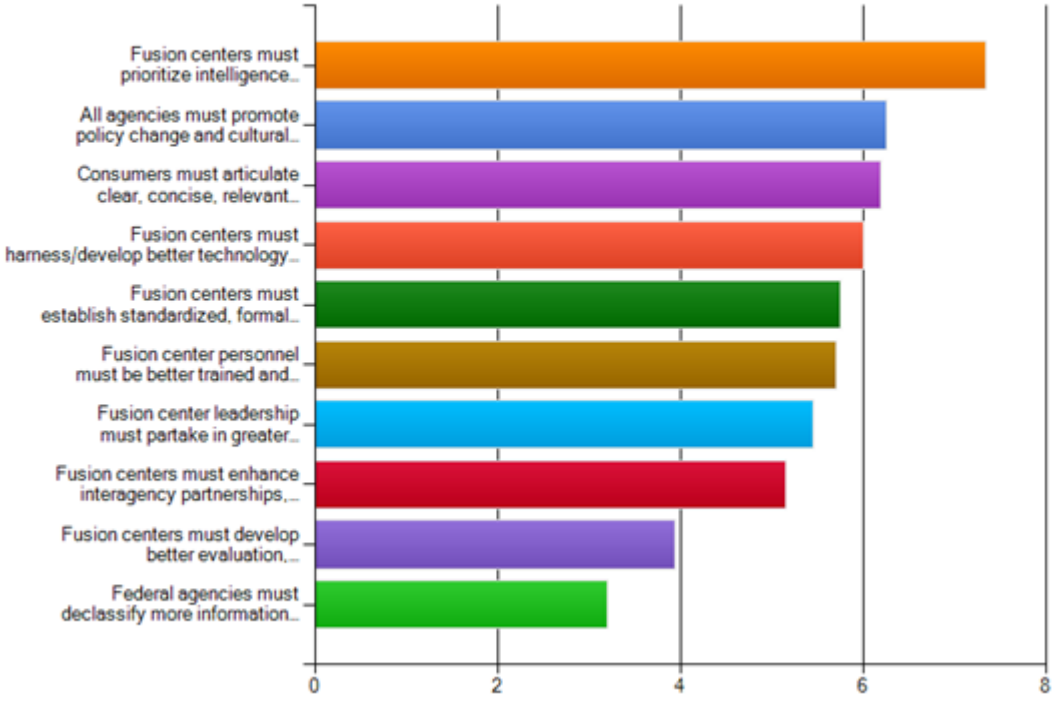


7. Please review each of the following items identified in Questionnaire #1 as significant factors, practices, and/or processes that would positively influence the flow of information between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.

	Least Important 1	2	3	4	5	6	7	8	9	Most Important 10	Rating Average	Response Count
Fusion centers must harness/develop better technology for information sharing: systems/portals where data, crime bulletins, SARs, IIRs, RFIs, etc. can be posted and shared with all partner agencies within a state or region; standardize the technology so that systems can be interlinked to facilitate this exchange nationally.	15.0% (3)	5.0% (1)	10.0% (2)	5.0% (1)	5.0% (1)	5.0% (1)	15.0% (3)	15.0% (3)	5.0% (1)	**20.0% (4)**	6.00	20
Fusion centers must establish standardized, formal reporting mechanisms and dissemination protocols for the timely, efficient exchange of information between fusion centers, agencies, and front line personnel.	5.0% (1)	5.0% (1)	5.0% (1)	10.0% (2)	**25.0% (5)**	15.0% (3)	10.0% (2)	5.0% (1)	20.0% (4)	0.0% (0)	5.75	20
Fusion centers must enhance interagency partnerships, collaborations, communication, outreach, and reach-back capabilities through collocation and the implementation of community, interagency, and sector-specific liaison officer programs.	**15.0% (3)**	10.0% (2)	**15.0% (3)**	5.0% (1)	10.0% (2)	**15.0% (3)**	5.0% (1)	0.0% (0)	10.0% (2)	**15.0% (3)**	5.15	20
Fusion center personnel must be better trained and educated in leadership, analysis, and intelligence.	15.0% (3)	5.0% (1)	5.0% (1)	15.0% (3)	0.0% (0)	15.0% (3)	**20.0% (4)**	0.0% (0)	10.0% (2)	15.0% (3)	5.70	20
Fusion center leadership must partake in greater outreach and marketing of the fusion center mission and intelligence requirements; explain what the fusion center does, capabilities, limitations, and what the consumer can provide the fusion center; share success stories and best practices to build trust and confidence.	5.0% (1)	10.0% (2)	10.0% (2)	**20.0% (4)**	15.0% (3)	5.0% (1)	0.0% (0)	15.0% (3)	15.0% (3)	5.0% (1)	5.45	20
Consumers must articulate clear, concise, relevant intelligence requirements; general requirements must be limited.	5.0% (1)	5.0% (1)	15.0% (3)	0.0% (0)	15.0% (3)	5.0% (1)	15.0% (3)	15.0% (3)	**20.0% (4)**	5.0% (1)	6.20	20
Fusion centers must develop better evaluation, feedback and follow-up mechanisms to identify the usefulness of information provided to and from consumers.	15.0% (3)	**30.0% (6)**	10.0% (2)	10.0% (2)	5.0% (1)	0.0% (0)	15.0% (3)	15.0% (3)	0.0% (0)	0.0% (0)	3.95	20
All agencies must promote policy change and cultural change in order to better facilitate information sharing across agencies, disciplines, and sectors.	5.0% (1)	0.0% (0)	10.0% (2)	**20.0% (4)**	5.0% (1)	15.0% (3)	5.0% (1)	**20.0% (4)**	0.0% (0)	**20.0% (4)**	6.25	20

Fusion centers must prioritize intelligence requirements and lead strategically focused collection efforts that meet the needs of consumers.	0.0% (0)	0.0% (0)	0.0% (0)	10.0% (2)	10.0% (2)	**20.0% (4)**	10.0% (2)	15.0% (3)	15.0% (3)	**20.0% (4)**	7.35	20
Federal agencies must declassify more information and produce more write-for-release and tear line reports that can be shared beyond the fusion center; standards must be developed for "Sensitive But Unclassified" information so that it can be easily shared and adequately protected.	20.0% (4)	**30.0% (6)**	20.0% (4)	5.0% (1)	10.0% (2)	5.0% (1)	5.0% (1)	0.0% (0)	5.0% (1)	0.0% (0)	3.20	20

Significant factors, practices, and/or processes that would positively influence the flow of information between domestic information/intelligence collectors, fusion centers, and the consumers of fusion center-generated information/intelligence.



THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF REFERENCES

Bain, Ben. "Confusion Over Fusion Centers." *Federal Computer Week*. October 8, 2007. http://fcw.com/Articles/2007/10/04/Confusion-over-fusion-centers.aspx?p=1. Accessed October 10, 2007.

———. "Lawmakers Blast DHS' Efforts to Share Intel with State, Local Partners." *Federal Computer Week*. February 28, 2008. http://fcw.com/articles/2008/02/28/lawmakers-blast-dhs-efforts-to-share-intell-with-state-local-partners.aspx. Accessed March 22, 2008.

———. "Lawmaker to DHS: Step it up with Fusion Centers." *Federal Computer Week*. March 20, 2008. http://fcw.com/articles/2008/03/20/lawmaker-to-dhs-step-it-up-with-fusion-centers.aspx. Accessed June 1, 2008.

Beasley, Norman. "The Way Forward with Fusion Centers: Challenges and Strategies for Change." *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*, 110th Cong., 1st sess., September 27, 2007. http://www.fas.org/irp/congress/2007_hr/092707beasley.pdf Accessed October 16, 2007.

Beasley, Norman, Douglas Johnson, Mike Sena, and Rick Salyers. "Liaison Officer Programs." Presentation at the 2008 National Fusion Center Conference, San Francisco, CA, March 18–20, 2008.

Blair, Dennis. "Luncheon Keynote Address." Presented to State of Intelligence Reform Conference, Bipartisan Policy Center, Washington, D.C., April 6, 2010. http://www.bipartisanpolicy.org/news/multimedia/2010/04/07/videos-447. Accessed August 14, 2011.

Bouche, Kenneth. "State and Local fusion Center and the Role of DHS." *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*. 109th Cong., 2nd Sess., 2006. http://www.fas.org/irp/congress/2006_hr/090706bouche.pdf. Accessed October 16, 2007.

Brafman, Ori and Rod A. Beckstrom, *The Starfish and the Spider: The Unstoppable Power of Leaderless Organizations*. New York: Penguin Group, 2006.

Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies*. Washington, DC: U.S. Department of Justice, Office of Community Oriented Policing Services, and Michigan State University, 2004.

CENTRA Technology. *Enhancing DHS Information Support to State and Local Fusion Centers: Results of the Chief Intelligence Officer's Pilot Project and Next Steps*. Burlington, MA: February 2008.

Chertoff, Michael. "Remarks by the Secretary of Homeland Security Michael Chertoff at the International Association of Chiefs of Police Annual Conference." Remarks presented to the International Association of Chiefs of Police Annual Conference, Boston, MA, October 16, 2006. http://www.dhs.gov/xnews/speeches/sp_1161184338115.shtm. Accessed June 9, 2007

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States*. Washington, D.C.: 2005.

"Committee Leaders Urge Secretary Chertoff to Move Forward with Information Sharing." In *United States House of Representative Committee on Homeland Security*. September 27, 2007. http://chsdemocrats.house.gov/press/index.asp?ID=275&SubSection=3&Issue=0&DocumentType=0&PublishDate=0. Accessed December 10, 2007.

Connolly, Tim. "Interagency Threat Assessment and Coordination Group." Presentation to the International Association of Law Enforcement Intelligence Analysts, Boston, MA, April 8, 2008.

Delbecq, Andre L., Andrew H. Van de Ven, and David H. Gustafson. *Group Techniques for Program Planning: A Guide to Nominal Group and Delphi Processes*. Glenview, IL: Scott, Foresman and Co., 1975.

Dizard III, Wilson. "Study: Flaws in Fusion Centers." *Government Computer News*. July 30, 2007. http://www.gcn.com/print/26_19/44738-1.html?topic=state-local. Accessed August 10, 2007.

Executive Order 13354: National Counterterrorism Center. *Federal Register* 69, no. 169 (August 2004).

Facer, Tom. "Interagency Threat Assessment and Coordination Group." Presentation to the 2008 National Fusion Center Conference, San Francisco, CA, March 17–20, 2008.

Gerencser, Mark, Reginald Van Lee, Fernando Napolitano, and Christopher Kelly, *Megacommunities: How Leaders of Government, Business and Non-Profits Can Tackle Today's Global Challenges Together*. New York: Palgrave MacMillan, 2008.

Global Justice Information Sharing Initiative. *Baseline Capabilities for State and Major Urban Area Fusion Centers*. Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2008.

———. *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, D.C.: Global Justice Information Sharing Initiative, Department of Justice, 2006.

———. *National Criminal Intelligence Sharing Plan*. Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2003.

———. *Privacy and Civil Liberties Policy Development Guide and Implementation Templates*. Washington, D.C.: Global Justice Information Sharing Initiative, Department of Justice, 2008.

Gorman, Siobhan. "Out of the Loop on Terror Threats: Homeland Security Excludes State, Local Officials from Group that Shares Data." *Baltimore Sun*. February 2, 2007. http://insaonline.org/pdfs/Article%202-Baltimore%20Sun.pdf. Accessed June 1, 2008.

Homeland Security Act of 2002. Public Law 107-296. 107th Cong., 2nd Sess. (November 2002), H.R. 5005, Title VIII.

Homeland Security Council. *National Strategy for Homeland Security*. Washington D.C.: Homeland Security Council, 2007.

Implementing Recommendations of the 9/11 Commission Act of 2007. Public Law 110-53, 110th U.S. Cong., 1st Sess (August 2007). H.R. 1, Subtitle C, Sec. 521, Sec 210D.

"Intelligence Community Civilian Joint Duty Program Honored as Innovations in American Government Award Winner." Office of the Director of National Intelligence Public Affairs Office. September 9, 2008. www.dni.gov/press_releases/20080910_release.pdf. Accessed April 15, 2011.

Intelligence Reform and Terrorism Prevention Act of 2004. Public Law 108-458, 108th Cong., 1st Sess. (December 2004).

Interagency Threat Assessment and Coordination Group. *ITACG: Intelligence Guide for First Responders*. Washington, D.C.: Interagency Threat Assessment and Coordination Group, 2009.

Johnson, Bart. "Status of Efforts to Support Increased Capacity and Sustainment Across the National Network of Fusion Centers." Briefing to the Criminal Intelligence Coordinating Council, Washington, D.C., May 12, 2011.

Krizan, Lisa. "Intelligence Essentials for Everyone." *Occasional Paper Number Six*. Washington, D.C.: Joint Military Intelligence College, 1999.

Larence, Eileen R. "Focus on Fusion Centers: A Progress Report." In *Prepared Testimony Before the Senate Committee on Homeland Security and Governmental Affairs Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration*. 110th Cong., 2nd Sess. http://www.fas.org/irp/congress/2008_hr/fusion.pdf. Accessed August 14, 2011.

Leavell, Ron. "Evolution of Regional Counterterrorism Centers Within a National Counterterrorism Network: Is It Time to Fuse More Than Information?" Master's thesis, Naval Postgraduate School, 2007.

Leiter, Michael. "Looming Challenges in the War on Terror." Remarks presented to the Washington Institute for Near East Policy, Washington, D.C., February 13, 2008. http://www.nctc.gov/press_room/speeches/wash-inst-written-sfr-final.pdf. Accessed March 7, 2008.

Linstone, Harold A. and Murray Turnoff. *The Delphi Method: Techniques and Applications*. Newark, NJ: Information Systems Dept., New Jersey Institute of Technology, 2002. http://www.is.njit.edu/pubs/delphibook. Accessed January 23, 2008.

Lipowicz, Alice. "CRS: Mission Creep at Fusion Centers." *Government Computer News*, July 9, 2007. http://www.gcn.com/online/vol1_no1/44629-1.html. Accessed August 10, 2007.

Logan, Chris. "2007 State Homeland Security Directors Survey." *Issue Brief*. December 18, 2007. Washington, DC: National Governors Association Center for Best Practices.

Lowenthal, Mark M. *Intelligence, From Secrets to Policy*. 3rd ed. Washington, DC: Congressional Quarterly Press, 2002.

Mahaskey, M. Scott. "Scott Redd: Imagination, Collaboration Keys to Counterterrorism." *Federal Times*. August 6, 2007, http://www.federaltimes.com/index.php?S=2945016. Accessed August 14, 2011.

Masse, Todd, Siobhan O'Neil, and John Rollins. *Fusion Centers: Issues and Options for Congress*. Washington, D.C.: Congressional Research Service, 2007. www.fas.org/sgp/crs/intel/RL34070.pdf (accessed September 9, 2007), 19.

McConnell, Mike. "Intelligence Community Civilian Joint Duty Program Implementing Instructions." In *Intelligence Community Policy Guidance Number 601.01*. Washington, D.C.: Office of the Director of National Intelligence, 2007.

Miller, Jason. "Better Information Sharing on the Horizon." *Federal Computer Week*. November 15, 2007. http://fcw.com/articles/2007/11/15/better-information-sharing-on-the-horizon.aspx. Accessed December 19, 2007.

Miller, Lehew and David Carabin. "Perspectives from the Field on the 2010 Baseline Capabilities Assessment." Presented at the Critical Operational Capabilities Gap Mitigation Workshop, Washington, D.C., August 24–25, 2010.

Mitchell, Jeff. "2006 State Homeland Security Directors Survey: New Challenges, Changing Relationships." *Issue Brief*. April 3, 2006. Washington, DC: National Governors Association Center for Best Practices.

Moody, Jamison. "DHS Office of Intelligence and Analysis Support to State and Local Governments." Adapted from U.S. Department of Homeland Security, State and Local Program Office presentation to Utah Statewide Information & Analysis Center Governance Board, Sandy, UT, January 26, 2010.

Murphy, Wayne M. "Making Homeland Security Intelligence Work for State, Local, and Tribal Partners: An Interagency Threat Assessment Coordination Group Progress Report." *Prepared Statement for U.S. Congress. House. Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment*. 110th Cong., 2nd Sess., March 13, 2008. http://www.fas.org/irp/congress/2008_hr/hsint.pdf. Accessed March 22, 2008.

National Commission on Terrorist Attacks upon the United States. *Final Report of the National Commission on Terrorist Attacks upon the United States*. New York: W.W. Norton & Company, 2004.

National Counterterrorism Center. "About the National Counterterrorism Center," http://www.nctc.gov/about_us/about_nctc.html. Accessed August 14, 2011.

National Counterterrorism Center. "ITACG Roles and Responsibilities." http://www.nctc.gov/itacg/itacg_roles_and_responsibilities.html. Accessed July 16, 2011.

National Counterterrorism Center. *NCTC and Information Sharing: Five Years Since 9/11: A Progressive Report*. Washington, D.C.: National Counterterrorism Center, 2006. www.nctc.gov/docs/report_card_final.pdf. Accessed March 2, 2008.

Office of Evaluation and Monitoring, United Nations World Food Program. *Choosing Methods and Tools for Data Collection*. http://documents.wfp.org/stellent/groups/public/documents/ko/mekb_module_13.pdf. Accessed August 13, 2011.

Office of Homeland Security. *National Strategy for Homeland Security*. Washington D.C.: Office of Homeland Security. 2002.

Office of the Deputy Director of National Intelligence for Analysis. *Analytic Transformation: Unleashing the Potential of a Community of Analysts*. Washington, D.C.: Office of the Director of National Intelligence, 2008.

Office of the Director of National Intelligence. *National Intelligence Strategy for the United States of America*. Washington, D.C.: Office of the Director of National Intelligence, 2005.

———. *National Intelligence Estimate*: *The Terrorist Threat to the U.S. Homeland*. Washington, D.C.: National Intelligence Council, 2007.

Okoli, Chitu and Suzanne D. Pawlowski. "The Delphi Method as a Research Tool: an Example, Design Considerations and Applications." *Information & Management* 42 (December 2004), 15–29.

Oliver-Hoyo, Maria and DeeDee Allen. "The Use of Triangulation Methods in Qualitative Educational Research." *Journal of College Science Teaching* 35, no. 4 (2006): 42–47.

Pile, David J. "Overview of the Office of the Director of National Intelligence and Current Intelligence Initiatives." Presentation to the Naval Postgraduate School, Monterey, CA, July 28, 2008.

Program Manager, Information Sharing Environment. *2010 Report on the Interagency Threat Assessment and Coordination Group*. Washington, D.C.: Office of the Director of National Intelligence, 2010.

———. *2010 Annual Report to Congress*. Washington, D.C.: Program Manager, Information Sharing Environment, 2010.

———. *Establishing the Interagency Threat Assessment and Coordination Group: Report for the Congress of the United* States. Washington, D.C.: March 2008.

———. *Information Sharing Environment Implementation Plan*. Washington, D.C.: Office of the Director of National Intelligence, 2006.

Quick, Michael. "Production, Dissemination, and Feedback." Presentation to the Fusion Center Leaders Program, U.S. Naval Postgraduate School, Monterey, CA, June 24, 2010.

Sullivan. Eileen. "Intel Centers Losing Anti-terror Focus." *The Associated Press*. November 29, 2007. http://www.usatoday.com/news/topstories/2007-11-28-3174603810_x.htm. Accessed December 10, 2007.

Tomachio, Jack. "Focus on Fusion Centers: A Progress Report." *Prepared Testimony before the Senate Committee on Homeland Security and Governmental Affairs Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration*. 110th Congress, 2nd Sess., April 17, 2008. http://www.fas.org/irp/congress/2008_hr/fusion.html. Accessed August 14, 2011.

Thomson, Bennie G., Peter T. King, Harman, Jane, Riechert, David G. (Subcommittee on intelligence, Information Sharing, and Terrorism Risk Assessment). "Committee Leaders Write Secretary Chertoff Regarding ITACG" to Michael Chertoff (Secretary, U.S. Department of Homeland Security). September 26, 2007. http://chsdemocrats.house.gov/SiteDocuments/20070927104243-98852.pdf. Accessed December 10, 2007.

Trella, Joe. "State Intelligence Fusion Centers: Recent State Actions." *Issue Brief*. July 7, 2005. Washington, DC: National Governors Association Center for Best Practices.

Tucker, David. *The Unconventional Threat to Homeland Security: An Overview*. Video lecture, Naval Post Graduate School, Monterey, CA, 2006.

"(U//FOUO) Concealment of Small Charge Improvised Explosive Devices." *Roll Call Release*. Washington, D.C.: Interagency Threat Assessment and Coordination Group, September 18, 2009.

U.S. Department of Homeland Security. "Activities & Programs: State and Local Fusion Centers." http://www.dhs.gov/xinfoshare/programs/gc_1156877184684.shtm. Accessed March 30, 2008.

———. "Fusion Center Fact Sheet." http://www.dhs.gov/files/programs/. Accessed February 12, 2011.

U.S. Department of Homeland Security and Global Justice Information Sharing Initiative. *DHS/DOJ Fusion Process Technical Assistance Program* 5th ed. Washington, D.C.: U.S. Department of Homeland Security and Global Justice Information Sharing Initiative, Department of Justice, 2010.

Wait, Patience. "Where the Data Meets the Road." *Government Computer News*. August 9, 2005. http://www.gcn.com/print/24_25/36781-1.html. Accessed March 2, 2008.

Watkins, Michael. *The First 90 Days: Critical Success Strategies for New Leaders At All Levels*. Boston, MA: Harvard Business School Press, 2003.

White House. *National Strategy for Information Sharing*. Washington, D.C.: White House, 2007.

———. "President Signs Intelligence Reform and Terrorism Prevention Act." December 17, 2004. http://www.whitehouse.gov/news/releases/2004/12/20041217-1.html. Accessed July 10, 2007.

World Health Organization. *Overview of Triangulation Methodology: Synthesis of Multiple Data Sources for Evaluation and Decision-making in HIV Epidemics, Based on Initial Experiences*. http://www.searo.who.int/LinkFiles/Facts_and_Figures_08Tri-Resource_Guide_Generalized.pdf. Accessed February 12, 2011.

Zupanc, Rudy. "Northeast Region Breakout Session." Presented at 2011 National Fusion Center Conference, Denver, CO, March 15–17, 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

3. Carl Walter
   ESRI
   Redlands, California

4. Keith Squires
   Utah Department of public Safety
   Salt Lake City, Utah

5. Edward Davis
   Boston Police Department
   Boston, Massachusetts

6. Jeff Carr
   Utah Department of Public Safety
   Salt Lake City, Utah

7. Daniel Linskey
   Boston Police Department
   Boston, Massachusetts

8. Paul Fitzgerald
   Boston Police Department
   Boston, Massachusetts