NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

STATE AND LOCAL INTELLIGENCE FUSION CENTERS: AN EVALUATIVE APPROACH IN MODELING A STATE FUSION CENTER

by

William A. Forsyth

September 2005

Thesis Advisor:	Robert Simeral
Second Reader:	Bill Pelfrey

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 2005	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE: State and Local Intelligence Fusion Centers: An Evaluative Approach in Modeling a State Fusion Center

5. FUNDING NUMBERS

6. AUTHOR(S) **William A. Forsyth**

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

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

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

In the final report on the attacks of September 11, 2001, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) found that the attacks were successful in part because information was not shared and analysis not pooled among the different agencies across all levels of government. Since that time, there have been significant strides to improve cooperation and close the intelligence gaps among the different intelligence and law enforcement services. Effective terrorism prevention, however, requires information and intelligence fusion as a cooperative process at all levels of government so that the flow of intelligence can be managed to support the identification of emerging threats to our homeland.

This thesis explains the value of a state/regional fusion center by examining three successful fusion centers in Arizona, Georgia, and Los Angeles. Recommendations from each agency on "lessons learned" as well as independent research have been provided to help state and local agencies develop their own fusion centers.

14. SUBJECT TERMS
Intelligence Fusion Center, Fusion Center Guidelines

15. NUMBER OF PAGES
110

16. PRICE CODE

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

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

STATE AND LOCAL INTELLIGENCE FUSION CENTERS: AN EVALUATIVE APPROACH IN MODELING A STATE FUSION CENTER

William A. Forsyth
Supervisory Special Agent, Federal Bureau of Investigation
B.A., University of Utah, 1985
M.A., Adams State College, 1991

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
September 2005

Author: William A. Forsyth

Approved by: Robert Simeral
Thesis Advisor

William Pelfrey
Second Reader

Douglas Porch
Chairman, National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

In the final report on the attacks of September 11, 2001, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) found that the attacks were successful in part because information was not shared and analysis not pooled among the different agencies across all levels of government. Since that time, there have been significant strides to improve cooperation and close the intelligence gaps among the different intelligence and law enforcement services. Effective terrorism prevention, however, requires information and intelligence fusion as a cooperative process at all levels of government so that the flow of intelligence can be managed to support the identification of emerging threats to our homeland.

This thesis explains the value of a state/regional fusion center by examining three successful fusion centers in Arizona, Georgia, and Los Angeles. Recommendations from each agency on "lessons learned," as well as independent research, have been provided to help state and local agencies develop their own fusion centers.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGEMENTS

When the famous astronaut Neil Armstrong made his first historic space flight in Gemini 8 (successfully docking two vehicles while in space), and had just reached the apex of his first orbit around earth, Houston Control asked him a series of questions, one of them being, "What does it feel like to be up in space?"; a reverent silence ensued and then Mr. Armstrong said, "Suddenly it's now!" Mr. Armstrong could not respond further to the question due to a series of additional questions that followed from Mission Control; he never elaborated on his statement.

Upon his safe landing back to earth, Mr. Armstrong was contacted by a reporter who had monitored the radio traffic between the space craft and the Control Center and asked, "What did you mean when you said, it was suddenly now?"

Mr. Armstrong answered by explaining that ever since he was a small boy he had dreamed of being an astronaut and imagined looking down on the earth from way up in space. Later, as a young adult, all of Armstrong's training and education was focused on that moment in time − when he would actually do what he had spent virtually his entire life preparing for − Mr. Armstrong said that when the question was asked, "How do you feel to be in space?", it hit him that the moment in time he had waited for was "suddenly here!" and he was a bit overwhelmed.

This thesis represents the last academic achievement necessary for completion of this Master's program. This effort is the culmination of an 18-month process that required focus, dedication, and sacrifice on the part of each student (and faculty member). Eighteen months does not seem like a long time, but much has happened personally, professionally, and family-wise. For me, this represents a dramatic conclusion of personal effort and training that (as Mr. Armstrong said) feels like "it's suddenly now!"

Like most significant events and achievements in my life, they are as much a result of collective efforts and support than an individual personal triumph. I cannot adequately express my thanks and gratitude to Dr. Chris Bellevita who, more than anyone else, was responsible for me being in this program. His encouragement and prodding got

me here. I thank him for his wonderful and wise insight into learning and the many helpful suggestions and "lessons learned" he shared during this program. He helped me through this whole process in ways that he will never know and helped me keep this endeavor in the proper perspective.

I must thank too, Dr. Paul Stockton, who has become such a good friend and advocate for the FBI in this program. Paul is a gifted teacher, animated and eloquent; his engaging style brings a wonderful perspective to his class discussions and forces thoughtful responses to difficult questions.

To my talented and insightful thesis advisors, Robert Simeral and Dr. Bill Pelfrey, thank you for your thoughts, suggestions, and long hours of work on my behalf to make this a paper worth reading.

To my class family of 0402, it has truly been a wonderful experience both personally and professionally to have made your acquaintance. Each of you has enriched my life and taught me so much about homeland security, leadership, and thinking "outside the box." I will truly miss our in-residence times together in the future, but will always treasure the memories we have made. Each of you are my friends forever, God bless you all in whatever roads you travel.

To my beautiful, wonderful wife of nearly 26 years, marrying you has been the single best decision I have made in my life. Thank you for all the selfless sacrifices you have cheerfully made on my behalf. Your support, encouragement and love have constantly sustained me all these years. Whatever my accomplishments have been, I owe them all to you. Thank you so much and I promise you more of my time.

To four of the best kids a father could ever hope for: Holly, Ben, Annie, and Chelsea! You have blessed my life in so many ways; thank you for your love, support, and friendship. You all are the product of a very special love, anticipation, and dreams come-true. I thank you for who you are and what you are becoming! I look forward to spending more time riding bikes, playing games, quiet talks alone, and just hanging out!

I. INTRODUCTION

During the events of September 11, 2001, law enforcement and intelligence agencies were thrust into a new mainstream of international terrorism unlike anything of the past. The need to collect, analyze, and disseminate good information across federal, state, and local jurisdictions became more important than ever. As a nation, we have done much to increase security, revise response protocols, and strengthen interagency relationships in order to defend ourselves and prepare for the next terrorist attack. There still remains a variety of issues that are unaddressed by most of our intelligence and law enforcement agencies in order for us to achieve the level of protection and security we desire, that is: the lack of actionable intelligence that is being shared at all levels.

Just after September 11, 2001, most state and local agencies looked to the federal government for support, leadership, and intelligence information that would be useful in defending ourselves against another terrorist attack. While the federal government has made efforts to improve the broader dissemination of information to state and local agencies, many still feel that the information provided by the federal government is dated, irrelevant to local issues, and generally not useful for local communities.

A. PURPOSE

Effective terrorism-related prevention, protection, preparedness, response, and recovery efforts depend on timely, accurate, and actionable information about whom the enemies are, where and how they operate, how they are supported, the targets the enemies intend to attack, and the method of attack they intend to use[1]. This thesis is intended to serve as a guide for efforts to:

- Identify rapidly both immediate and long-term threats;
- Identify persons involved in terrorism-related activities; and
- Guide the implementation of information-driven and risk-based prevention, response, and consequence management efforts.

[1] Gilmore Commission "Fourth Annual Report to the President and Congress," White House Office of the Press Secretary, December 15, 2002: 3.

Terrorism-related intelligence is derived by collecting, blending, analyzing, and evaluating relevant information from a broad array of sources on a continual basis. There is no single source for terrorism–related information. It can come through the efforts of the intelligence community; federal, state, tribal, and local law enforcement authorities; other government agencies (e.g., transportation, healthcare, general government), and the private sector (e.g., transportation, healthcare, financial, Internet/information technology).

For the most part, terrorism-related information has traditionally been collected outside of the United States. Typically, the collection of this type of information was viewed as a responsibility for the intelligence community and, therefore, there was little to no involvement by most state and local law enforcement entities. The attacks of September 11, 2001, however, taught us that those wanting to commit acts of terrorism may live in our local communities and be engaged in criminal and/or other suspicious activity as they plan attacks on targets within the United States and its territories.

Important intelligence that may forewarn of a future attack may be derived from information collected by state, tribal, and local government personnel through crime control and other routine activities and/or by people living and working in our local communities. Successful counterterrorism efforts require that federal, state, tribal, local, and private-sector entities have an effective information sharing and collaboration capability to ensure they can seamlessly collect, blend, analyze, disseminate, and use information regarding threats, vulnerabilities, and consequences in support of prevention, response, and consequence management efforts.

The President and the U.S. Congress have directed that an information sharing environment (ISE) be created in the next two years to facilitate information sharing and collaboration activities within the Federal Government (horizontally) and between Federal, State, tribal, local, and private-sector entities (vertically). The concept of intelligence/information fusion has emerged as the fundamental process (or processes) to facilitate the sharing of homeland security related information and intelligence at a national level, and, therefore, has become a guiding principle in defining the ISE.[2]

[2] United States Department of Homeland Security, "Presidential Directive (HSPD) #8," White House Office of the Press Secretary, December 17, 2003, paragraph (c).

Given that state centers specifically designed to facilitate such intelligence exchange do not currently exist in any routine manner, this thesis has been prepared as guidance for state agencies contemplating such an enterprise. These intelligence fusion centers should be designed to collect, analyze, and disseminate information to determine the credibility of terrorist threats and gauge their potential impact in their state or area. Based on this analysis of threat information, these fusion centers provide local and state policymakers and public safety officials with a variety of intelligence products useful at all stages of emergency operations.

B. IMPORTANCE OF RESEARCH

The importance of this research is incredibly self evident because terrorism prevention consists of collective activities that support efforts to detect, protect against, and disrupt terrorist threats or attacks against the United States and its interests. Preventing a terrorist attack means taking appropriate actions to avoid an incident or to intervene to stop an incident from occurring.

It is impossible to protect every potential target in our communities from every conceivable method of attack. It is also unrealistic to believe that jurisdictions will possess the capacity to identify and arrest every person involved in terrorism related activity or planning. Therefore, to be effective, prevention efforts must be intelligence-driven, adaptable, and multifaceted to meet the needs of defending our homeland. Developing efficient and operationally sound intelligence fusion centers at the local level have appeared to be more effective than other conventional means in protecting national assets. These centers, when properly organized can facilitate effective prevention efforts that depend on the ability of state, local, and tribal governments to collect, analyze, and disseminate homeland security related intelligence.[3]

[3] United States Department of Homeland Security, "The National Response Plan," White House Office of the Press Secretary, December 2004, 16.

THIS PAGE INTENTIONALLY LEFT BLANK

II. WHY THE NEED FOR FUSION CENTERS IN THE UNITED STATES TODAY?

The events leading to the attacks of September 11, 2001, not only highlighted America's lack of coordination within the intelligence community but it also reminded us that a terrorist attack in the United States was not a new phenomenon. American law enforcement and intelligence agencies had not taken seriously previous attacks by our enemies and we paid a great price; something needed to change. Since the 9/11 attacks, many Congressional, governmental, and private sector groups have met to discuss, analyze, and opine on what went wrong and who was to blame for the attacks. The 9/11 Commission and the Gilmore Commission Reports both articulated that "there lacks an acceptable level of awareness, prevention, preparedness, response, and recovery capabilities to cope with the uncertain and ambiguous threat of terrorism…"[4]

While no known international terrorist attacks have occurred in the United States since September 11, 2001, terrorist networks have carried out many attacks abroad, including the 2002 bombings in Bali, the 2002 bombing of a French Oil Tanker in Yemen, and the 2004 coordinated bombing of four commuter trains in Madrid. The Al-Qaeda terrorist network has openly called for a jihad against the United States and its citizens around the world, with all of this to consider, it is only logical to accept that more attacks within the United States are imminent.

International terrorist groups are not our only adversaries; we have to consider also domestic terrorists groups, which have different purposes and agendas but still create the same political and economic disruption in our country as the international terrorist groups. We are well aware that both domestic and international terrorist cells are living within the boundaries our own towns and cities across America. If our adversaries are living among us, watching and waiting to act, we can not rely solely on bits of information (often dated) provided by federal agencies that do not have the ability to determine the timely value of the information at the local or regional level. Conversely,

[4] Gilmore Commission, "Fourth Annual Report to the President and Congress," White House Office of the Press Secretary, December 15, 2002, 36.

federal intelligence and law enforcement agencies can benefit greatly from information provided by state and local entities. A unified and coordinated integration of the two philosophies are needed. Webster's Dictionary defines integration as … "the forming, coordinating, and blending into a functioning and unified whole."[5] This is the type of spirited cooperation we need to fight terrorism in the United States today.

The United States is currently the most technologically advanced, economically stable, and militarily superior country in the world and yet we don't utilize our collective capacity to its fullest extent. If one considers the possibilities of unifying the resources (operational and intelligence-wise) of state and local law enforcement, federal law enforcement, state and federal intelligence agencies and bureaus, military, fire, EMS, public health, and private sector enterprises, there is nothing that could not be done to make our country more safe and free of terrorism. With this type of integrated cooperation, the mistakes surrounding the events of 9/11 can be eliminated. There has not been a more urgent need in our recent national history when we have needed to become more united in our homeland security efforts. The preventative flow of intelligence data at all levels, from threat analysis to vulnerability assessment and response, is connected through an integrated, comprehensive all-agency, all-government, and all-sector system that is timely, useful, and proactive on a local, state, and national level. The enlistment of all our available resources, including the contributions of state and local governments providing inputs into this intelligence system, will help toward this end.

This idea of bringing all of the law enforcement, intelligence, military, and private sector agencies together at one area location seems to be of more benefit to state and local agencies and has proven to be less difficult to define, establish, and operate than a national level center.

In the analysis of the centers below, the writer has avoided the terms "best practices and best methods" because those terms are so relative. What works well in Los Angeles may not work well in Atlanta. Instead, each of the three centers will be

[5] Merriam-Webster, *Merriam-Webster's Collegiate Dictionary (*Merriam-Webster, Inc., Springfield, Massachusetts, 2003), 650.

highlighted and operational concepts and reasoning will be shared, each to be evaluated by the reader for their own utility. There will be a recommendation chapter that will suggest what is needed (at a minimum) in order to establish a well defined and operationally productive center. These suggestions are provided as guidance for states and localities to use as they consider establishing such centers but should not be considered as the "only way" a center can be created.

The document that follows is a look at three highly successful and productive intelligence centers that each focus on intelligence gathering and sharing. Each has a unique history and structure but they share a common goal: to facilitate timely and actionable information and intelligence sharing at all appropriate levels of government. .

A. FUSION CENTER INTERVIEWS

Several states within the America currently have some form of information fusion processing. I have chosen to examine three centers that have been pioneers in establishing state fusion centers and have proven track records of success in this field. This, however, does not mean that other states do not also have excellent information fusion centers and information sharing processes worthy of emulation. I have chosen the Arizona Counter Terrorism Intelligence Center (ACTIC), The Georgia Information Sharing and Analysis Center (GISAC), and the Terrorism Early Warning Center (TEW) in Los Angeles, California, as my benchmarks for evaluation. Each center is excellently run, monitored, and evaluated for efficiency and quality in the information sharing process. As I began the "inspection process" with each center, I started with asking the following set of standardized questions of each to get an appreciation of why the center was created and how it operates:

- Why did your state feel compelled to create and fund an information fusion center such as this?
- When information comes into the center, who correlates or triages the information? What are the criteria for this? How is information/intelligence categorized and shared?
- What is the information architecture at your center? What happens to the information from the time it enters the center to the time it leaves?
- Who classifies and/or re-classifies information at your center? What are the criteria?

- How is classified information received, handled, and disseminated? Is there a "Tear-Line" policy? What are the dissemination guidelines and policies for your center?
- What agencies participate in your center? Who are the stakeholders/recipients? What is done with information developed that is not related to your geographical area?
- Is your center operational 24/7? If not, what operational procedures are in place for stakeholders to provide or access information at your center "after hours"?
- What kind of intelligence products does your center produce? How often are they offered and how are they disseminated?
- What type of data bases and computerized connectivity with other agencies do you have?
- What poses the biggest challenge at your center? What do you need to make your center more effective?

III. INTELLIGENCE GATHERING, ANALYSIS, AND INFORMATION SHARING− HOW IS IT WORKING? A LOOK AT:

- The Arizona Counter Terrorism Information Center (ACTIC)
- Georgia Information Sharing and Analysis Center (GISAC)
- Terrorism Early Warning Center (TEW)

A. THE ARIZONA COUNTER TERRORISM INFORMATION CENTER (ACTIC)

On October 1, 2004, the Arizona Counter Terrorism Information Center (ACTIC) was officially opened and began business as a cross-jurisdictional Watch Center focused on enhancing information and intelligence sharing throughout the state of Arizona.[6] The center was a gubernatorial response to the horrific attacks of 9/11 and the subsequent change in which U.S. law enforcement and the intelligence community of the United States looked at national and domestic security matters. Indeed, not only the events of 9/11, but the many national and international events in the world have caused the U.S. Government to re-think the way it looks at homeland security and defense, foreign policy, and the relationships between local, state, and federal agencies.

One significant lesson learned from the events of the last 3 1/2 years is that state and local agencies are significant partners in homeland security. The new "grass roots" war against terrorism has to include more connectivity between local, state, and federal agencies combining resources and intelligence for the good of all to provide the level of national and domestic security demanded by the people of the United States.[7]

Immediately following the attacks of 9/11, Arizona, like many other states, had to rely on pre-existing emergency response protocols and information infrastructures to address local needs. That infrastructure at the time was based on an emergency response architecture based on the national threat levels of the 1990's and included the following:

---

[6] Lori Norris (Lieutenant, Arizona Department of Public Safety), interview with author, Phoenix, Az., February 16, 2005.

[7] The 911 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (W.W. Norton & Company, Inc., New York, 2004), 353-356.

- In 1997, the Division of Emergency Management (DEMA) worked with the Department of Public Safety (DPS) to establish a Domestic Preparedness Task Force. The group consisted of representatives from more than 40 public and private entities that convened to review appropriate response and recovery plans through out the state.
- The State of Arizona also established a State Emergency Operations Center (EOC) within DEMA that can be fully activated within one hour (as it was during 9/11). The EOC brings together all relevant public and private entities to address emergency situations.
- In 1998, DEMA developed a formal Emergency Response and Recovery Plan for the entire State of Arizona. The plan was developed as a comprehensive brake-down of the responsibilities of each state agency in a major disaster. The plan was developed with the expectation that it would be "practiced" prior to a real emergency or actual crisis event to identify weakness and recommend improvements.[8]

1. Arizona's Actions Following 9/11

Just after the attacks, Arizona officials immediately took steps to bolster their state's emergency preparedness and "brace" themselves for possible additional attacks. DPS activated its Domestic Preparedness Operations Center and established a 24 hour tip line for individuals to report suspicious activities or concerns. Additionally, DPS created a secure web-site as a vehicle to share information and updates with local and county authorities, dedicated additional intelligence analysts and investigators to collect and analyze terrorism related information, and appointed more personnel to the FBI's Joint Terrorism Task Force (JTTF).[9]

The U.S. Attorney General (Ashcroft) instructed each United States Attorney (USA) to establish multi-jurisdictional anti-terrorism task forces. In support of this request, the Arizona National Guard in Phoenix and Tucson began flying support missions for air combat patrols. Also, troops were sent to provide additional security at

---

[8] Janet Napolitano , " Securing Arizona; A Roadmap for Arizona Homeland Security," Arizona Governor's Office, April 23, 2003, www.governor.state.az.us/press/Securing_Arizona.pdf , accessed on July 5, 2005.

[9] 911 Commission Report, *Final Report of the National Commission on Terrorist Attacks Upon the United States* (W.W. Norton & Company, Inc., New York, 2004), 353-356.

the Hoover Dam and 10 of Arizona's major airports. Specially trained ANG and DPS personnel were also sent to provide additional security at the Palo Verde Nuclear Plant.[10]

To better organize the state's efforts, then Governor Jane Dee Hull, in 2001, appointed two members of her staff to better coordinate Arizona's contributions to homeland security by forming a Homeland Security Council. The main mission of this new council was to oversee all homeland security activities in the state and also develop and implement new and effective homeland security policies.

In December of 2002, Governor-elect Janet Napolitano conducted a thorough review of Arizona's homeland security readiness. This review found that while the state of Arizona took appropriate steps in responding to the events of 9/11, a number of critical issues impeded the state's ability to adequately address issues of homeland security on a long term basis. Some of the critical issues were as follows:

- Despite the attention from the Governor's Office with the appointment of two homeland security coordinators and the establishment of the new Homeland Security Coordinating Council, there was no single person or office responsible for organizing the statewide efforts to detect, prevent, and respond to terrorist attacks or other critical incidents;
- The state lacked a long term homeland security strategic plan that provided a clear vision of how it will work with county, local, and tribal governments to detect, prevent, and respond to acts of terrorism and other critical incidents;
- The data information systems used by federal, state, local, and tribal public safety entities were not linked and therefore unable to pass valuable information to identify trends and suspicious circumstances that may be indicative of an emerging terrorist threat or attack.
- The state had under-funded resources for anti-terrorism initiatives;
- The state did not have an electronic disease surveillance system capable of identifying an emerging biological or chemical weapons attack through the analysis of emergency room and other relevant data;

[10] Janet Napolitano, "Securing Arizona; A Roadmap for Arizona Homeland Security," Arizona Governor's Office, April 23, 2003,www.governor.state.az.us/press/Securing_Arizona.pdf , accessed on July 5, 2005.

- First responder's throughout the state all use different and independent radio systems that operate on different radio frequencies and do not allow them to communicate between agencies.[11]

Governor Napolitano's review also found that there was no comprehensive plan that focused on homeland security initiatives focusing on U.S. - Mexican Border issues which are considered a major vulnerability for the state.

Based on these findings, the State of Arizona developed a plan of action for establishing a long-term, fiscally prudent approach to homeland security. This plan provided a framework for enhancing the state's ability to detect, prevent, and respond to future acts of terrorism (or other critical incidents); it will also be a useful tool for system planning, future technology acquisitions and prioritizing and coordinating requests for state and federal funding.[12]

2. Improving Arizona's Ability to Respond to Attack

After reviewing the report, Governor Napolitano directed the state's Homeland Security Coordinating Council to implement a number of action items to correct the noted deficiencies previously identified, below are several that pertain to the ACTIC:

> Action Item #1 The state will appoint a Homeland Security Director to coordinate statewide efforts to detect, prevent, and respond to acts of terrorism and other critical incidents and expand the role of county, local, and tribal officials in strategic planning activities.

Despite the appointment of two homeland security coordinators and a Homeland Security Coordinating Council by Governor Hull, there was no single person or office held accountable for organizing the statewide efforts associated with terrorism prevention or response. This has negatively affected Arizona's ability to coordinate the various operational and strategic planning efforts critical to the state's homeland security mission and to develop and communicate a clear strategic vision pertaining to homeland security for county and local entities.

---

11 Janet Napolitano, "Securing Arizona; A Roadmap for Arizona Homeland Security," Arizona Governor's Office, April 23, 2003, www.governor.state.az.us/press/Securing_Arizona.pdf , accessed on July 5, 2005.

12 Ibid., 9-11.

In an effort to improve the coordination between all levels of government and the private sector, Arizona has established a permanent position of Homeland Security Director to be an advisor to the governor on homeland security issues and oversee the state's overall homeland security mission. The governor has also appointed a new Homeland Security Coordinating Council that will ensure representation of local, tribal, and private sector officials in homeland security strategic planning activities.

Action Item #2 The State will update and enhance its Emergency Response and Recovery Plan

In accordance with Arizona Revised Statues (ARS), title 26, Chapter 2, Article 1, the State of Arizona is required to prepare to respond to emergencies and disasters in order to save lives and protect public health and property. In the late 1990s the state did develop such a plan that addressed such issues as mutual aid, financial management, responsibilities of state departments, and transportation. While the state had some mention and description for response to a number of specific hazardous situations (such as bio-terrorism and WMD) the plan lacked specificity and clarity for roles and responsibilities of the state. The plan also lacked clarity as to how many of the stakeholders in the state would be linked into this plan along with other state agencies and tribal governments.

The governor of Arizona therefore, mandated an update on the state's emergency response plan and directed several initiatives requiring annual evaluations and review of the state's readiness for such an event. Among those mentioned in the directive was a comprehensive statewide threat and vulnerability assessment that identifies potential targets and areas of concern. This assessment includes an analysis of potential targets for attack, such as buildings, power plants, transportation centers, and fuel storage facilities, as well as detailed response plans that include how federal, state, local, and tribal agencies will work together to respond to critical and WMD incidents. To facilitate this plan, the state focused its attention on developing a way of sharing relevant portions of the assessment on an ongoing basis with state, local, tribal, and private entities so that critical assets and infrastructures can be protected.

> Action #3 The State of Arizona will take steps to establish a statewide integrated justice system that links the information systems used by federal, state, local, and tribal criminal justice entities in such a way to support the identification of emerging terrorism related trends.

The state set improving information technology and infrastructure that supports criminal justice activities as a top priority. The state planners recognized that rapid, consistent access to informational databases at all levels of government was critical to accomplish this goal. Currently, over thirty-eight states in the United States have begun efforts to create "integrated justice information systems" that link various components of the criminal justice system (police, courts, corrections) to each other that allows for the rapid transfer of information about criminal activities and the places they occur. Law enforcement officials and policy makers will be able to identify suspicious and unusual trends and develop information-driven trends, which allow for information-driven strategies that effectively target people and criminal activities.[13]

It will be a priority of the state to link the independent information systems used by city, county, tribal, and state criminal justice entities to allow for the rapid flow of information about the people who commit crimes and the places they occur. This information sharing will support efforts by law enforcement to identify suspicious trends and effectively target those involved in criminal activity. Public safety information links is a good start but Arizona wanted additional connectivity with other government systems including those that support transportation, public health, social services, and public utilities. State, local, and tribal agencies work with one another daily but often this work is stove piped in individual agency systems and policy measures. As part of the homeland security measure, the State of Arizona began taking steps to link public safety information systems with non-public safety information systems in order to:

- Support multi-disciplinary, proactive, and community focused activities;
- Provide predictive analysis and capabilities; and
- Improve the delivery of emergency and non emergency services.[14]

---

[13] Janet Napolitano, "Securing Arizona; A Roadmap for Arizona Homeland Security," Arizona Governor's Office, April 23, 2003, www.governor.state.az.us/press/Securing_Arizona.pdf , accessed on July 5, 2005.

[14] Ibid.

Action Item # 4 The state will establish a 24-hour intelligence and information analysis center that will serve as a central hub to facilitate the collection, analysis, and dissemination of crime and terrorism related information.

One of the most serious challenges affecting homeland security is the timely exchange of intelligence and critical information among local, state, and federal agencies. Accurate and timely intelligence is the key to the most fundamental responsibility of a government protecting its citizens and critical infrastructures. Determined to ensure this free interchange of information, the Arizona Department of Public Safety (DPS) was designated by the FBI and the U.S. Attorney's Office to be the central point of disseminating information generated by the federal agencies.

Since 9/11, DPS continued this service to various agencies throughout Arizona by email, fax, National Law Enforcement Telecommunications System (NLETS) and a secure website. As a result, DPS expanded its capabilities to provide additional support to a growing stakeholder base. To accommodate this expanded duty, DPS immediately took steps to establish the Arizona Counter-Terrorism Information Center (ACTIC). This center is operating on a twenty-four hour basis providing intelligence and support to local, state, and federal law enforcement agencies as well as other agencies addressing homeland security needs. The ACTIC has a focused responsibility for the following:

- Providing tactical and strategic intelligence collection, analysis, and dissemination support to local, state, and federal law enforcement agencies;
- Maintaining and disseminating an on-going threat analysis for the State of Arizona and its critical infrastructure;
- Providing informational support to the Governor and other critical governmental leaders;
- Maintaining a secure web site to disseminate intelligence and critical information accessible to all law enforcement and first responder agencies;
- Maintaining the Anti-Terrorism Information Exchange (ATIX) secure web site portal for the dissemination and exchange of information to law enforcement and public and private stakeholder agencies that support homeland security efforts;

- Functioning as the state's central point of dissemination for homeland security threat level conditions and other information generated by the FBI, U.S. Attorney's Office and other state, local, tribal, and federal agencies;
- Maintaining and updating the necessary databases to support on-going investigations;
- Maintaining contact with the FBI Joint Terrorism Task Force, the U. S. Attorney's Office of Anti-Terrorism Task Force, and other state, local, and federal law enforcement agencies in on-going investigations;
- Providing necessary training on intelligence function and the role of law enforcement and private citizenry in guarding against terrorist attacks.

The ACTIC was developed to meet the demands of the above action items and be more responsive to the needs of law enforcement in its fight to protect America's homeland. Like all of the existing information/intelligence fusion centers operating in the country today, the ACTIC is a work in progress. The ACTIC is designed to be a true cross-jurisdictional partnership, integrating local, state, and federal law enforcement and first responders, emergency management and, when appropriate, the private sector.

3. Mission Statement

The mission of the ACTIC is to protect the citizens and critical infrastructures of Arizona by enhancing intelligence and domestic preparedness operations for all local, state, and federal law enforcement agencies. Mission execution will be guided by the understanding the key to effectiveness is the development and sharing of information between participants to the fullest extent as is permitted by law or agency policy.[15]

4. How the ACTIC Works

a. Organizational Structure

The ACTIC is comprised of integrated groups (squads) consisting of sworn (law enforcement) and non-sworn (analytical) personnel from participating local, state, and federal agencies who have been assigned to a specific terrorism or criminal category. The operational lay-out of the ACTIC is divided into two parts as mandated by federal guidelines. The first area consists of local, state, and federal law enforcement agency personnel on temporary duty assignments with direct liaison to their home

[15] Arizona Counter-Terrorism Information Center Information Bulletin, "Arizona Intelligence Bulletin Report," November 2004, 1.

agency. These assignments are critical as these personnel provide first hand and timely information that address community concerns utilizing ACTIC resources. The people assigned to the "local side of the ACTIC" provide and important local connection with state agencies that allows for information sharing in a two sided fashion.

The second side of the ACTIC is comprised of personnel assigned to the FBI Joint Terrorism Task Force (JTTF). The members of the JTTF are also individuals who come from local, state, and federal agencies and who also have additional training and clearances to work with and analyze classified information. The JTTF is also organized into squads by investigative category. Personnel assigned to the JTTF are sworn Agents, Detectives, and Analysts with security clearances based on the needs and priorities of the participating agency and the JTTF. The JTTF allows for "High-Side information" (classified) to be collected, analyzed, "scrubbed", and then disseminated for local use. Classified information needing to be passed to the other side is done so by members with clearances and have a need to know. Over 95% of the information received or collected, however is non-classified information. The JTTF side of the ACTIC allows for the important federal and national information sharing to occur that has direct local and state impact for the State of Arizona.

The ACTIC is organized into two operational components that coincide with overall mission responsibilities. The first component is criminal intelligence which focuses its attention on crime prevention. The intelligence side of the ACTIC utilizes its information gathering, analysis, and dissemination efforts in a proactive way so as to assess, interdict, prevent, and discourage criminal activities. This proactive approach also has a huge counter terrorism focus as well which involves information gathering from a variety of sources including the collection of "soft" information. The ACTIC defines soft information as information which typically can't be used in court because it is derived from hearsay, rumors, anonymous tips, suggestions, and hunches that are all used in the development of intelligence files. Many times, this soft information is developed to a point where a criminal or terrorist investigation can be opened.[16]

---

16 Arizona Counter-Terrorism Information Center Information Bulletin, "Arizona Intelligence Bulletin Report," November 2004, 1.

The investigative component acts in a strictly reactive mode designed to arrest and prosecute the criminal offender. The investigative side focuses its attention on identifying suspects and witnesses, recovering stolen property, and procuring viable evidence for court presentation. This investigative side focuses its attention on the more immediate, short term criminal issues affecting state and local jurisdictions in Arizona. Both sides of the ACTIC work in close harmony with the Arizona FBI Field Office squads working parallel federal issues or where a particular criminal matter could best be prosecuted either federally or locally.

The ACTIC operates in a non-classified information sharing mode. Generally, information is characterized as "For Official use Only" (FOUO) or "Law Enforcement Sensitive." Sensitive or classified information is vetted through the local FBI Joint Terrorism Task Force (JTTF) to members of the ACTIC with appropriate clearances. Classified information needing to be disseminated to a broad based law enforcement population is "scrubbed" in the JTTF and appropriately disseminated in as timely a fashion as can be done. The ACTIC is divided into various sections to address a specific intelligence/information functions, the following are the ones most useful in information sharing:

b. Intake/Watch Section

The Intake/Watch Section is the central location for all information coming into the ACTIC. In conception, this section is designed to be a twenty-four hour, seven-day operating facility to take all incoming information. Currently, this section is not operational 24/7 but is moving quickly in that direction to provide more immediate response to local, state, and federal shareholders.

ACTIC managers require all personnel to serve rotating shifts in the Intake/Watch Section to educate personnel on the over-all mission, role, and responsibilities of the ACTIC. Assigned personnel are responsible for receiving and routing telephone calls, processing mail, managing informal and formal requests for information, and inputting information into the ACTIC database. The Intake/Watch personnel also promote information sharing using state of the art technology, databases to support law enforcement activities. These people working in this section are also

responsible monitoring all sources of media, intelligence sources, database maintenance, and homeland security resources for the immediate and timely identification of incidents and patterns affecting Arizona.[17]

c. Criminal Investigations Research Unit (CIRU)

The CIRU functions as a gateway to a variety of law enforcement and commercial data bases as a resource for all shareholders. This unit queries open source documents, proprietary, law enforcement, and classified information that can be exploited in the development and management of general intelligence, the detection and prevention of terrorism, the investigation of criminal offenses and the identification of individuals. The CIRU is the heart of the intelligence search engine at the ACTIC.[18]

d. The Field Intelligence Group (FIG)

The FIG serves as a central liaison point for coordination of local intelligence and investigative matters between federal, state, and local agencies. The FIG serves as a bridge between the federal and local law enforcement investigations. The FIG, as currently organized, is law enforcement based and focuses on issues that primarily have an FBI nexus. The purpose of the Phoenix FBI's FIG is to support the ACTIC as a centralized intelligence management structure in addressing the intelligence needs and priorities of the geographical boundaries of the Phoenix FBI Field Office. One of the main functions of the Phoenix FIG is to provide analytical reports to State and Federal Executive Managers, FBI Headquarters, and the U.S. Intelligence Community, as well as, local, state, federal, and foreign law enforcement agencies.

It is hoped that the information provided will help policy makers and senior state and local officials with appropriate decision-making tools. This mission is accomplished in a coordinated and synchronized approach using the following six step method: 1.) **Requirements** are identified information needs, what we must know to safeguard the nation. 2.) **Planning and Direction** is the management of the entire effort, from identifying the need for information to delivering an intelligence product to a

---

[17] Gil Orantego (FBI Joint Terrorism Task Force Supervisor), interview with author, Phoenix, Az, March 16, 2005.

[18] Ibid.

consumer. 3.) **Collection** is the gathering of raw information based on requirements. 4.) **Processing and Exploitation** involves converting the vast amount of information collected to a form usable by analysts. 5.) **Analysis and Production** is the conversion of raw information into intelligence. 6.) **Dissemination** is the last step, which directly responds to the first cycle, is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements.[19]

e. Analytical Units

The primary function of the analytical units is to conduct intelligence-based assessments of threats and vulnerabilities within the borders of Arizona. The analytical unit identifies and monitors known and suspected terrorists and groups, analyze terrorist activities and produce strategic and action-oriented intelligence data for the benefit of policy makers, administrators and managers. Analysts contribute to daily intelligence reports and routinely publish their findings for state-wide law enforcement distribution. All of the personnel assigned to these units are screened and vetted for the necessary security clearances allowing for a coordinated and collaborative exchange. Secret and Top Secret are the highest classifications needed but most information collected and disseminated is at the non-classified, law enforcement sensitive level.

The Analytical section of the ACTIC is divided into two parts: **1.) Strategic Analysis**−this group researches, studies, and publishes analytical results for long term planning of ACTIC operations, and intelligence and investigative objectives. **2.) Tactical Analysis** – This group researches and analyzes information with/for on-going intelligence and investigative objectives of the operational squads assigned to the ACTIC and to the other investigative bureaus of the Arizona DPS. These analysts, along with other law enforcement personnel try to identify any potential terrorism link in the other criminal activities being investigated. Some of the criminal activity leading to such a connection includes auto theft, fraud, identity theft, narcotics trafficking, gambling, organized crime, and financial crimes.

[19] Gil Orantego (FBI JTTF Supervisor), interview with author, Phoenix, Az, March 16, 2005.

f. Joint Terrorism Task Force (JTTF)

The FBI's JTTF in Arizona is responsible for providing investigative and operational support for terrorism cases. The JTTF accomplishes that mission by joining federal, state, and local law enforcement agencies in a coordinated manner to detect, deter, prevent, and investigate acts of terrorism that threaten the United States national interest at home or abroad. The JTTF is an integral part of the ACTIC and is housed within the same building. The JTTF is the main repository for any classified information received and can "scrub" this information making it suitable for appropriate dissemination to units within the ACTIC.

g. Intelligence Squads

The intelligence squads are part of an ad hoc task force comprised of state, local, and federal law enforcement analysts. They are responsible for providing follow-up support to all information received into the ACTIC. In addition, each agency representative is tasked with coordinating with their home agency to identify any homeland security concerns within their communities. These squads, in coordination with the appropriate Analytical Unit, monitor all terrorist and extremist organizations that impact the State of Arizona, its citizens, and the nation. Analysts in this squad are responsible for the development of organizational profiles on all terrorist organizations that impact the State of Arizona and the nation.

The ACTIC also has sub-intelligence squads which include: 1.) **Critical Infrastructure Assignments** refers to personnel assigned to address critical infrastructure concerns. They will identify, monitor, and conduct risk and vulnerability assessments of the various infrastructure sites within the State of Arizona. 2.) **Public Health and Biological Threats Assignments** are personnel assigned to this sub-unit to focus on identifying, monitoring, and conducting risk and vulnerability assessments concerning public health threats posed by chemical and biological hazards. This group also focuses on detecting and preventing terrorists attacks that involve or threaten the use of chemical or biological weapons. This sub-unit works closely with the Arizona Department of Emergency Management, the Center for Disease Control, the Poison

Control Center, public health agencies, and private health care providers to accomplish this task.

h. Hazardous Material Weapons of Mass Destruction Unit (HazMatWMD)

The HazMat/WMD Unit was created to identify, monitor, and conduct risk and vulnerability assessments pertaining to the movement, storage, and destruction of weapons of mass destruction and radiological material within the State of Arizona. This Unit has responsibility for detecting and preventing terrorist acts that use or threatens the use of WMDs. All personnel assigned to the HazMat/WMD Unit have obtained all necessary security clearances to coordinate and share information across units.

i. Liaison Squad

The Liaison Unit is responsible for establishing and developing liaison contact with local, state, federal, and private agencies and promoting ACTIC's purpose and mission. This Unit also provides training on the method and benefits of passing information to the Center and suggestions on how to combat terrorist activities and criminal acts. The Liaison Unit also has a sub-section which coordinates and tracks ACTIC automation systems and training in terrorism prevention and ensures that all ACTIC personnel are current in training and certifications.[20]

All of the units, sections, and personnel at the ACTIC are organized and trained for one function; to work in harmony with existing law enforcement and private sector agencies in protecting the citizens of Arizona against terrorist attacks. Like all new endeavors, there are always "rough edges" to smooth out before the system is working right, the ACTIC has put together a well thought out and organized approach to fighting crime and terror, an excellent model for any state to follow.

j. ACTIC Information Flow

Information at the ACTIC is collected and disseminated using a web based program called the "Watch Log Entry System" (WLE) that manages the collection, assignment, update, and disposition of incoming information and events. The WLE distributes a threat warning and report feature to all approved shareholders within the

[20] Lori Norris (Lieutenant, Arizona Department of Public Safety), interview with author, Phoenix, Az, February 16, 2005.

state of Arizona. This particular feature of WLE allows for better coordination of information and resources within the statewide public safety community for a faster and more integrated response. The ACTIC-WLE improves the overall availability, quality, and quantity of watch and threat information available throughout the Arizona Public Safety community.

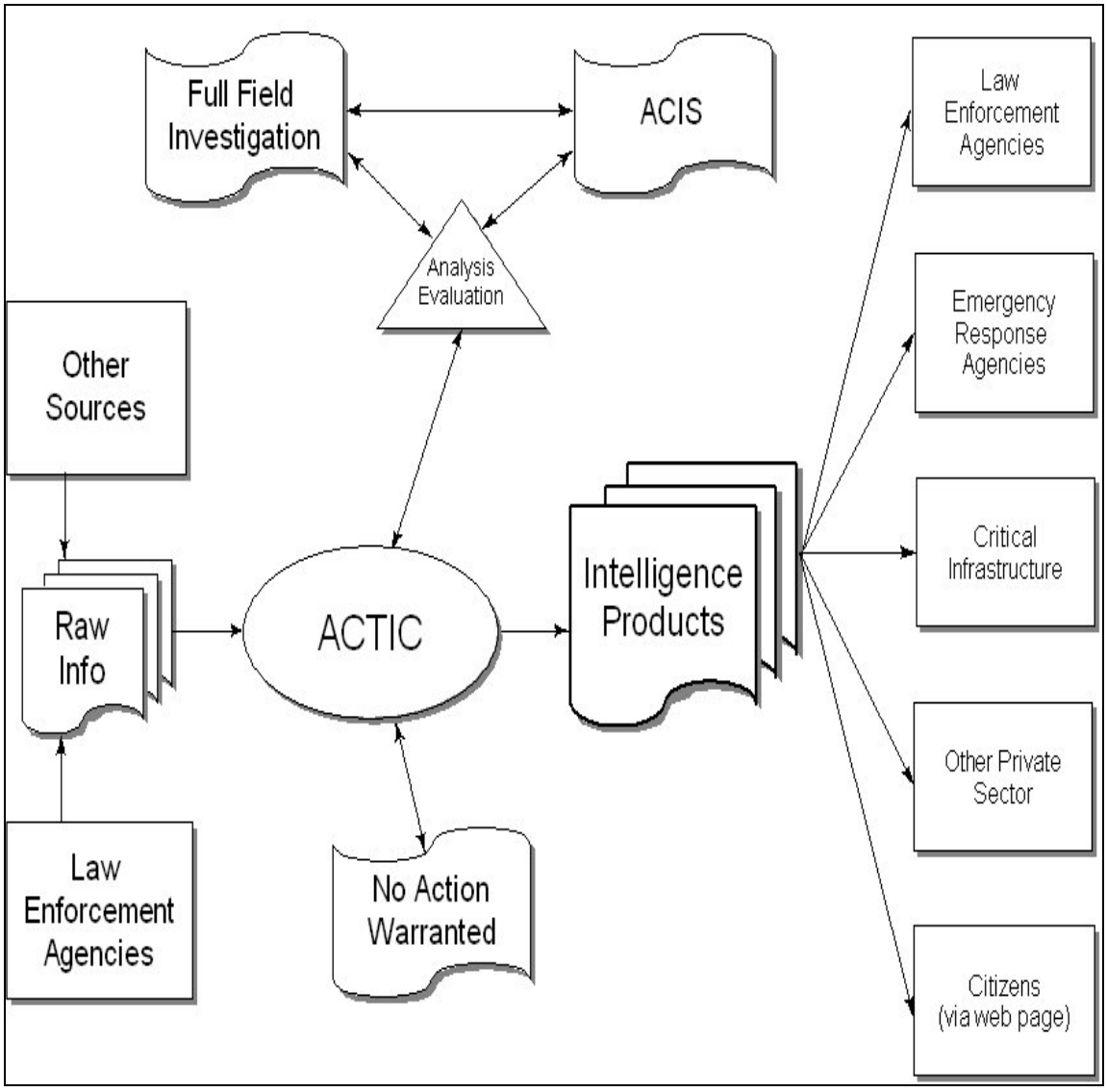


Figure 1. Provided by the Arizona Counter Terrorism Information Center, this is an informational flow chart design for the ACTIC depicting how information is accepted and handled at the center.

k. WLE Roles/Responsibilities

Intake Personnel − Personnel who creates a watch log event using incoming information received from law enforcement, general public referrals, media, and private sector sources. The intake personnel enter the information into the data base which then makes the information searchable. Multiple intake personnel can up-date or modify information from other intake personnel.

Operations Supervisor − This position supervises all responsibility for the watch log events relating to their area of expertise. This is the only person who has authority to create a watch log event, assign an event to another supervisor, refer to another shareholder or agency, and authorize an intelligence report to be written from a watch log event(s).

General User − Any authorized ACTIC member is a general user and has the ability to pass, receive, update, or report on a watch log event. A general user can also refer an event to another general user and create an intelligence report based on a watch log event.[21]

l. WLE Events

Drafts − The initial state of a watch log event created by intake personnel or an operational supervisor. A new watch log event still being formulated with initial information and details is considered a "draft." Events in the draft stage are not searchable and only the intake personnel or operations supervisors can view a draft. Once all of the initial information and details have been gathered and reported, the event can then be submitted into the system. The submit action moves an event into an "open state" which then makes it searchable for shareholders.

Open − A watch log event that contains all of the initial incident information and has been submitted into the system by the intake personnel or supervisors. General users/shareholders are able to modify or up-date any part of the open watch log event.

---

[21] Arizona Counter Terrorism Information Center Training Class, "Watch Log Entry System Training Class," v1.0, Lockheed Martin, November 1, 2004, 6-7.

Locked − A completed watch log event that cannot be updated. Events that are in the "locked" mode can only have information added if the operations supervisor unlocks the event and then submits the new information.[22]

As a nation, the United States has a unilateral commitment to the safety of the country and its citizenry. To accomplish this task, federal, state, and local governments, law enforcement, and state agencies (public and private) must all work together to eliminate the need of utilizing ineffective and random prevention strategies and to focus on new ways to address national security.

The State of Arizona has made a commitment to work with city, county, local tribal and private sector entities and to put into place the necessary information, communications technology, and operational strategies that support the government's efforts to keep Americans safe. The state leadership of Arizona has worked hard in developing a statewide strategy to protect its people utilizing the cooperative efforts of all of the groups previously mentioned.[23] The ACTIC plays a major part in this objective, judging from its operational effectiveness, the ACTIC well serves the people of Arizona and is a worthy model for other states, contemplating the development such a center.

B. THE GEORGIA INFORMATION SHARING AND ANALYSIS CENTER (GISAC)

Like most states in the after-math of September 11, 2001, state leaders looked at their own vulnerabilities and matched those against their available resources. In response to the terrorist attacks, Georgia's Governor Roy Barnes created the Georgia Homeland Security Task Force (GHSTF) to devise and implement a homeland security strategy to protect Georgia citizens and infrastructure from terrorist attacks. The GHSTF's first priority was to initiate the Georgia Information Sharing and Analysis Center (GISAC) project in support of the GHSTF's broader mission, encompassing intelligence analysis, planning, crisis management, and consequence management, to secure the State of

---

22 Arizona Counter Terrorism Information Center Training Class, "Watch Log Entry System Training Class Manual," v1.0, Lockheed Martin, November 1, 2004, 6-7.

23 Janet Napolitano, "Securing Arizona; A Roadmap for Arizona Homeland Security," Arizona Governor's Office, April 23, 2003, www.governor.state.az.us./press/Securing_Arizona.pdf, accessed on July 5, 2005.

Georgia from terrorist threats and attacks. GISAC was officially created on October 25, 2001 and is one of only a few of state-level agencies dedicated solely to homeland security, antiterrorism, and counter-terrorism operations. Governor Barnes' successor, Governor Sonny Perdue, further developed the GISAC by designating it to be a primary component of the Georgia Office of Homeland Security.

1. Mission

The mission assigned to the GISAC project was to serve as the focal point for the collection, assessment, analysis, and dissemination of terrorism intelligence information relating to Georgia. GISAC was not intended to replace or duplicate the counter-terrorism duties of the Federal Bureau of Investigation, but rather to enhance and facilitate the collection of intelligence information from local and state sources, and to integrate that intelligence information into a system that will benefit homeland security and counter-terrorism programs at all levels.[24]

Soon after it began operations, GISAC established itself as the state's clearinghouse for terrorism-related intelligence information. It quickly developed protocols and relationships that enhanced its capabilities for the gathering, assessment, analysis, exchange, and dissemination of intelligence information between local, state, and federal government agencies; corporate security executives; and the private sector owners and operators of critical infrastructure assets.

Additionally, under the provisions of the **Antiterrorism Act** (OCGA 35-3-60), the **Antiterrorism Training Act** (OCGA 16-11-150), and **Georgia Bureau of Investigation (GBI) Investigative Division Directive 8-8-18**, in the State of Georgia, GISAC has the primary responsibility for developing and evaluating information about persons and/or organizations engaged in terrorist activities, investigating terrorist activities, and liaising with GBI work-units and other law enforcement agencies engaged in counter-terrorism operations and investigations[25].

---

[24] Robert I. Hardin, "Georgia Information Sharing and Analysis Center Information Intake and Management," Georgia Homeland Security Task Force/GISAC Directive # 03-002, Atlanta, Ga, January 1, 2003, 1-2.

[25] Official Code of Georgia Annotated, Title 16, Atlanta, Georgia, 2003, www.legis.state.ga.us/legis/2003_04/hinfo/wrap4c.htm, accessed on June 18, 2005..

The Federal Bureau of Investigation (FBI) categorizes terrorism as either domestic or international, depending on the origin, base, and objectives of the terrorists. The GISAC has adopted the following FBI definitions for use in their daily operations:

- Domestic Terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United State or its territories without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
- International Terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state. These acts appear to be intended to intimidate or coerce a civilian population, influence the policy of a government by intimidation or coercion, or affect the conduct of a government by assassination or kidnapping. International terrorist acts occur outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the person they appear intended to coerce or intimidate, or the locale in which the perpetrators operate or seek asylum.

2. Definitions

For the operational purposes, the GISAC has also incorporated the following definitions:

- Terrorist Act − An act which constitutes a crime against the person or against the residence of an individual (1) which is committed with the specific intent of and may reasonably be expected to instill fear into such person or persons or (2) which is committed for the purpose of restraining that person or those persons from exercising their rights under the Constitution and laws of this state and the United States and (3) any illegal act directed at other persons or their property because of those persons' beliefs or political affiliations (OCGA 35-3-60).
- Terrorist Attack − Any terrorist act or incident attempted or perpetrated against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives.
- Terrorist Incident − A violent act or an act dangerous to human life, in violation of the criminal laws of the United States, or of any state, to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives (FBI).

- Suspected Terrorist Incident − A potential act of terrorism for which responsibility cannot be attributed to a known or suspected terrorist group. Assessment of the circumstances surrounding the incident determines its inclusion in this category (FBI).
- Terrorism Prevention − A documented instance in which a violent act by a known or suspected terrorist group or individual with the means and a proven propensity for violence is successfully interdicted through investigative activity (FBI)
- Terrorism Intelligence Information − information historical, strategic, and/or tactical, that is pertinent to: 1.) the identification of persons, groups, or organizations that commit terrorist attacks, or are engaged in activities in support of, or in preparation for, terrorist attacks; 2.) the investigation of specific terrorist attacks by local, state, or federal law enforcement agencies, and the identification, arrest, and prosecution of the perpetrators of such acts or incidents; and 3.) the prediction and subsequent prevention of terrorist attacks through collection, integration, investigation, evaluation, and sharing of such information.

Additionally, *Terrorism Intelligence Information* involves circumstances that establish sufficient facts to give a trained law-enforcement or criminal investigative agency, officer, investigator, or employee a basis to believe that there is reasonable possibility that an individual or organization is involved in terrorist activities.

- **Antiterrorism Act − OCGA 35-3-60** – a law enacted by the Georgia General Assembly to "assist law enforcement personnel in the State of Georgia to identify, investigate, arrest, and prosecute individuals or groups of individuals who illegally threaten, harass, terrorize, or otherwise injure or damage the person or property of persons on the basis of their race, national origin, or religious persuasion.", and to establish "a special Antiterrorism Task Force within the Georgia Bureau of Investigation."
- **Threat Assessment** − the process of gathering and assessing information about persons, groups, or organizations, which may have the interest, motive, intention, and capability of perpetrating terrorist attacks. Most often, the term refers to the process of assessing certain information and circumstances in order to determine the probability that an actual terrorist attack is occurring, or is imminent.
- **GISAC Intelligence Request** − An inquiry for information available through the GISAC Terrorism Intelligence System. The requester must be a GISAC Participant or member of a GISAC Participating Agency, and must provide a reason for the query that meets GISAC mission criteria.

- **Need to Know** − Any GISAC Participant or member of a GISAC Participating Agency has a need to know when information requested will aid in the assessment of terrorism intelligence.
- **Right to Know** − Any GISAC Participant or member of a GISAC Participating Agency; as well as government officials whose agencies may be involved in incident response and/or consequence management; and managers of businesses and organizations, when their business or organization is specifically identified as a target of terrorist activity has a right to know when information received will aid in the assessment of terrorism threat information or terrorism intelligence.
- **Right to know** − when information received will aid in the assessment of terrorism threat information or terrorism intelligence.
- **Reasonable Suspicion of Terrorist Activity** − A set of circumstances that establishes sufficient facts to give a trained law-enforcement or criminal investigative agency, officer, investigator, or employee a basis to believe that there is reasonable possibility that an individual or organization is involved in terrorist activities.

3. Participants

State agencies and organizations that directly participating in the GISAC include:

- Georgia Office of Homeland Security (GOHS)
- Georgia Homeland Security Task Force (GHSTF)
- Georgia Bureau of Investigation (GBI)
- Georgia State Patrol (GSP)
- Georgia Emergency Management Agency (GEMA)
- Georgia Department of Defense / Georgia National Guard (GANG)
- Georgia Sheriff's Association (GSA)
- Georgia Association of Chiefs of Police (GACP)
- Georgia Association of Fire Chiefs (GAFC)

The manner of participation of each the several State agencies and organizations in the GISAC project varies according to each agencies resources, expertise, and related responsibilities. Currently, GISAC's day-to-day operations, facilities, personnel, finances, and administration are managed by GBI supervisors.

Federal agencies that participate in the GISAC project as "Homeland Security Partners" include:

- US Department of Homeland Security (DHS) − Washington, DC
- Federal Bureau of Investigation (FBI) − Atlanta
- Joint Terrorism Task Force (JTTF) − Atlanta

4. Staffing

GISAC is currently staffed by state-level law enforcement and homeland security agencies and organizations that include a total personnel roster of 18 individuals:

- Georgia Bureau of Investigation
  - Inspectors – 1
  - Special Agents in Charge – 1
  - Assistant Special Agents in Charge – 1
  - Special Agents – 5
  - Intelligence Analysts – 2
  - Investigative Assistant –1
- Georgia State Patrol
  - Investigators – 1
- Georgia Emergency Management Agency
  - Critical Infrastructure Analysts − 2
- Georgia National Guard / Department of Defense
  - Intelligence Analysts – 1
- Georgia Sheriff's Association
  - Investigators/Agents – 1
- Georgia Association of Chiefs of Police
  - Investigators/Agents – 1
- Georgia Association of Fire Chiefs
  - Investigators/Agents – 1

Salary, vehicle, equipment, and supply expenses associated with GISAC personnel are born by their respective employing agencies. The facilities and furnishings, including computer and communications equipment, are funded by grants and contributions from several of the participating agencies.

5. Duties and Responsibilities

GISAC's principal duties and responsibilities can be categorized as follows:

- Collection, analysis, and sharing of terrorism intelligence information;
- Terrorist threat assessment and monitoring;
- Terrorist incident response;
- Development and implementation of special projects, strategies, and initiatives.

Terrorism Intelligence: The primary function of GISAC is to collect, integrate ("fuse"), investigate, evaluate, and share information pertaining to possible terrorist activities in Georgia, for the purpose of preventing terrorist attacks from occurring or, if they do occur, to mitigate their consequences and extract useful information from the ensuing investigation.

As information is received at GISAC, it is initially documented by GISAC investigators and analysts, and then immediately evaluated by GBI supervisors, who filter, classify, and disseminate it. When appropriate, GISAC supervisors assign GISAC personnel to conduct follow-up investigation and analysis.

After review by GBI supervisors, the "raw" terrorism intelligence information is forwarded to GISAC's **GEMA**, **GANG**, **GSA**, **GACP,** and **GAFC** representatives, who review it within the context of their own particular areas of interest and responsibility.

The GEMA, GANG, GSA, GACP, and GAFC representatives may subsequently recommend certain actions to GISAC supervisors and/or their own agency/organization managers in order to disrupt or prevent possible terrorist attacks, or to mitigate and manage the consequences of an attack.

Terrorism intelligence information collected by GISAC is initially documented on the GISAC Activity Log, access to which is restricted to GISAC personnel. When deemed appropriate by GBI/GISAC supervisors, GISAC agents and/or analysts are assigned to conduct follow-up investigations, research, and analyses regarding the raw information in order to better determine its credibility, accuracy, and relevancy, and to gather additional relevant information. Terrorism intelligence information that meets the criteria of the GBI's Criminal Intelligence System is entered as an *Intelligence Report*

into that system. Investigations that arise from terrorism intelligence information are documented in the GBI Case Management System as Assistance Rendered, Terrorism or Intelligence investigations. The GBI Criminal Intelligence and Case Management Systems are operated in compliance with 28 CFR rules and regulations, and its data is available for query and analysis by approved law enforcement agencies / personnel in Georgia, as well as certain other states.

GISAC publishes and distributes a monthly terrorism-intelligence bulletin for state and local law enforcement and public safety agencies, homeland security officials, and other "need to know" entities. The *GISAC Intelligence Bulletin* summarizes statewide activities and concerns, and provides relevant information from local, state, and federal sources.

GISAC maintains a pager-based communications system, through which it can instantaneously communicate terrorism alerts, updates, and notifications to key public safety, homeland security, and emergency management officials throughout the state. Currently, the GISAC is not operational 24 hours a day but can be accessed thru 911 dispatchers and on-call GISAC personnel can be called or paged for immediate response if needed.

Terrorist Threat Assessment: A secondary, but critical role of GISAC that is interrelated with the terrorism intelligence collection and analysis process is its terrorist threat assessment function. Occasionally, information reported to GISAC, or information developed through subsequent investigation and analysis, will indicate that a terrorist attack may be underway, or imminent. On those occasions, GISAC personnel use all available resources in an effort to quickly and effectively evaluate the credibility of the information, develop additional relevant information, and notify response agencies and other appropriate entities in hopes of preventing or disrupting the attack or, at least, mitigating its consequences.

The procedure used to assess terrorist threat information is a unique investigative process that involves conventional investigative methods, as well as more technical

research methods that utilize queries of both open and restricted databases, and computer analyses. Essentially, threat assessment is a three-component process:

- **Identify** – identification of persons, groups, or organizations that have the interest, motive, and capability to perpetrate terrorist attacks.
- **Investigate / Evaluate** – assessment of persons, groups, or organizations who are identified as potential terrorist threats. Through **Manage** – implement an appropriate response to the threat (i.e. refer to JTTF, continue to investigate or monitor, disseminate warnings or alerts, etc).

Terrorist Incident Response: If and when there is a terrorist attack, involving weapons of mass destruction (WMD) or that otherwise results in significant damage, casualties, and/or disruption, in Georgia, or if large-scale terrorist attacks occur elsewhere within the US, GISAC will initiate its Incident Response Protocol (IRP), through which it will immediately notify Georgia's Director of Homeland Security; the JTTF; local and state public safety and response agencies, and other potentially affected entities, private sector as well as governmental. Additionally, ancillary response protocols will be immediately implemented, with GISAC personnel responding to the incident command post; manning GISAC communications systems at the GISAC Intelligence Operations Center; maintaining a computerized Incident Tracking System; exchanging incident-related information with other local, state, and federal law enforcement agencies; and monitoring the activities of other responding agencies.

Special Projects, Strategies, and Initiatives: GISAC was created by the GHSTF to develop and implement initiatives they deem to be necessary for the protection of Georgia's citizens from terrorist threats and attacks. Since its creation, GISAC has operated as the single state-level agency dedicated solely to homeland security issues. Subsequently, from time to time, GISAC is called upon to utilize its resources to perform special projects, develop and implement strategies, and implement initiatives as directed by the GHSTF and/or the Director of Homeland Security.

6. Information Intake & Management

Information that is collected by GISAC personnel is carefully documented and very tightly managed. Normally, incoming information is documented by GISAC personnel on GISAC Activity Report forms. This form, which may be completed on a computer or handwritten, is designed to collect detailed information from the source.

Once completed, the GISAC Activity Report is immediately forwarded to a GBI supervisor, who will review it, confirm or modify its classification according to type, priority, and urgency; and when deemed appropriate, assign it to investigators and/or analysts for follow-up action (investigation, research, analysis, or dissemination to other agencies or entities). The information captured on the GISAC Activity Report form is later entered into the GISAC Activity Log, which stores details of the information that can be queried for operational and administrative purposes.[26]

All terrorism intelligence information that meets the submission criteria for the GBI's Criminal Intelligence System is entered as *Intelligence Reports* into that system. When deemed appropriate by GBI/GISAC supervisors, agents and/or analysts are assigned to conduct follow-up investigations and analyses regarding the raw information in order to better determine its credibility, accuracy, and relevancy, and to gather additional relevant information. When additional research and investigation does not demonstrate that submitted information is credible, the information is not retained as intelligence information. Short term, as well as full-scale, investigations that arise from terrorism intelligence information are documented in the GBI Case Management System.

The GBI Criminal Intelligence and Case Management Systems are operated in compliance with 28 CFR rules and regulations, and their data is available for query and analysis by approved law enforcement agencies / personnel in Georgia, as well as certain other states.[27]

7. How the Information Flow Works at the GISAC

The procedure outlined below is how GISAC personnel will document and further process information that comes into the Center. Essentially, the procedure will rely on investigative and analytical personnel to initially document the information on a GISAC Activity Report form, as the information is received. After the information is initially documented, it will be the responsibility of the GISAC supervisors to review it; confirm or modify its classification according to type, priority, and urgency; and when deemed

[26] Bob Hardin (Commander, GISAC), interview with author, Atlanta, Ga., February 23, 2005.

[27] Robert I. Hardin, "Georgia Information Sharing and Analysis Center Information Intake and Management," Georgia Homeland Security Task Force/GISAC Directive # 03-002, Atlanta, Ga, January 1, 2003, 1-2.

appropriate, assign it to investigators and/or analysts for follow-up action (investigation, research, analysis, or dissemination to other agencies or entities).

a. GISAC'S Function

GISAC's mission is to serve as the focal point for collection, analysis, sharing and dissemination of information relevant to threats or attacks of a terrorist nature within and against the State of Georgia, its citizens, or infrastructure. Thus, it is critically important that all incoming information be properly documented and managed so that real indicators of actual terrorist activities / attacks can be recognized and referred for preventative action and consequence management as quickly as possible. In order to effectively and efficiently recognize and assess terrorist threats, and communicate that information to the agencies/persons who should have it, GISAC personnel must diligently and aggressively perform their information intake and management roles.

b. Information Intake

Terrorism related Information comes in to GISAC personnel through a variety of means, including telephone, fax, email, websites, news media outlets, publications, mail, and in person. That information, if possibly related to any terrorism issue, domestic or foreign, or to any potential target of a terrorist attack, must be immediately documented by the recipient on a **GISAC Activity Report** form. A copy of the GISAC Activity Report form is attached to this directive. The template for GISAC Activity Report form is electronically maintained on the GISAC server at **GISAC1 / Data / Forms & Templates**, where it can be printed out (blank) and used in making handwritten entries on the paper form, or the information can be electronically entered in the gray form-fields on the template, and the completed form can then be printed out for submission to GISAC supervisors, and an electronic version of the Report will be saved to the Activity Reports folder located on the GISAC server at **GISAC1 / Data / Activity Reports**.

c. GISAC Activity Reports

The **GISAC Activity Report** is the entry-portal for all information/requests submitted to, or collected by, GISAC personnel. The various labeled blanks, drop-down boxes, and checkboxes are intended to assist the recipient / author in obtaining as complete information as possible, and in accurately and quickly

classifying that information. The Report is divided into sections where the author should note information for "Subject-Person," "Subject-Vehicle,", "Subject-Business/Organization", "Target / Focus of Threat," "GISAC Classification," and "Criminal Activity."

The narrative section of the Report is where the author should summarize the information/request. The space allowed for the narrative on the Activity Report form is relatively small, and should be used to document only a brief overview of the information/request, consisting of only two or three sentences. GISAC supervisors will later rely on that narrative when they enter the Activity Report information in the GISAC Activity Logbook.

The complete and detailed narrative of the information will be documented on separate blank pages, which are to be marked with the GISAC Activity Report Number (assigned by supervisor) and attached to the completed Activity Report form. Any other documentation that is relevant to the information on the Activity Report should be similarly marked with the Activity Report Number and attached.

The bottom portion of the Activity Report is to aid supervisors with routing the information for follow-up action (investigation, research, analysis, etc.) and to document any subsequent dissemination of the information.

When a GISAC Activity Report is completed, it should be immediately submitted to a GISAC supervisor. Upon receiving a GISAC Activity Report, GISAC supervisors will, as soon as possible, confirm or modify the classification assigned to the Report (in accordance with classification guidelines), and then further process the information as determined by the GISAC supervisor, or as indicated by applicable GISAC protocols. GISAC supervisors (or designee) will assign Activity Report Numbers and log the required information in the GISAC Activity Logbook.[28]

[28] David Proctor (Special Agent, Georgia Bureau of Investigation), interview with author, Atlanta, Ga., February 23, 2005.

d. Gisac Activity Report Numbers and Logbook

The GISAC Activity Logbook will be maintained by GISAC supervisors, but will be accessible to all GISAC personnel. Other guidelines pertaining to the assignment of Activity Report Numbers and maintenance of the GISAC Activity Logbook are as follows:

- A three-ring binder will be used as the GISAC Activity Logbook for the purpose of maintaining a permanent record of Activity Reports generated by GISAC. Information submitted to, or collected by, GISAC personnel will be documented on a GISAC Activity Report form, which will be submitted to a GISAC supervisor (or designee), who will then assign the Activity Report Number, and make a corresponding entry in the GISAC Activity Logbook. At some point in the future, the GISAC Activity Logbook will be created electronically and will be maintained on the LAN, with access limited to GISAC personnel.
- GISAC supervisors (or designee) must assign Activity Report Numbers, and direct any follow-up action (investigation, research, analysis, etc.) and/or dissemination outside of GISAC. Such direction may be accomplished on a case-by-case basis, or through pre-established protocols.
- Activity Report Numbers will be assigned and logged chronologically by fiscal year, July 1st through June 30th. The first two digits indicating the last two digits of the fiscal year followed by a hyphen, and then five more digits, which will be the sequential identifier for the Activity Report. At some point in the future, a third series of alphanumerical characters may be added to denote the GISAC Classification assigned to the Activity Report.

Each page of the Activity Report Logbook will be divided into nine sections as follows:

Activity Report Numbers will consist of a series of two distinctive numerical identifiers. The first two digits will identify the fiscal year. The second series (five digits) will be the sequential identifier for Activity Reports initiated by GISAC during the fiscal year.

Date Initiated should be the date the information/request is received, or the earliest date thereafter.

Author should be the investigator/analyst who originally receives the information/request, or who completes the GISAC Activity Report form.

Classification will be the GISAC classification assigned to the information/request by the Author, if approved by the GISAC supervisor,

or as ultimately determined by the GISAC supervisor. If multiple activities are involved in the information/request, the GISAC classification should be based upon the most significant or serious of those activities.

Activity Location or Target/Focus of Information will identify the county (if in Georgia) most prominently involved in the information/request, the location [city, state (if not in Georgia), or country] that is the focus or target of the information/request, or the location from which the information/request is believed to have originated.

Activity Description should be two or three sentences describing the information/request (the activity). If multiple activities are involved, the description should focus on the most significant or serious activity.

Person(s) Assigned for Follow-Up Action(s) will be the investigator and/or analyst assigned to conduct follow-up investigation, research, analysis, or dissemination outside of the Center (if applicable).

Date Follow-Up Action(s) Assigned will be the date the follow-up investigation, research, analysis, or dissemination outside of the Center is assigned to the GISAC investigator or analyst.

Date Follow-Up Action Completed will be the date the follow-up investigation, research, analysis, or dissemination outside of the Center is accomplished.

In the GISAC Activity Logbook, a new page will be used to begin each month's entries. The month and calendar year should be listed at the top of each of the pages in the GISAC Activity Logbook. If removed from the GISAC Activity Logbook, the Logbook pages will be filed by fiscal year and month. The folders containing the GISAC Activity Logbook pages will be maintained in chronological order in the GISAC Case File Cabinet(s).

e. GISAC Protocols

The most significant and serious information/requests that come in to GISAC will be managed according to very specific and pre-established protocols, which will ensure that all of the appropriate persons / agencies are provided the information in a timely manner. Those protocols will require GISAC personnel to make certain notifications, and will utilize special forms with checklists on which to document the details of those notifications. The protocol documentation will be attached to and maintained with the corresponding GISAC Activity Report.

Additionally, with regard to the most significant and serious information/requests, certain protocols will be implemented with regard to how GISAC personal are to respond. These response protocols will specify what GISAC personnel should do when notified that a terrorist attack has occurred, is underway, or is believed to be imminent. The GISAC protocols will be described and implemented in later GISAC Directives.

- Group Name: Information Intake Group
- Group Location: GISAC "War Room"
- Group Mission/Objectives: The Information Intake Group is primarily responsible for manning the GISAC telephones and documenting information, and requests for information, that are submitted by officials and agencies, as well as the general public. As the information / requests are documented on GISAC Activity Forms, they are forwarded to the Information Evaluation Group for review and follow-up action, if deemed necessary. Intelligence information submitted to GISAC will be integrated with pre-existing intelligence and new intelligence from other sources and utilized as tactical intelligence by a variety of public safety agencies to manage the terrorist incident, investigation, and consequences.

f. Intelligence/Alert Dissemination

The flow of terrorism intelligence and threat information reported "down" to GISAC from an official federal governmental source, and then shared by GISAC with other governmental and/or private stakeholders:

- Intelligence/Alert Source: Federal Bureau of Investigation (FBI) / Joint Terrorism Task Force (JTTF), United States Department of Homeland Security (DHS), Department of Defense (DoD), Central Intelligence Agency (CIA), Georgia Office of Homeland Security (GAOHS), terrorism intelligence and homeland security entities in other cities/states/countries, etc.
- Intelligence/Alert Source notifies GISAC of terrorism related intelligence/threat information via electronic, written, or in-person communications:
- In most instances, urgent and/or high-priority terrorism intelligence/threat information is initially disseminated to GISAC Supervisors through direct face-to-face contact with Atlanta FBI/JTTF Supervisors. This information exchange is facilitated by the fact that GISAC and the Atlanta FBI/JTTF are housed on adjacent floors of the same building. GISAC and FBI/JTTF Supervisors subsequently coordinate further dissemination of that

intelligence/threat information, as well as their respective operational responses.

- Credible information concerning terrorist threat information is immediately assessed by GISAC Supervisors and staff as to what persons/organizations should be notified, and by what means. GISAC maintains a list of telephone numbers, pager numbers, and email addresses for executive officers and designated points-of-contact for most of Georgia's federal, state, and local public safety agencies, as well as members of the Georgia Homeland Security Task Force and Georgia Homeland Security Central Command, and security managers at many of the state's critical infrastructure (CI) facilities and key asset/resource (KA-R) sites.

The FBI, DHS, and elements of the DoD commonly use secure electronic communications systems to disseminate terrorism intelligence/threat information to state and local stakeholders. Those systems include the following:

- **Secure Telephone Unit (STU)** – telephone equipped with encryption capabilities used for voice communications involving classified information, encryption mode can only be accessed with the proper key.
- **STU Fax Machine** – operates similar to STU in the transfer of information in document form.
- **Homeland Security Operations Morning Brief (HSOMB)** – a daily electronic document summarizing the previous day's reporting to DHS's Homeland Security Operations Center (HSOC); published and disseminated by DHS's Office of State and Local Government Coordination (OSLGC) to state and local LE personnel.
- **Homeland Security Information Message (HSIM)** – usually a single-issue, electronic document used by the DHS/HSOC to communicate uncorroborated threat information to U.S. government agencies, State and Local Homeland Security Advisors, the private sector, and public in an expeditious manner; disseminated via e-mail.
- **Joint DHS/FBI Information Bulletin** – usually a single-issue, electronic document used by the DHS/HSOC to communicate information to educate the counter-terrorism intelligence, homeland security, and law enforcement communities about terrorism related issues; usually designated as LES or FOUO; disseminated via e-mail.
- **Joint FBI/DHS Intelligence Bulletin** – usually a single-issue, electronic document used by the DHS/HSOC to provide law enforcement personnel/entities with current, relevant terrorism information developed from counter-terrorism investigations and analyses, but does not contain

threat warning information; usually designated as LES; disseminated via e-mail.

- **Regional Information Sharing Systems (RISS) – Anti-Terrorism Information Exchange (ATIX)** – secure internet based communications system; managed through six regional centers that are funded and overseen by US Dept. of Justice, Bureau of Justice Assistance, Office of Justice Programs; available to local, state, and federal law enforcement (LE) personnel.
- **Law Enforcement On-Line (LEO)** – secure internet based communications system available to local, state, and federal LE personnel; supports secure e-mail communications between enrolled members; managed by FBI.
- **Joint Regional Information Exchange System (JRIES**) – secure internet based communications system; managed by DHS; available to local, state, and federal LE personnel.
- **Homeland Security Information Network (HSIN) – SouthEast Emergency Response Network (SEERN)** – secure internet based communications system; managed by DHS; uses JRIES platform; will integrate two-way, real-time communications of CI/KA-R and other private sector stakeholders with government counter-terrorism intelligence and homeland security entities; still in development. SEERN is one of four regions involved in the HSIN pilot program, with the main "hub" of the SEERN region being located in Atlanta.[29]

NOTE: DHS intends for HSIN-JRIES to become the single primary information sharing and communications system to connect their HSOC with federal, state, and local public safety entities, as well as with the security management for critical infrastructure – key assets/resources – and other private sector communities. Reportedly, the HSIN system will enable the HSOC to easily and quickly disseminate information and alerts to network members, and network members should be able to easily submit information to the HSOC, where it will be assimilated and analyzed with all other intelligence from a variety of perspectives – global, national, regional, state, and local.

g. GISAC Supervisor: GBI Inspector, Special Agent in Charge, Assistant Special Agent in Charge, or Designee

GISAC Supervisors are the primary points-of-contact for incoming official intelligence/alert information designated as classified (Secret, Top Secret), "Law Enforcement Sensitive" (LES), and "For Official Use Only" (FOUO). Dissemination of

[29] Stephen Clark (Chief Analyst, Georgia Emergency Management Agency) interview with author, Atlanta, Ga., February 23, 2005.

classified, LES, and FOUO intelligence from GISAC must be reviewed and approved by a GISAC Supervisor. When authorized to share such information with other state and local stakeholders, GISAC can employ a variety of communications systems, depending on the urgency, priority, and sensitivity/classification of the information.

GISAC maintains its own internal telecommunications system, but relies on the Georgia Bureau of Investigation's computer network, which includes internet access. Additionally, GISAC can utilize both GEMA's and the GBI's Communications Centers, which provide enhanced communications capabilities on a 24/7 basis.

h. Organizations

GISAC has established close working relationships with numerous organizations that have serious interest in terrorism related information, threats, incidents, and counter-measures. These organizations are able to serve as two-way communications conduits, through which GISAC can easily and quickly disseminate information to organization members, and through which members can forward information and concerns to GISAC. Some of these key "stakeholder" organizations are listed below:

- Georgia Homeland Security Task Force (GHSTF)
- Georgia Sheriff's Association (GSA)
- Georgia Association of Chiefs of Police (GACP)
- Georgia Association of Fire Chiefs (GAFC)
- SouthernShield (consists of representatives of state homeland security and counter-terrorism intelligence operations from Georgia, Alabama, Florida, South Carolina, North Carolina, and Tennessee)
- PrivateShield (consists of representatives of corporate security operations for corporate icons with major assets in the Atlanta area)

i. Activity Report (former Lead Sheet)

- Will include all reported suspicious activity to GISAC from law enforcement and concerned citizens.
- Activity Numbers (Lead Numbers) will be assigned by a supervisor at the time of the supervisor's review/assignment.
- The information will remain an ACTIVITY REPORT if it does not qualify as an INTELLIGENCE REPORT.

- Any follow up documentation, to include records checks, developed as part of the ACTIVITY REPORT follow up; will be maintained in the ACTIVITY REPORT file.
- A SUPPLEMENTAL ACTIVITY REPORT will also be available for additional documentation. The supplemental will also be database driven.

j. Intelligence Report T

- Will be developed at the direction of a supervisor.
- Will be written from information obtained in the ACTIVITY REPORT and any follow up investigation.
- The information being reported should be criminal or suspected criminal activity.
- The INTELLIGENCE REPORT will be entered/maintained in accordance with GBI Policy.

k. Intelligence Case

- Will be opened at the direction of a supervisor.
- Must have a criminal violation.
- An INTELLIGENCE REPORT may develop into an INTELLIGENCE CASE at the supervisor's discretion.
- The case file will be maintained in accordance with GBI Policy.

l. Analytical Support

Analytical support involves assembling terrorism intelligence information in a logical manner in an effort to determine patterns and meaning. GISAC Analysts and Agents can provide a variety of analytical and charting services in support of terrorism investigations. These services include the following:

- **Fusing Information:** Review and merge intelligence information with existing data in the intelligence system so that it may be analyzed.
- **Link Charting:** Establish relationships among entities, individuals or organizations in an investigation.
- **Event Charting:** Show the chronological relationships between persons, organizations, and related events.
- **Flow Charting:** Depict the flow of money, narcotics, weapons, stolen goods or other commodities through the elements of a criminal and/or terrorist network.
- **Activity Charting:** Define the pattern or sequence of a terrorist operation, including modus operandi.

- **Telephone Toll Analysis:** Condense large volumes of data into easy to read automated reports from which the significant telephone activity may be identified.
- **Case Analysis:** Summarize intelligence information, investigative actions taken and the main findings associated with these actions, and the activities of the subjects.
- **Special Publications:** Develop publications on various terrorism intelligence topics. The topics are determined by interest, availability of data and need for the information.[30]

m. Dissemination

Terrorism intelligence information will be disseminated to members of GISAC participating agencies when the requester has a need to know and a right to know the information in the performance of their duties.

Dissemination of information requested or submitted to GISAC will occur only with the express authorization of a GISAC supervisor, or when there is a specific dissemination protocol established by GISAC policies or procedures that dictates when and how certain information is shared/disseminated.

Information requested or submitted through GISAC will be disseminated to the GBI work units in the jurisdiction of the request/submission unless such dissemination is limited by GISAC or applicable federal restrictions.

GISAC Intelligence Reports (maintained in GBI Criminal Intelligence System) will only be disseminated by GISAC or the GBI Intelligence Unit with the express authorization of a GISAC supervisor. This will ensure that classified and sensitive information is not improperly released, and that GISAC is aware of any submissions or requests by other agencies that may be relevant to terrorism issues.

GISAC and the GBI Intelligence Unit will maintain a record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside of GISAC or the GBI Intelligence Unit.

---

[30] Stephen Clark (Chief Analyst, Georgia Emergency Management Agency), interview with author, Atlanta, Ga., February 23, 2005.

Nothing in this directive shall limit the dissemination of an assessment of terrorism intelligence information to a government official or to any other individual when necessary to avoid imminent danger to life or property.

In fact, when information relating to a potential terrorist threat is received, GISAC proactively identifies public safety and other government agencies, as well as private-sector entities that may have a legitimate need to know about the threat. Subsequently, information is shared in a manner that will enable governmental and private-sector entities to protect life and property.

n. Conclusion

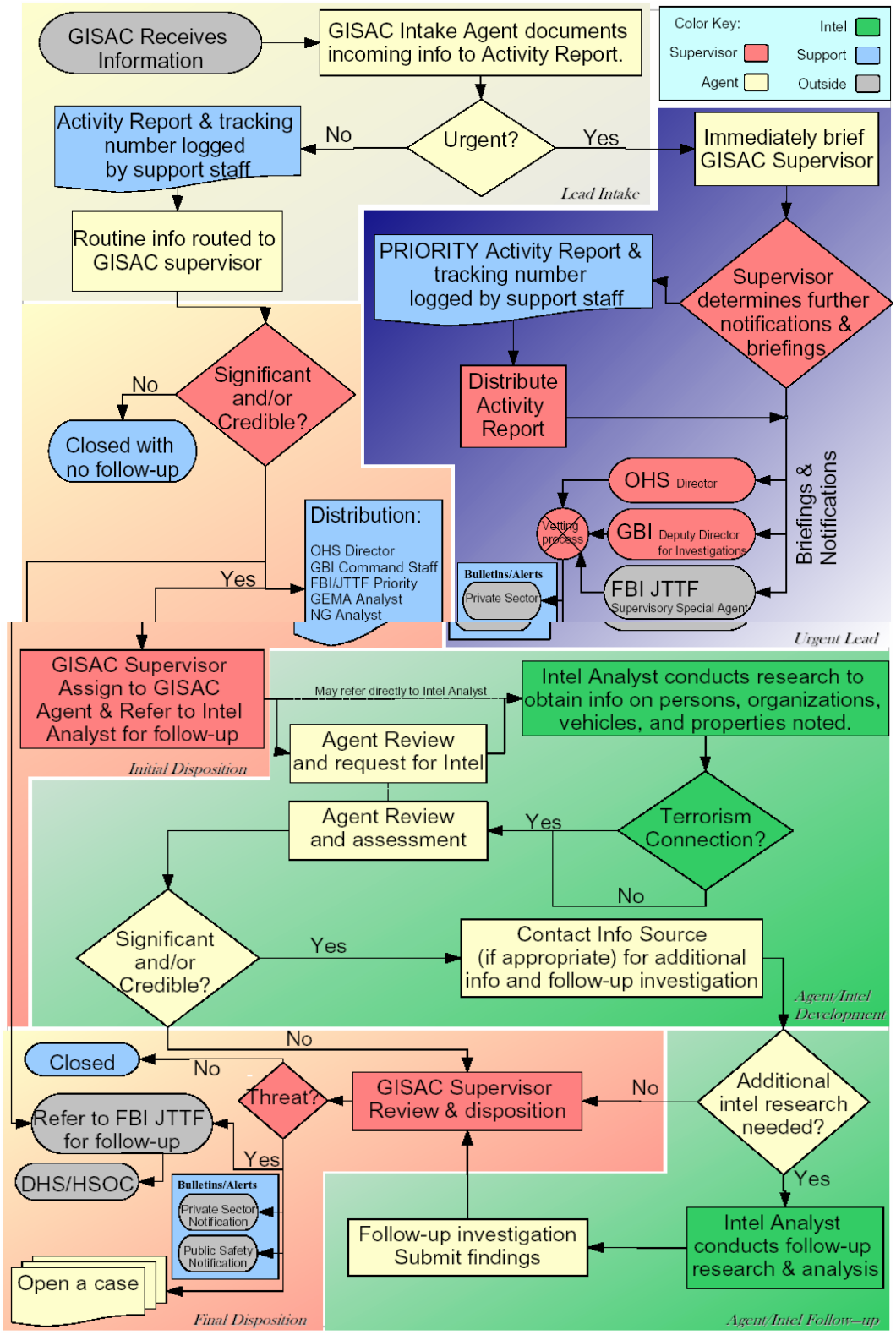
One important mile stone that helped to determine the GISAC's value was the Group of Eight (G8) Summit held at Sea Island, Georgia on June 8-10, 2004. This was the first major event to test the GISAC and its ability to collect, analyze, and disseminate relevant intelligence, with a variety of local and federal agencies in a national forum. The GISAC was also responsible for coordinating event activities and dignitary travel with these agencies and still maintain a sense for public safety issues such as rioting and street crimes. Because the GISAC was already operational, coordination of these activities were accomplished with few problems. The GISAC was the central intelligence and command center for the state during this event and proved itself very capable in coordinating both the law enforcement and intelligence activities for this event.[31]

The GISAC is one of many similar preventive initiatives that evolved by state agencies in response to the terrorist attacks of September 11, 2001. Information/intelligence fusion centers like the GISAC are important in identifying and addressing the gaps in our state and local intelligence networks. States where such centers do not exist run the risk of missing important clues that could identify, detect, and prevent a terrorist attack in their communities. The measures and practices implemented by the GISAC project represent significant improvements to Georgia's capabilities to

[31] Charles D. English, "The Georgia Information and Sharing Analysis Center: Model for State and Local Governments Role in the Intelligence Community", Thesis Paper, Naval Post Graduate School, Monterey, Ca, June 2004, 44-46.

detect terrorist threats posed by domestic, as well as international terrorists. The strength of the GISAC lies in its people and its resolve to meet the needs of the people of Georgia. The GISAC is a well run and well organized intelligence center that is evolving to meet the changing security needs of the terrorist threats of tomorrow.

The diagram below, provided by GISAC, represents the flow of information handling and evaluation handled at the GISAC:



C THE TERRORISM EARLY WARNING CENTER (TEW)

Los Angeles County boasts as being the largest metropolitan area in the Untied States with a population of over ten million people, living in 88 cities and spread over 4,000 square miles of urban terrain. Calculating an appropriate methodology for terrorism prevention and response coordinated with law enforcement, fire, public health, military, and emergency services is no small task. Like many large metropolitan areas, Los Angeles County realized that the casual partnerships formulated in the past were no longer enough to provide the detailed cooperation and planning needed for an effective security partnership that this vast area needed.

The Terrorism Early Warning Center (TEW) was the first operating fusion center in the country and was created to form a countywide group that was capable of a highly coordinated response to acts of terrorism, based on careful assessments of information, intelligence and detailed planning. The TEW met for the first time in October 1996 through the hard work and vision of two Los Angeles County Sheriff's Deputies, Sergeant John Sullivan and Deputy Larry Richards. Sullivan and Richards watched the many acts of terrorism in the world (mostly under the direction and funding of Osama bin Laden) and realized that the terrorist groups were operating from a complex network located in various parts of the world. Sullivan and Richards believed that the only way to effectively fight a terrorist network is to have a counterterrorism network working against it that shares information among different federal, state, local and private sector agencies. From this basic premise, the TEW was created.

The first TEW meeting was held with only a hand-full of representatives from the Los Angeles Sheriff's Department, the FBI, Los Angeles Police Department, representatives from the California Office of Emergency Services, and several from academic and research institutions. Sullivan and Richards shared a vision and strategy with this small group that instilled cooperation and team work. Many in that first meeting understood the importance of working together with other agencies if they wanted to be successful in combating terrorism.[32]

30. John P. Sullivan (Sergeant, Los Angeles County Sheriff's Department), interview with author, Los Angeles, Ca., February 16, 2005.

The Los Angeles County TEW initially set out to create a management framework and establish interagency partnerships among the various participating agencies. While "cooperation" among law enforcement agencies was a relatively common idea, the every day practice was far from a reality. Sullivan and Richards knew that the only way to make the TEW work (correctly) was to develop relationships that allowed interagency information sharing, fuse the different intelligence disciplines, share information, jointly investigate emerging threats, train and exercise against terrorist scenarios, and provide tactical support to responding agencies. This model did not exist and was not commonly embraced by initial shareholders. The previous standard operated in the traditional stovepipe model, where information flows up and down the agency hierarchy but rarely outside the walls of the agency. The TEW had the formidable task of implementing this new idea into a county having 45 different police departments, 38 fire departments, and 80 hospitals. Many said it could not be done![33]

The TEW got its first test in the summer of 1998 when the first national anthrax alerts were being generated. The TEW was the first such fusion center to predict that the anthrax attacks were coming to Los Angeles County. This prediction was predicated upon intelligence and open source information sharing which the TEW collected, analyzed, and then disseminated as an Emergency Preparedness Bulletin on terrorism awareness to agencies within Los Angeles County. These Emergency Preparedness Bulletins served as policy advisories on how to respond to weapons of mass destruction and anthrax for law enforcement agencies through-out California. A short time after the bulletins were disseminated the anthrax attacks began! Although the attacks were all identified as hoaxes, agencies throughout California began looking to the TEW for information, situational updates, and bulletins which were used to set policy and operational response plans for law enforcement and fire departments.[34]

---

[33] John P. Sullivan (Sergeant, Los Angeles County Sheriff's Department), interview with author, Los Angeles, Ca., February 16, 2005.

[34] Lois Pilant, "Strategic Modeling," Police Law Enforcement Magazine, Los Angeles, Ca, May 2004, 2-3.

Over the years, the TEW has consistently provided the same type of support and direction for such events as the "Westwinds Exercise," Y2K, and the Democratic National Convention. The TEW's input into the success of these events really gave the TEW the recognition it needed to both expand its operational influence and to attract funding support from local, county, and federal sources. The TEW's value was being recognized for the first time by many agencies within the Los Angeles County area as a place to look for helpful answers, information, and support.

The events of 9/11 forever changed the way U.S. law enforcement and fire departments looked at emergency response for first responders. Los Angeles County was no exception; immediately after the first plane crashed into the World Trade Center, the TEW expanded operations with additional staff from local, state, and federal agencies operating as a part of the LA County Emergency Operations Bureau (EOB). Since 9/11, the TEW has maintained a permanent position (with limited staff) at the LA Sheriff's Department EOB. With this evolution, the TEW now has permanent funding through Los Angeles County and the FBI's Joint Terrorism Task Force (JTTF).[35]

TEW's success at facilitating cooperation, teamwork, and information sharing among agencies in Southern California is no small feat. Commander Michael Grossman stated "the cooperation and team spirit needed to make the TEW work took years to cultivate, many of the TEW's shareholders were agencies that did not have a history of working cooperatively with other agencies in the past." The TEW has succeeded because of the personalities of the initial people assigned to work and develop the TEW. Grossman stated that once there is a trust between agencies (which starts at the working level) real sharing can take place. Grossman noted that "it just takes time to build that trust-it's a process not an event."[36] By creating partnerships in the public and private sectors with relevant disciplines, the TEW was able to develop the network needed to address the intelligence gaps that previously existed between federal, state, and local levels.

---

[35] Michael Grossman (Commander, Los Angeles County Sheriff's Department), interview with author, Los Angeles, Ca, February 17, 2005.

[36] Ibid.

1. The Mission and Role of the TEW

The TEW is designed to be an all source, all phase multi-agency, interdisciplinary, intelligence fusion center for the Los Angeles County Metropolitan Area. The TEW works during all phases of operations (pre-, trans-, and post-attack or threat) to assess the impact of terrorism and related threats in order to provide situational awareness and understanding to decision-makers at agencies of all levels, to include fire, health, and law.

The TEW also, monitors trends and potentials which may result in terrorist threats or attack within the Los Angeles County Area. The center evaluates all sources of information, including open source data, researching threat information to guide operations, training, and planning efforts. These "early warning" efforts provide support for law enforcement, fire, and emergency response personnel in making better informed decisions when a crisis is happening. The TEW also works to identify precursor events when assessing trends and potentials, with a focus on prevention and mitigation.[37]

2. Responsibilities

The TEW monitors trends and assess threats that could result in terrorist attacks in Los Angeles County. Currently, members of the TEW evaluate media accounts, information from federal, state, and local agencies, and other open-source data to determine the credibility of the information or source. As part of this assessment, the TEW identifies terrorism precursor events so that prevention and mitigation efforts can be undertaken.

The TEW also establishes protocols to identify and distinguish those threats credible enough to warrant a response and determine the level of response that is required. This has the extra benefit of providing cost savings because more complete information is available for initiating an appropriate level of response, rather than always sending a full-force response.[38]

---

[37] James P Royal (Sergeant, Los Angeles Police Department), interview with author, Los Angeles, Ca., February 16, 2005.

[38] John P. Sullivan (Sergeant, Los Angeles County Sheriff's Department), interview with author, Los Angeles, Ca., February16, 2005.

The TEW also assess threats and hoaxes, suspicious devices, and suspicious outbreaks of disease. Part of this responsibility includes monitoring special events that have the potential for terrorist attack.

During an incident, the role of the TEW is to provide information to incident commanders. In addition to providing "playbooks and target folder" (response information folders) the TEW continues to gather intelligence and assess new information for actionable cause. TEW's familiarity with their vast reservoir of information makes them a well prepared group for identifying potential sources of attacks, recommending courses of action, and providing continuing intelligence support and technical assistance to on-scene incident commanders. The TEW has been integrated into the Los Angeles area Unified Command structure for the last seven years.

3. Goals

The LA TEW is the focal point for analyzing the strategic and operational information needed to respond and combat terrorism and protect critical infrastructure within its area of responsibility. Special emphasis is placed on early detection of emerging threats, including acts employing weapons of mass destruction (MWD) such as chemical, biological, radiological, or nuclear (CBRN) agents and information warfare (IW or cyber-terrorism).

The LA TEW supports the Los Angeles County Emergency Operations Center (CEOC), the interagency terrorism working group (TWG), and the jurisdictional EOC's of all 88 cities in the operational area of the TEW. The TEW assesses all source information, including police reports, leads, and open source intelligence (OSINT), to forecast trends, potentials and support operations.[39]

4. Objectives

The LA TEW's objectives include:

Providing indications and warnings (IW), including on-going disease surveillance to the public safety community and critical infrastructure partners to enhance prevention and readiness.

---

[39] Roz Rosentrater (Crime Analyst, Terrorism Early warning Center), interview with author, Los Angeles, Ca, February 16, 2005.

Performing Operational Net Assessments (PONA) to gauge in the impact of a specific threat or attack and development viable courses of action for the CEOC, city EOC's, department operations centers (DOC's), and incident command posts (ICP's), to enhance the response to an attack.

5. Strategies

The LA TEW embraces a network approach to threat assessment, decision support and course of action development. The TEW utilizes data-mining tools, as well as standardized "Intelligence Preparation for Operations (IPO)" products to build all-source situational awareness and a common operating picture for the interagency response community. Typical IPO products include playbooks, response information (Target) Folders, Mission Folders, and Templates. A key element of the TEW process is the net assessment process to assess incident consequences.

6. Action Plans

During a known threat period or the aftermath of an attack, the LA TEW will actively monitor and assess situational awareness and status of all events that may impact the operational area. In addition, the LA TEW employs advanced technological means (known as forensic intelligence support units) to facilitate situation assessment and course of action development for the public safety community.

The LA TEW (either actual staff or virtual capacity) will focus on monitoring key public gatherings, the status of emergency services, and the status of all infrastructural components. The impact of actual attacks within and without the TEW's area of responsibility will be assessed in order to gauge resource needs and shortfalls and to develop potential courses of action to support incident resolution.

In preparation for an actual operation, the LA TEW provides support the operational areas CEOC, and the incident unified management structure.

- Assesses and develop new technology, tools, and analytical frameworks to improve support.
- Develops improved methodology to achieve net assessment mission.

7. Outcome Verses Output

The LA TEW provides a platform of network, multilateral, and horizontal communication of the threat information, and intelligence needed to manage a complex urban emergency operation. The LA TEW's net assessment process provides all source/all-phase fusion to perform "Operations/Intelligence Fusion" with an emphasis on both current and future operations. The LA TEW bridges the gap between crisis action planning and deliberate planning to provide the information necessary to achieve interoperability for complex, interagency, interdisciplinary, coalition-type operations.

TEW Watch Supervisor Sergeant James Royal and Crime Analyst Roz Rosentrater provided the following information regarding how the TEW works and products useful for shareholders:

a. Indications and Warning (Pre-Attack/Trans-Attack)

The TEW provides the following operational and strategic information for senior decision makers and on-scene commanders:[40]

- Intake point for all terrorism related leads, reports, including crime reports and leads.
- Assesses pre-incident indicators from a multidisciplinary perspective.
- Conduct threat assessment and estimates.
- Develop response and threat assessment tools (playbooks and target folders).
- Scan and monitor open source indicators of terrorist activity to assess trans and potentials.
- Synthesize threat information from all sources to develop situational awareness.
- Coordinate TLO (public sector law, fire, health) and ILO (private sector Infrastructure of Liaison Officers) programs.
- Develop collection plans; task leads to investigative agencies (e.g. JTTFs, and other criminal investigative/intelligence entities), and provide analytical support to same.
- Maintain liaison with other fusion centers throughout California and the nation.

[40] Roz Rosentrater (Crime Analyst, TEW), interview with author, Los Angeles, Ca, February 16, 2005..

- Provide consequence management consultancies (e.g. threat assessments), technical support and reach back.).
- Conduct training and special workshops on terrorism and emerging threats.
- Issue Advisories, Alerts, and Warnings, as well as special reports.

8. Operational Net Assessment (Trans-Attack/Post-Attack)

During an actual event, the TEW performs operational net assessments to determine the scope of the event and its impact on the Operational Area. The net assessment mission supports the Operational Area Emergency Operation Center (CEOC), and other command nodes within incidence unified command structure. A typical net assessment mission would follow this model:

- As directed, the TEW will provide a Unified Command Structure (UCS) with the impact of an actual attack on the Operational Area, gauge resource needs and shortfalls, continuously monitor and assess situational awareness/status, and act as the POC and law enforcement circles for interagency liaison in order to develop options for courses for actions for incident resolution.
- Conduct situation assessment (determined ground truth).
- Provide Advisories, alerts, warnings, net assessment and develop mission folders.
- Conduct Resource/Situation Assessment and assess alternative courses of actions for incident resolution.
- Bridge investigative and response information needs, supporting county EOC, County EOC, City EOCs, Department Operations Centers, JIOC, and Unified Command Post, provide information/intelligence support for mutual aid and military support to civil authorities.

One question that needs to be asked is, "Are there any measurements that can be referred to that indicate the TEW is accomplishing its goals? There are currently no known measuring standards which indicate that a fusion center such as the TEW is meeting its goals or making a difference in the fight against terrorism. That said, however, there are some tangible characteristics that need to be referred to as a sign of success. Since the creation of the TEW, however, some very positive changes have occurred within the law enforcement community in Southern California. New management frameworks between law enforcement agencies have been created and polished, this has taken years to develop and overcome traditional barriers and road

blocks that prevent intra-agency cooperation. In 1999, a major WMD Field Training Exercise was held in Los Angeles (Westwinds). One of the scenarios would involve an anthrax attack due to the potential of such an attack. The TEW was a major sponsor of that exercise because of the intelligence they developed and produced several emergency Preparedness Bulletins on terrorism awareness to include WMD and anthrax. Approximately one week later, the (now somewhat famous) anthrax attacks started in various parts of the United States.[41] The TEW was clearly able to show that the center was using the intelligence collected to take a proactive approach to terrorism.

The TEW has grown from a hand full of people (mainly from the law enforcement community) to nearly 400 officers, analysts and specialists from police, fire, military, federal law enforcement and intelligence officers, fire, public health, and private sector representatives. It is an organization that has become a national model for fusion centers across this country- they must be doing something right!

The issue of developing a viable standard to measure the efficacy of such centers is yet to be developed but could be the basis for a future thesis project.

9. Functional Description

The TEW has two major functions: Indications and Warnings (I&W) and operational net assessment. To fulfill these complex missions, the organization is divided into six interactive, multi-agency, and interdisciplinary elements. These elements are designated to operate as a complete network and are described as follows:

Officer-in-Charge (Command Element), who provides command, direction, and supervision, interacts with unified command structures responsible for sanitizing and disseminating classified information as necessary and ensuring multi agency coordination with local, state, and federal agencies.

Analysis/Synthesis Element (A/S) This is the central intergrading hub of TEW Net Assessment Group. This element tasks out requests for information to all other functional elements, then collects and integrates their individual products into a cohesive

41 Lois Pilant, "Strategic Modeling," Police Law Enforcement Magazine, Los Angeles, Ca., May 2004, 2-3.

assessment. This includes capturing investigative information, intelligence from all sources criminal, classified, open source/OSINT, cyber INT cyber Net, imagery, reconnaissance, data bases, etc. and analyzing and synthesizing it. A/S Element also synchronizes the information from the Law-Intel Element, Consequence Management, epidemiological I (EPI-INTL), and Forensic I Support (FIS)/Field Assessment Support Team (FAST) Element into a useable product for decision-makers. Products issued by the A/S Element include advisories, alerts, warnings, issue-specific white papers, and mission folders. Mission folders integrate treats specific playbooks, venue specific target folders, intelligence information, resource information, archival information on technical dimensions of threats of threat agents, resource status, and potential course of action for incident mitigation and response.

Investigative Liaison Element (INV-LNO) The Analysis/Synthesis Element. This element is responsible for processing, tracking, and collecting all criminal and national security intelligence information and leads related to terrorism. This element is the primary point of contact with all classified, national and state data bases, and with investigative and intelligence efforts at all levels of the government. This is the Operational Area/County link with the California Antiterrorism Information Center (CATC) and the Federal Bureau of Investigations (FBI). This element is the link to the national network of joint terrorism task forces especially the Los Angeles Task Force on terrorism. The INVLO Element has the capacity to deploy field observers and surveillance teams to assist specific threats. This element is also responsible for tasking other specialized investigative entities to develop a complete intelligence picture. Information and intelligence developed by the Law Intel Element is integrated with other information/intelligence products developed by its partner Net Assessment Elements through.

Consequence Management Element (CM) This element is staffed by members of the fire service, law enforcement, and medical professionals (EMS/Operational Medicine) in order to assess current and future resource status, provide technical reference, and develop potential courses of action for response to terrorism involving chemical, biological, radiology, nuclear and large scale explosives (CBRE). This

element has the primary responsibility for developing playbooks, targets folders, monitoring the status of resources, personal and critical logistical requirements for initiating and sustaining a comprehensive response.

Epidemiological Intelligence Element (Epi-Intel) This element integrates disease surveillance for all threats (especially biological terrorism) to complete analysis/assessment. This element assures integration of public health, law enforcement investigations, provides planning estimates on distribution of casualties, potential quarantine and treatment issues. This element ensures accurate and complete flow of information during intentional suspicious outbreaks, conducts continual monitoring to ensure early recognition and warning. This element is also responsible for food and water surety and agriculture issues (including liaison to the public health community, water districts (IEDWP, MWD), and U.S.D.A. etc."

Forensic Intelligence Support (FIS) Element and Field Assessment Support Team (FAST) This element is responsible for field assessment and reconnaissance activities. This element supports multi agency's responses with specialized detection and sampling equipment and coordinates law enforcement support to fire service mass casualty, mass decontamination (MCMD) operations. This element is also responsible for "virtual reach back" to specialist (at the national laboratories, military, etc.) to help us assess the situation and potential practical courses of action. This element is responsible for modeling and simulation of potential incident consequences using technical means. The FAST is the field expedient component of the FIS Element and links field information back to the TEW's Assessment Group.[42]

10. Intake and Informational Flow

The TEW is currently in the process of merging with the Joint Regional Intelligence Center (JRIC) in Norwalk, California and the following description of the informational flow used at the TEW is a combination of what is currently in place and what will be the new procedure later in 2005.

---

[42] James Royal (Sergeant, Los Angeles Police Department), interview with author, Los Angeles, Ca, March, 2005.

TIPS/Leads: Initial tips and leads come from a variety of sources to include private citizen call-ins, information from other law enforcement agencies and intelligence organization, the EMS community, military, and private business. All initial tips/leads will be handled by appropriate intake personnel (depending on the source of the tip) and will be entered into the JRIC tips/leads database for review by a collection manager.

Tips/Leads Recorded in Database: Tips/Leads will be input by intake personnel into a common JRIC tips/leads database (MEMEX) via a standard intake screen. Intake personnel immediately bring all urgent tips/leads to the immediate attention of a collection manager.

Analysis Collection Manager Review: An analysis supervisor/collection manager will review each tip/lead that is entered into the TEW/JRIC database. The collection manager will evaluate each tip/lead as to source reliability and content validity, and task an intelligence analyst to conduct any necessary follow-up.

Initial Notification to TEW/JRIC Management: The analysis supervisor will make initial notifications to the TEW/JRIC manager regarding tips/leads which require immediate action, or may require a decision as to dissemination of a bulletin, advisory, alert, or warning.

Dissemination: All TEW/JRIC dissemination products are reviewed by managers prior to release. The dissemination is made to the "approved" recipient list (all share holders).

Leads Assigned to Analysts: The analysis collection manager assigns each lead to one or more analysts for intelligence and lead value.

Analysis: Analysis refers to the ability separate information into "component parts" so that it can be understood from a structural (or network) point of view. This includes identifying and analyzing the relationships between the parts (or bits) of information. The TEW/JRIC Analysis section is comprised of subject matter experts from a variety of fields, who monitor terrorism trends and assess threat information which could result in terrorist attacks in the Los Angeles Operational Area.

The analysis process involves identifying information from tips, leads, and cases regarding known or new terrorist groups, activities, and actors, identifying known or new tactics, techniques, procedures, identifying potential target vulnerability and location information. Each analyst will share and receive appropriate intelligence information with other units and agencies, and will consult with other subject matter experts from other agencies. This process will be used to analyze individual and case information and analyze trends and potential indicators of future terrorist activities.

These analysts assess information from a variety of sources, including open source and classified material, and try to evaluate all tip/lead case, trend and threat information for evidence of patterns and indicators that may be present. This process is sometimes called "connecting the dots" which attempt to fit isolated and unrelated information into a more meaningful pattern.

TEW Cells: The TEW is divided into operational cells with subject matter specialists who provide analysis during the vetting and evaluating process. The following is a description of each of the four cells:

- Consequence Management − assess law enforcement, fire service, and health consequences of events by assessing real-time situation and resource status.
- Investigative Liaison- coordinates with investigation and intelligence teams from local, state, and federal agencies.
- Epidemiological Intelligence − is responsible for real-time disease surveillance, food and water surety, agricultural threat issues and coordination with disease investigations.
- Forensic Intelligence Support − provides technical support, CBRN reconnaissance, geo-spatial (mapping, imagery, and modeling products) and coordinates feedback among the field, TEW, and subject matter experts.

Investigative Liaison: Investigative Liaison Officers (INV-LNO) are non-operational and will coordinate all lead and case information between the TEW and investigative/intelligence teams form local, state, and federal agencies.

Leads Assigned to FBI, LASD, and LAPD: Investigative Liaison Officers will be responsible for ensuring that all leads requiring investigative follow-up are properly routed to the appropriate FBI, LASD, and LAPD squads.

Leads Assigned to Outside Agencies- Analytical Support: Investigative Liaison Officers will be responsible for ensuring that all leads are followed-up and are routed to the appropriate agency. Analytical support to outside agencies maybe provided by TEW analysts.

The primary agencies that have full-time members (officers and analysis) are as follows: Los Angeles County Sheriff's Department, Los Angeles Police Department, The FBI, Los Angeles County and City Fire Departments, Los Angeles Airport Police, Los Angeles Office of Public Safety, and the Los Angeles Department of Health. The primary focus of the TEW is to assess, detect, monitor, and if possible, disrupt terrorist attacks focused in the Los Angeles County area. In formation developed which is not related to this geographical area is forwarded to an appropriate agency (usually the JTTF) by an investigative liaison officer.

There is also a position at the TEW called "The Terrorism Liaison Officer (TLO). The TLO is an integral part of the connectivity between the TEW and the 1st Responder community (police, fire, health, private sector) and are the points of contact for these agencies.

Two other positions are about to be initiated within the TEW; the first, is an Infrastructure Liaison Officer who is the point of contact with railroad, highway and airport officials and provide planning and security briefings for these groups. The second position is the Private Sector Terrorism Response Officer who provides awareness and facilitates reporting of suspicious circumstances by the general public (i.e. bus stops, shopping malls, and special events) to the TEW/JRIC as a regional clearinghouse.

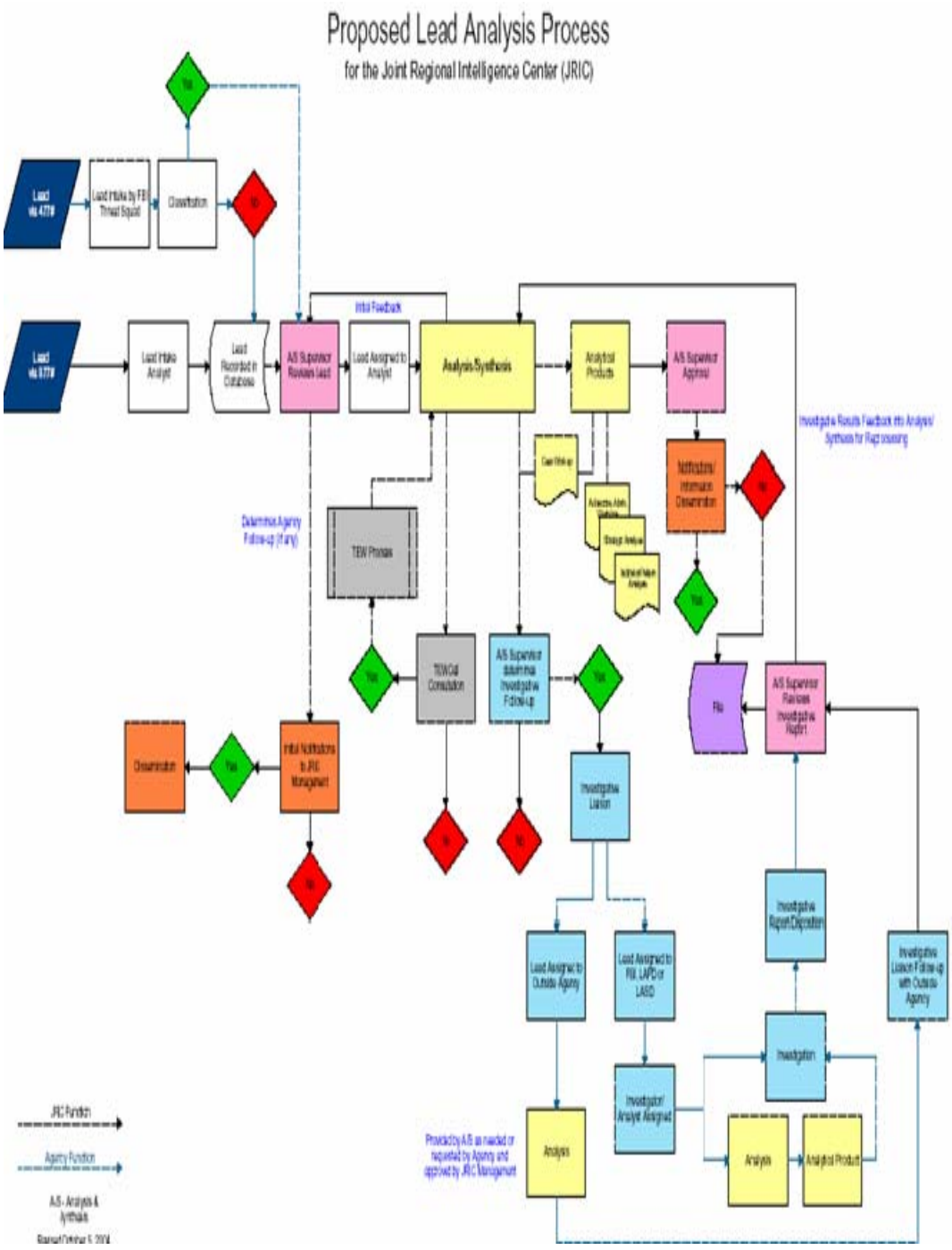
The TEW currently is not operational 24 hours a day; however, emergencies and urgent matters occurring after 6:00pm are routed through the 911 dispatch system. The TEW assigns "duty pagers" to staff for call-outs and secure text messaging.

11. Conclusion

The TEW has proven to be a powerful tool in both integrating and coordinating local and regional resources in fighting terrorism. The strength of the TEW comes from the full partnership of staff from agencies and jurisdictions drawn from a broader range of public safety disciplines. Having more than just a law enforcement focus, the TEW can utilize its diversity to better represent the cooperation and collaboration of a vast information and intelligence network that capitalizes on sharing information to exploit our adversaries. By including fire, public health, military, and private sector entities into this important homeland security partnership, which has traditionally been seen solely as a law enforcement problem, it allows law enforcement to view the terrorism problem from additional points of view. These added perspectives allow for a more comprehensive response to our nation's security needs.

The operational flow chart that follows depicts how information and intelligence will be directed and handled at the TEW as it is received. The chart depicted is a proposal for how information and intelligence is handled and evaluated when the TEW merges with the Joint Regional Information Center (JRIC) sometime in 2006.

Diagram provided by Sergeant John Sullivan, Los Angeles County Sheriff's Department.


Proposed Lead Analysis Process
for the Joint Regional Intelligence Center (JRIC)
Lead via 4779
Lead Intake by FBI Threat Squad
Classification
No
Yes
Lead via 9779
Lead Intake Analyst
Lead Recorded in Database
Intel Feedback
A/S Supervisor Reviews Lead
Lead Assigned to Analyst
Analysis/Synthesis
Analytical Products
A/S Supervisor Approval
Investigative Results Feedback into Analysis/ Synthesis for Reprocessing
Determine Agency Follow-up (if any)
TEW Process
Case Write-up
Subjects/Addresses Database
Strategic Analysis
Notifications/ Information Dissemination
No
Yes
TEW/Oral Consultation
A/S Supervisor determine Investigative Follow-up
Yes
File
A/S Supervisor Reviews Investigative Report
Dissemination
Yes
Intial Notifications to JRIC Management
No
No
No
Investigative Liaison
Investigative Report/Deposition
Lead Assigned to Outside Agency
Lead Assigned to FBI, LAPD or LASD
Investigative Liaison Follow-up with Outside Agency
Investigation
Investigator/ Analyst Assigned
Analysis
Analysis
Analytical Product
Provided by A/S as needed or requested by Agency and approved by JRIC Management
JRIC Function
Agency Function
A/S - Analysis & Synthesis

THIS PAGE INTENTIONALLY LEFT BLANK

IV. RECOMMENDATIONS

This chapter was originally titled "Best Practices-Best Methods," however, for purposes of this paper the word "best" seems to have an insufficient meaning. The word best has relative meaning based on unique circumstances, events, and operational environments. Therefore, what is a "best method" for intelligence collection and sharing in Los Angeles might not be the best method in Atlanta. Atlanta and Los Angeles are both large metropolitan cities but they have dissimilar local crime and terrorism problems; each city requires a different approach to their specific crime issues. For this reason, the author chose to title this chapter "recommendations" based on the recommendations of the analysts, supervisors and managers at each of the three fusion centers as well as the personal observations and opinions by the author

A Fusion Center requires the involvement and participation of all levels of government and private sector enterprises in order to identify the intelligence gaps. The FBI defines an intelligence gap as any question that identifies a lack of information about a criminal or terrorist threat.[43] That is, identifying the intelligence and information gaps tells us what we don't know about the things we do know. Intelligence requirements seek to fill the gaps of missing information useful to decision makers and policy advisors.

The attacks of September 11, 2001, in our country, and those most recently on July 7 and 21 (2005) in Great Britain, demonstrate that those who want to commit acts of terrorism in our homeland may already be living in our local communities and are now engaging in suspicious or criminal activities in our neighborhoods as they prepare for future attacks against us. The "fusing" process discussed in this paper illustrates the need for good collection and information management into actionable intelligence from all sectors at one location to support the immediate identification of emerging terrorism-related threats (at a local level) so that information and intelligence gaps are minimized.

[43] Michael G. Potts, "Field Intelligence Group Operating Guidance for the Implementation of the FBI Intelligence Cycle," FBI Policy Memo, April 2004, 2.

Successful counterterrorism efforts require the coordinated efforts of federal, state, tribal, local, and private sector agencies that have well-established information sharing capabilities to collect, analyze, and exploit information to be used against our adversaries. State/Regional Fusion Centers appear to be the best mechanism in achieving this end because they provide an opportunity to break down intelligence stovepipes and overcome many of the traditional turf wars that have prevented the cooperative efforts needed.

The kind of coordination this paper suggests is more than having a group of people from various agencies sitting together in a room. The level of coordination needed requires collaborative relationships that allows for appropriate interaction with each other while fostering trust between them. People must be able to leave their respective agencies and become a member of a new organization, each member being a resource from a home agency to be utilized for the common good of the center. In this way, the many parts are brought together to make a whole.[44]

The experiences of our many task forces nationwide have proven that, collectively, we can address criminal and terrorism problems faster, more efficiently, using less individual resources, and at reduced costs by working cooperatively rather than individually. Individuals assigned to these centers must be able work in an atmosphere of trust and mutual cooperation to make a fusion center successful. As with any endeavor, the process of inter-agency cooperation is usually slow but support from senior management from all participating agencies will go a long way in bringing these efforts to fruition more quickly.

The three centers previously described have different structures and missions and each center has adopted different strategies to overcome problems unique to their geographical locations. The following recommendations are provided as guidance for states and regions contemplating the creation of such a fusion center. The recommendations provided have been compiled during on-scene interviews and observations of managers and supervisors from each center. These recommendations

44 Merriam-Webster, *Merriam-Webster's Collegiate Dictionary ,11th Edition* (Merriam-Webster, Inc., Springfield, Massachusetts), 650.

come from individuals with extensive training and experience in fusion center development and should be considered as useful "lessons learned" for state officials attempting to create fusion centers of their own. Some recommendations provided by the Homeland Security Council in April 2005 are also included.[45]

A. DEFINITIONS

The following definitions are provided to convey some universal understanding of the terms and concepts presented in this paper and provide a common basis in addressing the issues of an information/intelligence fusion center:

Information–Raw data or facts that have not been processed or analyzed with regard to any other information.

Intelligence–Information that has been processed and analyzed to determine its meaning and relevance to other information. It is the product of a systematic collection, analytical, and evaluation process from raw data into an actionable meaning.

Operational Intelligence–Intelligence that is required for planning and conducting major operations to accomplish objectives within an operational area.

Intelligence Fusion–The process of organizing, analyzing, and synthesizing (blending) information from multiple sources to create vetted, validated intelligence products.

Information Sharing–The process by which raw data is collected and disseminated among agencies, governments, and individuals.

Intelligence Fusion Center ("Fusion Center") –A physical location where analysts receive, process, and analyze all-source information and synthesize their analysis into intelligence products suitable for dissemination to relevant agencies and officials. They are also referred to as information/intelligence fusion centers and simply as "fusion centers." For purposes of this paper, the term "fusion center" will be used.

[45] U.S. Department of Homeland Security, "Homeland Security Advisory, Intelligence and Information Sharing Initiative," (White House Office of the Press Secretary, April 28, 2005), 3-5.

Risk Assessment–The process of identifying key assets and evaluating the threats to and vulnerabilities of these assets. Risk assessments generally include three distinct components: criticality, vulnerability, and threat.

Criticality Assessment–A systematic effort to identify, evaluate, and prioritize a jurisdiction's assets. Criticality assessments attempt to gauge the relative importance of these assets and determine the impact of an attack against them.

Vulnerability Assessment–A systematic effort to identify and evaluate the weaknesses and susceptibilities to attack of a jurisdiction's assets. In identifying and evaluating existing weaknesses, a vulnerability assessment can determine ways to eliminate or mitigate the risks stemming from those weaknesses.

Threat Assessment–A systematic effort to identify and evaluate existing or potential terrorist threats to a jurisdiction and its assets. Threat assessments may yield only general information about potential risks due to the difficulty in accurately assessing terrorist capabilities, intentions, and tactics.[46]

B. LEGISLATION

Appropriate legislative agreements, laws, and memorandums of agreements need to be drafted and in place – that define collection, analysis, dissemination, procedures, and working partnerships–without infringing on the rights of private citizens.

In the aftermath of the 9/11 attacks, a number of legislative bills and laws were signed in an effort to improve information sharing at all levels of government; among them are:

- The USA Patriot Act, signed in October 2001, among other things, mandates and gives law enforcement officials at all levels greater powers and authority for information sharing and gathering.
- The Intelligence Reform and Terrorism Prevention Act, signed in 2004, created a new national intelligence chief with direct mandates of creating environments for improved intelligence sharing across all levels of government.

---

[46] Lessons Learned Information Sharing website, "Best Practices, Local Anti-Terrorism Information and Intelligence Sharing: Intelligence Support for Response Operations," July 10, 2005, www.LLIS.gov, accessed August 13, 2005.

- The Homeland Security Advisory Council in an April 2005 report on information and intelligence sharing gave strong recommendation that all states should establish multidiscipline fusion centers.

C. PHYSICAL FACILITY

Realtors have an old saying, "location, location, location!" as a way of reminding buyers that property values differs from one area to another. Where the fusion center is located will have an impact as to what agencies will participate there. A center that is located in the heart of a large metropolitan city would pose significant commuting problems for staff members living in adjacent communities. Also, a major traffic accident or natural disaster could render the downtown area of a large city inaccessible.

The facility must be represented by various state and local agencies that have established this facility for processing terrorism-related information and producing analyzed intelligence for public safety officials. By seating officers and analysts from various agencies together at one location, they naturally develop personal relationships that help to break down interagency resistance that prohibits information exchange. This center will become the home of an information sharing network comprised of a group of agencies sharing information and intelligence with one common purpose.

This facility should be operational 24 hours a day and have an appropriate staff and work space to accommodate representatives from all shareholders. Centers should have (at the minimum) work spaces to include phones (secure/non-secure), faxes, computer work stations, shredders, copy machines, conference and meeting rooms, white boards, cable TVs, satellite antennas, Secure Video Television Conferencing (SVTC), monitors, projectors, one or more situation/incident command room(s), and appropriate IT tools and infrastructure to support the connectivity needs of the state or region at this facility with funding for system up-grades.

The facility should be a separate center (not part of an existing EOC, etc.), a center that has been adopted for no other purpose. Efforts to maintain appropriate operational procedures and maintain proper security in this type of environment is much

easier. This facility must be large enough to accommodate all operational, analytical, and task force related needs and must accommodate future growth demands (which will be inevitable).

The facility must have suitable secured parking and storage capabilities, as well as access control for all visitor and employees entering the center.

The facility should have back-up generating machines, pumps, and fuel in the event of electrical disruptions or long-term power outages.

The center must have a designated secret compartmental information facility (SCIF) area for SCI information, which is separated from the rest of the center. Appropriately cleared individuals will handle all classified information collection, storage, analysis, and "scrubbing," and ensure proper dissemination.[47]

The facility should be able to accommodate sleeping quarters for an appropriate number of staff on a rotating basis for an extended period of time to address long-term crises.

D. INFORMATION TECHNOLOGY (IT)

The TEW in Los Angeles is utilizing an information data base at the center developed by the FBI called the TITAN system as a way of sharing certain information and products to a variety of shareholders.[48] Currently, there are nearly 500 law enforcement members with 200 additional members being screened for inclusion, and almost 100 corporate members from various security related industries. It works like this, TITAN takes the initial application from a potential member, vets the application against the member base and, once approved, then pushes certain information to the member based on their "need to know." Members of the TEW and JTTF decide the member's level of "need to know." Law enforcement and intelligence agencies would have a greater need to know than an associate in the private sector. Levels of "access" to

[47] Interviews at all three fusion centers indicate that less than 2% of information received is at a classified level and therefore the SCIF areas at these centers remain very small in relation to the rest of the center.

[48] James Royal (Sergeant, Los Angeles Police Department), interview with author, Los Angeles, Ca, March 1, 2005.

more law enforcement sensitive information would be restricted from members not having the need to know particular aspects of on-going law enforcement activities. TITAN primarily handles "sensitive but unclassified" information but could easily be expanded to accept and disseminate "classified" information as needed.[49] This particular data base system (or something compatible with inter-face capabilities) could be utilized nationwide to allow each state the ability to communicate with each other on a day-to-day basis. The particular system is not as important as the ability to communicate and access information from neighboring states or regions instantly without any communication barriers.

The goal of each state fusion center should be to have connectivity to collect and disseminate appropriate levels of information with every police, sheriff, fire, EMS, county public health, transportation, and private sector agency within the state. This level of communication should be available 24 hours a day, seven days a week.

E. FUNDING

Funding for a fusion center can come from federal, state, and private sector resources. Funding for the TEW in Los Angeles, for example, is received partly from the County and City of Los Angeles, the FBI, and the State of California. The centers in Arizona and Georgia primarily utilize funding received by state funds and funds committed by the FBI. Federal funds can become available at certain times depending on world and national events which can also be used to offset local costs. Available grants and application kits can be found using the DHS/ODP website at: www.ojp.usdoj.gov. One drawback to using only federal funds for intelligence centers is that those funds rarely continue for more than a couple of years, so when the federal funding ends, significant operational cutbacks have to be made by local agencies who don't have the funds to continue such activities. Often, when this scenario happens, the end result is a cut in personnel.

Funding for fusion centers need to be looked at from two perspectives: short- and long-term. Short-term funding covers start-up costs (such as building

[49] Ibid.

construction/renovations, security systems, fencing, lighting, office equipment and supplies, etc.). Long-term funding is obtained for ongoing operational costs such as personnel, training, updating equipment, overtime, computer systems and networks. Typically, federal funds should be considered as short-term funds that can be cut during any given funding year. The generation of long term funding should be looked at from the local and/or state levels.

In FY 2004, 2005, and 2006, The Office of Domestic Preparedness (ODP) has set aside several grant programs for fusion center technical assistance that can be used for creating state fusion centers (with guidance modeling for a LA TEW style center).[50] The grant is called the Urban Area Security Initiative (UASI) and gives money to states for various local homeland security purposes that include personnel, equipment, training, exercises, and fusion centers. Federal funding for anti-terrorism information and intelligence sharing can be the difference in having a fusion center or not. Federal funding is helpful because it eases the fiscal burden of local budgets and, at the same time, fosters greater cooperation and support from all agencies participating at the center.

Staffing and funding are the two biggest issues to deal with when creating a fusion center. DHS has provided funding to state and local agencies for protective clothing, computers, WMD exercise gear, etc., but little for personnel. Many agencies are reluctant to hire additional personnel, using other grant funding, for fear future funding will be dropped and the additional personnel costs would then have to be absorbed by the local agencies (who are typically unable to continue providing those added costs). If ongoing funding could be budgeted for staffing, part of that budget should be earmarked for a career track within the fusion centers that allows the center to create incentives and advancement plans for personnel who want to stay there and advance. Fusion centers draw people from local law enforcement, fire, and health agencies that have not created adequate career advancement opportunities for their employees at the center. As a result, after two years, well-trained and experienced

[50] Kevin Saupp (Technical Assistance Program Manager, Office of Domestic Preparedness), interview with author, Washington, D.C., July 22, 2005.

personnel have to decide whether to leave and advance within their agency or stay at the center in a career-ending position.[51]

DHS also offers money from the 2005 Homeland Security Grant Program (HSGP), which provides a single application kit and program guidance for multiple funding programs to enhance our nation's homeland security efforts.[52]

One observation from the author; as I have traveled around the country over the last five years working with state and local agencies in anti-terrorism activities, state and local agencies have always looked to (and expected) the federal government to provide all (or a major portion) of the funding, training, and equipment for anti-terrorism projects and programs. State budgets have not factored expenses for such newly specialized activities (such as fusion centers). Recent history, however, has taught us that state and local governments must change the way they have looked at addressing (and fund) their local security needs. A reasonable person would have to ask, "how much longer and how much more money can the U.S. Government continue to pour into state coffers when we are engaged in a costly war overseas, the national debt skyrocketing, social security on the brink of bankruptcy, and now we have just sustained one of the worst natural disasters (Katrina) in the last 100 years?"

The recent hurricane (Katrina) in the South has illustrated that the federal government is not an entity of endless money and resources that can be instantly relied upon in every situation and condition. Each state and city must work toward achieving a greater level of self reliance and less dependence on the federal government in order to be fully prepared. At the least, state and local governments should have emergency operation plans and resources to independently deal with local disasters (man-made or natural) for the first three to five days of the incident without any federal support. State and local authorities must make the hard choices that the fight for homeland security calls for. This may come in the form or raising taxes, selling local or state bonds, portions of

---

[51] James Royal (Sergeant, Los Angeles Police Department), interview with author, Los Angeles, Ca, July 21, 2005.

[52] Department of Homeland Security, Office of Domestic Preparedness, "Fiscal Year 2004 Terrorism Early Warning (TEW) Expansion Program: Grant Application Kit and Program Guidelines," March 2004.

state lottery proceeds going towards local homeland defense, or cutting other social entitlements often taken for granted and largely spent on non U.S. citizens.

F. STAFFING

As mentioned previously, having the right personnel is vital for having a successful center. Beyond having employees who are motivated, competent, and hardworking, they must have the proper education and training in intelligence synthesis and analysis. This kind of background is not easily found at the local or state level. The author has observed some departments and local agencies simply transferring secretaries and clerks to positions of "analyst" within an intelligence bureau to meet an immediate need, often with little or no training in intelligence. While many of these people are excellent employees, their skills and knowledge base is lacking when it comes to addressing the analytical needs of an intelligence center. The lack of uniform training and standards creates a big problem not only for the individual state center but it also hampers effective intelligence coordination and dissemination between other state and federal centers.

One suggestion to address this problem would be to develop an "Intelligence Analyst Academy" (IAA) at the state level. Since the fusion center will be gathering information and intelligence from virtually all law enforcement, fire, public health, and private sector groups within the state, representatives from each group should be canvassed and recruited to develop a suitable candidate pool to draw from for students at the IAA. Former government and military employees or retirees with intelligence backgrounds and clearances could be recruited for these positions as well.

The students could be taught in a variety of subjects such as: intelligence gathering methods and techniques, the difference between information and intelligence, what is analysis and how it is done, report writing standards, handling/processing in-coming information, phone tips, how to handle un/classified information, training on various data bases used by the center and state, and daily production products (dissemination). There are a variety of subjects and courses that could be developed in the IAA curriculum and a certification process which could be the subject of another thesis.

At the end of the IAA, students would receive a state certificate indicating they were "certified" as an intelligence analyst. To keep the certification current, analysts would have to complete 20 -40 hrs of "in-service" training each year. For career development and promotional purposes, advanced courses or certificates could be offered at the Academy. The IAA should receive the same attention and emphasis by state leaders as the police and fire academies do to make it effective.

G. GENERAL GUIDELINES–ORGANIZATION/STRUCTURE (THE PROCESS)

Jurisdictions employ a number of mechanisms to share terrorism-related information. Dissemination is the foundation for sharing. Historically, information has flowed "downward" from federal and state agencies to local entities that then disseminated the information to appropriate public safety and private sector groups. A common complaint with that procedure is that much of the information is not timely or relevant for local jurisdictions that eventually get the information. In recent years, local law enforcement has collected information at the local level and began transmitting it "upward" to state and federal entities for appropriate use and dissemination. When information begins to flow in both directions, national and local entities can benefit from the developing information networks that are forged and used to facilitate the flow of information across all levels of government.

With that said, local agencies must have in place specific policies as to what kinds of information they will share and to whom. Dissemination policies allow for standards to be set that allow for appropriate persons to have access both within and without the agency. Without standardized intelligence products, agencies and departments will waste valuable resources and not share information effectively.[53]

One of the principal outcomes of a fusion center is the identification of terrorism-related leads; that is, any nexus between crime-related information and terrorist activities on a broader scale. Although the primary emphasis of information/intelligence fusion is

[53] David L. Carter, "The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies," FBI Law Enforcement Bulletin, Washington, D.C., June, 2005, .6-7.

to identify, deter, and respond to emerging terrorism-related threats, a collateral benefit to state and local entities is that it will support ongoing efforts that address non-terrorism-related issues as well.

Managers and directors of each fusion center provided specific guidelines and suggestions as essential requirements for establishing such a center, as follows:

The sustaining foundation of any agency is determined by the quality of its personnel. Staff personnel must have up-to-date training, awareness, and understanding of the global and domestic threat environments current in the world today. This is achieved by ongoing training and information/intelligence analysis. Detailees should plan on a two-year minimum commitment to the center. Center personnel must develop a clear understanding of the links between terrorism-related intelligence and non-terrorism-related information, so that precursor activities can be quickly identified as indicators of an emerging threat. Analysts can then separate the "wheat from the chaff" and direct resources toward issues posing the most immediate threat.

More specific to organization and staffing, specialized analytical cells are needed in the center with more expertise regarding certain groups, regions, and possible tactics. The analytical groups could also be divided into strategic analysis, gap analysis, and targeting projection thus creating more subject matter expertise within the center. By allowing certain staff members to receive advanced training and specialized proficiencies, they can become subject matter experts that improve and add credibility for the center.

Connectivity to and with all shareholders utilizing the center must be provided, including an appropriate IT infrastructure with security backstops to ensure appropriate levels of information, based on the needs and responsibilities of the shareholder. It would not be appropriate for private sector business staff (for example) to have access to data bases containing ongoing law enforcement investigational information.

Connectivity with critical intelligence networks, analysis centers, communication centers, and information repositories is mandatory. Ideally, each state would have at least one fusion center. Each state should be able to have connectivity with the other fifty state

fusion centers as well as connectivity to a national fusion center (yet to be created). The logical location for this National Fusion Center would be next to (co-located with) the National Counterterrorism Center (NCTC) outside Washington, D.C. Local FBI JTTFs and Field Intelligence Groups (FIGs) help bridge some of the gaps between local and federal agencies but they are not enough. A national fusion center, created in a similar fashion to the local fusion centers and co-located with the NCTC, would fill the gaps currently in our system that prevent intelligence proficiency.

Electronic networking provides the best and safest way of sharing information across jurisdictions. Agencies must have secure intranet and email systems that can disseminate mass volumes of information instantly and with ease. These systems can be password protected allowing for different levels of access based on people (and agency) needs and rights to know.

There must be a clear delineation of roles, responsibilities, and requirements at each level of government participating in the fusion center. Senior officials must also be informed about this asset as another source for information in policy and planning issues. Fusion centers can play a vital role in drafting emergency announcement broadcasts during ongoing disasters. This objective can easily be done by tabletop and full field exercises.

The center must have clear intelligence and information requirements with the federal intelligence community, guiding planning, collection, analysis, dissemination, and reevaluation efforts.

Publicity for the center is crucial. The center must be well advertised, with appropriate telephone numbers published, to promote continuous interaction between the center and all shareholders (particularly the private sector and general public).

While most information handled in a fusion center is non-classified (law enforcement sensitive), there are times when a center would generate or receive classified information (usually via a JTTF) in monitoring an emerging threat. Center staff must be trained in guidelines and policies. Appropriate storage areas and cleared personnel must be in place to accommodate such information.

In an executive order on information sharing, from President Bush, he directed federal and local agencies to "protect the freedom, information privacy, and other legal rights of Americans in the conduct of intelligence-sharing activities."[54] Strict guidelines and procedures must be in place to ensure that this executive order is not violated.

Active participation by specially trained and/or educated people (subject matter experts) are needed to provide immediate insight and help on evaluations for threat/attack assessment and recovery estimates.

The center must have continuous interaction with the private sector and the general public. This can be done through advertisements, Agency Liaison Officers, private sector liaison contacts, and tip and information lines to the center.

As described, the fusion process involves every level of government and tries to embrace all sections of public and private disciplines to ensure that no intelligence gaps are unidentified. At a minimum, fusion centers should be organized at a statewide level with each state establishing and maintaining a center with the previously described caveats to facilitate the fusion process. In larger metropolitan areas, localized fusion centers should be considered to establish similar capacities that provide links with larger state, regional, or federal fusion centers. The Los Angeles TEW is perhaps the best example of how a large metropolitan area makes this all work. The Los Angeles TEW has been consistently successful in monitoring incoming intelligence, identifying trends, and coordinating responses with law enforcement, fire, health, military and emergency service agencies for the past ten years!

National standards now being developed and finalized by DHS should provide additional guidance on this process, however, particular infrastructures and operational protocols used by individual jurisdictions should be based on the specific needs and capabilities of each jurisdiction.

---

[54] George W. Bush (President of the United States), Executive Order #13356, "Executive Order Strengthening the Sharing of Terrorism Information to Protect Americans," White House Press Office, Washington, D.C., August 27, 2004, 2.

Under the direction of DHS, a Homeland Security Council was organized in October of 2004 for the purpose of exploring issues and possibilities in forming statewide fusion centers.[55] The following suggestions were provided by this council as additional criteria for inclusion into the fusion process:

H. MANAGEMENT AND STRUCTURE

- The center must clearly define the management structure and determine who is in charge and what entity will be in charge of daily operational activities. Leadership can become confusing when personnel from multiple agencies come together in one place, each with different ranks and operating protocols.
- The center must clearly define goals and objectives so all shareholders can understand and support the fusion process.
- The center must clearly establish a process to define information and intelligence collection requirements.
- The center should develop the appropriate agreements and memorandums of understanding that communicate requirements.

I. PLANNING AND REQUIREMENTS

- Conduct a comprehensive and compatible risk analysis to include threat, vulnerability, and consequence assessments.
- The center should be able to identify patterns and trends that reflect emerging threats.
- Must have well defined collection requirements based on risk assessments.
- Readily identify circumstances and events that are indicators and/or precursors of threats or attack.
- Be able to identify and tap into sources and repositories of data and information warehouses that help identify indicators and precursors.
- Identify existing collection gaps through evaluation of current sources of information/data banks.
- Create public awareness (both of the problem and the center) activities that enhance situational awareness by the public. Develop partnerships with public and private officials that help with making this awareness a reality.

[55] U.S. Department of Homeland Security, "Homeland Security Advisory, Intelligence and Information Sharing Initiative," April 28, 2005, 3-4.

- Develop and incorporate mechanisms to support reporting of collected information (e.g., 911 system, tip lines, internet, and connections to key information systems).
- Identify and understand the different regulatory, statutory, and privacy issues that impede the collection and sharing of information.
- Most of the above issues can be accomplished by having a robust training and exercise program in place that emphasizes each criterion.

J. COLLECTION PROCESS

- Communicate collection requirements to relevant state, federal, tribal, local, and private sector entities.
- Mitigate roadblocks to collection activities.
- Compile both classified and unclassified data banks of information and intelligence that is generated by people, organizations, and governments.
- Serve as an initial point of contact (24/7) for information provided by various state and federal agencies (e.g., FBI, DOD, DHS, CIA, NSA, e-mail bulletins, and telephone calls) for the receipt of the following:

    1. Immediate threat information (classified/unclassified)
    2. Long-term threat information (classified/unclassified)
    3. Tactics and methods used by terrorists (classified/unclassified)

- Integrate with other reporting systems (e.g., 911), and establish an easy to use capability for the public for reporting suspicious activities in conjunction with the Joint Terrorism Task Force.
- Establish a process for identifying and tracking the reports of suspicious activity and threats-follow-up.

K. ANALYSIS

- The center must be able to blend data, information, and intelligence received in high volume and from a multiple of sources.
- Reconcile and de-conflict various data streams, and validate the credibility of this data received from these collection sources.
- Evaluate and analyze data and information using subject matter experts to help decision makers.
- Identify and prioritize risk factors and threats faced by the various jurisdictions (e.g., local, county, state, and region).
- The center must be able to produce value-added intelligence products that are timely, accurate, and useful for the end-users. These intelligence

products will support the development of performance-driven, risk-based prevention, response, and consequence management programs.

- The center's analysis will produce specific protective measures to identify and disrupt potential terrorist attacks during the planning and early operational stages.

L. DISSEMINATION, TASKING, AND ARCHIVING

- Identify those entities and people (e.g., officials, executives) responsible for developing and implementing prevention, response, and consequence management efforts and cultivate their support and funding.
- Provide relevant and timely intelligence to those entities responsible for implementing prevention, response, and consequence management efforts (public and private sectors).
- Develop appropriate archival mechanisms for data, information, and intelligence, for future review and to support future response efforts.
- Establish a method for tracking performance-based prevention, response, and consequence management measures.
- Establish the ability to track performance metrics associated with prevention, response, and consequence management efforts.
- Provide feedback and after-action reports to information collectors and providers.

M. REEVALUATION

- Develop a tracking system of achievement prevention, response, and consequence management performance metrics so as to evaluate impact on the risk environment.
- Constantly up-date threat, vulnerability, and consequence assessments so as to update the risk environment.
- Continue to monitor and assess the effectiveness of national (e.g., federal, state, tribal, and local) intelligence and information collection requirements process.
- Continue to monitor the center's operational, procedural, and policies to ensure that all information and intelligence needs of the shareholders are being met.[56]

---

56 U.S. Department of Homeland Security, "Homeland Security Advisory, Intelligence and Information Sharing Initiative," April 28, 2005, 5-6.

N. FINAL THOUGHTS

Looking ahead to the next ten years will require fusion centers to adjust proceedures, up-date technologies and information sharing systems, hire better trained and multi-lingual analysts and investigators, and develop long term funding strategies to maintain the quality of these centers for the future. The next ten years will require fusion centers to raise the bar of operational expectations to include more intensive training and exercising, improved social network analysis, improved interagency and interdisciplinary collaboration at the state and federal levels, and improvements in recognizing emerging threats and groups.

The events of the last five years have only re-confirmed the need for our intelligence and law enforcement community to change our methods of operations. Despite many evolving changes in the intelligence community, there remains a similar structure of stovepipes and old-time cultures consistent with the cold war era. Whatever our failures were prior to 9/11, the U.S. intelligence community did what it was designed to do; it focused on U.S. interests overseas, with little attention to the activities linking overseas activities with domestic events. The complete scope of necessary changes is still being evaluated with real world events continuing to be a driving factor. General discussions about how to fix the problem have resulted in a number of proposals to create new organizations and new networks (like fusion centers). The suggestions presented in this thesis will give states a foundation to develop suitable fusion centers for themselves in an effort to distance themselves from the line of thinking that lead to the disconnected events leading to 9/11.

V. CONCLUSION

As various committees within the United States Government have reviewed the circumstances leading to the events of September 11, 2001, evidence suggests that the collective information leading to that event fell into an intelligence void somewhere between foreign and domestic threats. The U.S. foreign intelligence agencies were watching for foreign based threats to our homeland that were generated from overseas and the domestic agencies were looking for evidence of foreign sleeper cells preparing to act within the United States. At the time, none of the agencies were looking for a foreign threat aimed at domestic targets nor was there a way to share each agency's information that might show such a threat existed. The attacks that came were not from deeply entrenched sleeper cells but from foreigners who had recently infiltrated into the United States to launch their attacks on that day.

The final report generated from the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission Report) suggested that the September 11th attacks were successful (in part) for the following reasons:

- Intelligence was not properly shared due to legal, procedural and inadvertent reasons.
- The hand-offs of information were lost across agency divides, separating the foreign and domestic intelligence information systems.
- Individual agencies were not working as a team, each had individual specialties but no governing body to provide oversight and ensure that the intelligence holes were filled.[57]

The incidents of both 9/11 and those more recently of July 7, 2005 (in the U.K.) provide the reminders that information gathered by state and local agencies can be extraordinarily useful in fighting terrorism if properly collected, analyzed, and disseminated. In preparation for a terrorist attack, terrorists may be engaged in other criminal activities such as trafficking, smuggling, narcotics activities, finance operations and money laundering in local areas. Often, state and local agencies are better able to

[57] The 9/11 Commission, *Final Report of the National Commission on Terrorist Attacks Upon the United States (*W.W. Norton & Company, Inc., New York, 2004), 353.

identify, report on, and help prevent terrorist acts before the terrorists have an opportunity to act than some of the better known federal agencies. When fully functional and integrated, a state or local intelligence center working in close coordination with regional and/or federal agencies can collect, analyze, and disseminate actionable intelligence and provide a bridge to the intelligence gaps identified by the 9/11 Commission. This multi-level coordinated effort allows for a more blended anti-terrorism approach while at the same time breaking down the stovepipes and agency barriers that have maintained the bureaucratic turf wars of the past.

This thesis has been written to provide both a model and an argument for the merits of a fusion center and how it can provide state and local agencies an opportunity to break down the barriers currently impeding information sharing. Much has been done at the federal level to help improve the atmosphere of intelligence flow across all levels of government but state and local agencies can also facilitate such activities by not only utilizing the various federal grants and loans now available but also local and state resources generating funding for the careful creation of localized integrated fusion centers.

APPENDIX

A. THE GEORGIA INFORMATION SHARING AND ANALYSIS CENTER (GISAC) INFORMATION CLASSIFICATION SYSTEM OUTLINE:

1. CLASS 1 INFORMATION – High Threat, High Urgency, High Priority

1-A − Terrorist Attack / Activity Related to WMD (Information, with specificity and credibility, indicating that a WMD terrorist attack, activity, or event has occurred, is occurring, or is imminent)

1-B − Terrorist Attack / Activity Not Related to WMD (Information, with specificity and credibility, indicating that a non-WMD terrorist attack, activity, or event has occurred, is occurring, or is imminent)

1-C − Apparent / Alleged Criminal Activity Related to Terrorism (information relating to criminal activity, such as those involving guns, bombs, threats, thefts, etc., that appear to be associated with extremists groups or other terrorist organizations)

1-D − Apparent / Alleged Criminal Activity Not Related to Terrorism (information relating to criminal activity that does not appear to be associated with extremist groups or other terrorist organizations)

2. CLASS 2 INFORMATON – Undetermined Threat, Some Urgency, Medium Priority

2-A - Vague Terrorist Threats (Information, without specificity, indicating a possible terrorist attack/threat, or information that may constitute only suspicious circumstances that appear to be, or are consistent with, possible terrorist activity)

2-B - Suspicious Circumstances (suspicious persons, activities, vehicles, infrastructure related, etc.)

2-C - BOLOs, Alerts, & Bulletins (look-outs and warnings communicated from government sources)

3. CLASS 3 INFORMATION – Low Threat, Not Urgent, Low Priority (absent specific threat)

3-A - Requests for Assistance/Queries ("Do you have any info about?")

3-B - Protest Event (anti-war, anti-government, animal rights, abortion, etc.)

3-C - Target Event (sporting events, concerts, celebrations, inaugurations, dignitary appearances, etc.)

3-D - Other (information that does not appropriately fit into any of the categories listed above and is deemed to be low threat, low priority, and not urgent)

B. THE GEORGIA INFORMATION SHARING AND ANALYSIS CENTER (GISAC) PERSONNEL ASSIGNMENTS:

1. Duties: Answer telephone calls, and document submitted information and requests.
2. Instructions, aids and "go-bys":
    a. GISAC Activity Report forms: See Attachment A
    b. Instruction Sheet(s) and Examples: See Attachment B
    c. Important Telephone Numbers: Black notebooks in "War Room"
3. Personnel Administration Issues:
    a. Supervision:
    b. Shift Supervisors: One GBI ASAC or SAP per shift.
    c. Inspector: GISAC Inspector is Robert Hardin

4. Work Hours / Shifts: Initially, the GOC will operate with two 12-hour shifts, shift times to be announced. As the situation develops, the number of shifts, shift times, the number of personnel utilized per shift may be modified.

5. Duties / Expectations: Agents assigned to the Information Intake Group should be at GISAC and in the War Room at least 15 minutes before their shift begins for shift briefing and new instructions.

6. Sign-In / Sign-Out: There will be a sign-in and sign-out sheet in the War Room; all agents will sign the sheet beside their name, and will note the time of their arrival and departure at the end of their shift. Agents will not sign in as on duty more than 30 minutes prior to their assigned shift time, unless expressly authorized by a supervisor.

7. Breaks: Breaks can be taken as needed.

8. Clothing: Business-casual attire is authorized. Khaki pants and blue GBI "golf shirts" can be worn, but patches, badges, and weapons should not be displayed when outside of the GISAC office suite.

9. Display of Identification and Weapons: Agents are encouraged to display credentials while in GISAC office, but should not display any identifying badge, patch, or credentials when out of the GISAC office suite.

10. Parking: Agents should park their vehicles at the southwestern corner of the parking lot in front of the building.

11. Sickness or Injury: Agents who become ill or injured should immediately contact their GISAC shift supervisor for instructions

12. Contacts with family & friends: Calls to family members and friends from the GISAC office are permitted, but should be very limited in time and number. Calls made with personal cell phones or at personal cost while off duty are allowed without limitation.

C. THE GEORGIA INFORMATION SHARING AND ANALYSIS CENTER (GISAC) EQUIPMENT/SUPPLIY NEEDS:

1. Office Equipment
   a. Locations:
      - Telephones
      - Copy Machines
      - Laptop(s)??
      - Printers
      - Shredders
   b. Operating Instructions
      - Telephones
      - Copy Machines
      - Laptop(s)??
      - Printers
      - Shredders
2. Supplies Needed:
   a. Forms
      - Instructions
      - Examples/Samples

      b. Ink Pens
3. Agent Equipment:
   a. Weapons
      - Duty Weapon
      - Exposure of weapons in the building and parking lot
   b. Other Equipment
      - Portable Radios
      - Southern Linc Radios
      - Cell Phones
      - Laptops

4. The various systems, both traditional and "high-tech," used by GISAC to disseminate terrorism intelligence/alert information to other state and local entities are:

a. Conventional Communications Systems

- Telephone (traditional)
- Fax Machine
- Cellular Telephone (voice, text, and photo)
- Southern Linc Radio (two-way and group mobile)
- Local Area Network (LAN) E-mail
- Internet E-mail
- Pagers (Georgia Technology Authority Paging System)
- GBI Radio (two-way mobile and base)
- National Law Enforcement Telecommunications System (NLETS)

b. Mass Communications Systems

- Blast Fax – GEMA's automated fax transmitter that is pre-programmed with fax numbers that are categorized into various groups, including the following:
- Georgia Emergency Management Staff
- Georgia Office of Homeland Security
- Georgia Homeland Security Task Force
- Police Chiefs
- Sheriffs
- 911 Centers
- Department of Motor Vehicle Safety
- Dept. of Natural Resources−Law Enforcement
- Emergency Coordinators (for all state agencies)
- EMS/Ambulance Services
- Fire Departments
- EMA Directors

- **Dialogic System** – automated telephone calling and messaging system that can rapidly call numerous pre-programmed telephone numbers and transmit a pre-recorded voice message. Information is categorized similarly to the Blast Fax groups listed above.

- **Group E-mail** – internet E-mail system with pre-programmed and categorized E-mail addresses enabling simultaneous transmission of messages and documents to computers and PDA's. E-mail addresses are categorized similarly to the Blast Fax groups listed above.

- **Group Paging** – for state personnel and others who have assigned GTA Paging System pagers, individuals or groups can be rapidly paged with an alpha-numeric message.

c. Bulletins and Alerts GISAC collects, compiles, and summarizes significant terrorism, public safety, and homeland-security related information in two separate bulletins. GISAC also occasionally prepares and distributes alerts/notices regarding urgent and high-priority terrorism and homeland security issues. Those electronic publications are described below:

- ***GISAC Open Source Bulletin*** – a weekly publication consisting of credible items of information and articles pertaining to terrorism, public safety, and homeland security issues that are compiled through research of numerous unrestricted internet sources. This bulletin contains no classified, LES, or FOUO information and is widely disseminated to state/local government officials and corporate security executives. It is primarily disseminated via E-mail and fax through GEMA.

- ***GISAC Intelligence Bulletin*** – a monthly publication consisting of synopses and copies of terrorism and homeland security information/intelligence generated by GISAC or derived from other official bulletins, notices, and alerts that may not be available to other state/local agencies. This bulletin is designated as "Law Enforcement Sensitive" (LES) and is only disseminated to state/local/federal law enforcement agencies. It is primarily disseminated via E-mail.

- ***GISAC Homeland Security Notice*** – an occasional publication, usually featuring a single terrorism/homeland security issue that is of particular concern, warranting rapid dissemination to the state/local public safety agencies. Most notices are designated as LES.

D. THE GEORGIA INFORMATION SHARING AND ANALYSIS CENTER (GISAC) FACILITIES, LODGING, AND SUBSISTENCE NEEDS:

1. Orientation to facilities:
    a. Office layout
    b. Group locations
    c. Exits
    d. Key Cards
2. In-House Food & Beverage Supplies:
    a. Bottled Water
    b. MRE's
    c. Snacks
3. Emergency Equipment and Evacuation:
    a. Emergency Exits
4. Equipment
    a. Fire Extinguishers
    b. Flashlights
    c. Emergency Exits / Stairwells
    d. Gathering Site
5. Bathrooms:
6. Break Room(s):
7. Security Procedures:
    a. Access to Office
    b. Visitors
8. Lodging:
    a. Direct Billing
    b. Two occupants per room (on shift/off shift)
9. Off-Site Meals:
    a. Locations
    b. Direct Billing
10. On-Site Meals:

BIBLIOGRAPHY

Arizona Counter-Terrorism Information Center Information Bulletin. "Arizona Intelligence Bulletin Report" (November 2004): 1-4.

Arizona Counter-Terrorism Information Center Training Class Manual. "Watch Log Entry System Training Class" (November 2004): 1-22.

Bush, George W. "Executive Order (13356) Strengthening the Sharing of Terrorism Information to Protect Americans" White House Press Office (August 2004):1-17.

Carter, David L. "The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies". FBI Law Enforcement Bulletin (June 2005): 1-26.

English, Charles D. "The Georgia Information Sharing and Analysis Center: A Model for State and Local Governments Role in the Intelligence Community". Thesis Paper, Naval Post Graduate School (June 2004): 1-62.

Georgia Bureau of Investigation. "Operations Guide Manual". (.Information Provided by Bob Hardin, Commander, Georgia Information Sharing and Analysis Center, March 2005): 1-177.

Gilmore Commission Report. "Fourth Annual Report to the President and Congress. White House Office of the Press Secretary (December, 2002): 1-462..

Hardin, Robert, I. "Georgia Information Sharing and Analysis Center Information Intake and Management". Georgia Homeland Security Task Force/GISAC Directive #03-002 (January 2003): 1-4.

Hewitt, Christopher. *Understanding Terrorism in America: From the Klan to Al Qaeda.* London, Routledge, 2003.

Johnson, Loch K., and Wirtz, James J. *Strategic Intelligence, Windows Into a Secret World An Anthology.* Roxbury Publishing Company: Los Angeles, California, 2004.

Lessons Learned Information Sharing Website (LLIS). "Best Practices Local Anti-Terrorism Information and Intelligence Operations Sharing: Intelligence Support for Operations. available at www.llis.gov, accessed on June 25, 2005.

Lowenthal, Mark. *Intelligence: From Secrets to Policy,* 2nd Edition, CQ Press, Washington, D.C., 2003.

Merriam-Webster. *Merriam-Webster's Collegiate Dictionary,* 11th Edition, Merriam-Webster, Inc., Springfield Massachusetts, 2003.

Napolitano, Janet. "Securing Arizona; A Roadmap for Arizona Homeland Security, (April, 2003): 1-26.

Pilant, Lois. Police "Law Enforcement Magazine: Strategic Modeling". (May 2004): 1-4.

Potts, Michael G. "Field Intelligence Group Operating Guidance for the Implementation of the FBI Intelligence Cycle", FBI Policy Memo (April 2004): 1-9.

Tamman, Maurice and Stanford, Duane, Barnes. "Planning Anti-Tterrorism Intelligence Center for Georgia". Atlanta Journal-Constitution, October 26, 2001.

The 911 Commission. "Final Report of the National Commission on Terrorist Attacks Upon the United States" W.W. Norton & Company, Inc. (April 2005).

The Markle Foundation, "Protecting America's Freedom in the Information Age", New York, New York, (2002): 1-39.

Title16. *Official Code of Georgia Annotated.* Atlanta, Ga. www.legis.state.ga.us/legis/2003_04/hinfo/wrap4c.htm, accessed on June 18, 2005.

United States Department of Homeland Security, "Presidential Directive (HSPD) #8", White House Office of the Secretary, (December 2003): 1-7.

United States Department of Homeland Security. "National Response Plan, White House Office of the Press Secretary, (December 2004).

United States Department of Homeland Security. "Homeland Security Advisory, Intelligence, and Information Sharing Initiative", (April, 2005): 1-28.

United States Department of Homeland Security, Office of Domestic Preparedness, "Fiscal Year 2004 Terrorism Early Warning (TEW) Expansion Program: Grant Application Kit and Program Guidelines" (March 2004).

United States Department of Homeland Security. Homeland Security Advisory Council, "Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion" White House Office of the Press Secretary (April, 2005): 1-11.

Weapons of Mass Destruction Countermeasures Unit, FBI. (WMDCU). "Annual Field Office Report (AFOR), (April 2004): 1-16.

Woodbury, Glen. "A Networked Country of Information Sharing and Collaborative Intelligence Operations" Homeland Security Affairs (July 2005): 1-5.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Fort Belvoir, Virginia

2. Dudley Knox Library
   Naval Post Graduate School
   Monterey, California

3. Paul Stockton, Director
   Center for Homeland Defense and Security
   Naval Post Graduate School
   Monterey, California

4. Chris Bellavita, Director of Programs
   Center for Homeland Defense and Security
   Naval Post Graduate School
   Monterey, California

5. Rudy Darken, Professor
   Center for Homeland Security
   Naval Post Graduate School
   Monterey, California

6. Bill Kelly
   Office of Domestic Preparedness
   Department of Homeland Security
   Washington, D.C.

7. Captain Robert Simeral, Professor
   Center for Homeland Defense and Security
   Naval Post Graduate School
   Monterey, California

8. William Pelfrey, Professor
   Office of Domestic Preparedness
   Department of Homeland Security
   Washington, D.C.

9. Linda A. Cranston
   FBI Academy Librarian
   Quantico, Virginia

10. Michael G. Potts, Section Chief
Intelligence Management Section
FBI Headquarters, Room 1B223
Washington, D.C.