Title: "Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies"

Final Report Submitted To:

The National Institute of Justice

Final Report Submitted By:

Michigan State University
301 Admin Bldg
East Lansing, MI 48824
Phone (517) 355-5040
Fax (517) 353-9812

Date Submitted:

October 1, 2011

Investigators:

David Carter, Ph.D.
Steven Chermak, Ph.D.
Ed McGarrell, Ph.D.
Jeremy Carter, Ph.D.
Jack Drew
School of Criminal Justice
Michigan State University
East Lansing, MI 48864
Phone: 517-432-5574
Fax: 517-432-1787

Title: "Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies"

Project Abstract: State, local, and tribal (SLT) law enforcement agencies play a critical role in securing the homeland, and understanding and improving the intelligence practices of these agencies will enhance public safety. Better intelligence must be collected, analyzed, and shared, but little is known about the intelligence practices of SLT agencies. This project addresses these gaps. Specifically, we examine the experiences of SLT agencies and fusion centers for building an intelligence capacity, understand critical gaps in the sharing of information regarding intelligence, and identify obstacles related to other key intelligence issues, such as measuring performance and communication between agencies. In addition, we examine the activities of three fusion centers to identify strategies that appear to be successful in increasing the information flow across agencies, the major obstacles of effective intelligence gathering and information sharing, and to identify key practices for integrating domestic intelligence into the information sharing environment and overcoming these obstacles.

Our research design consisted of two methodologies. First, we conducted a national survey of SLT agencies with two different samples. Our first sample consisted of personnel responsible for establishing state fusion centers and thus was critically involved in building the state-level intelligence infrastructure. The second sample was comprised of state, local, and tribal personnel charged with building an intelligence capacity in different sized agencies in all regions of the country. Second, we conducted three fusion center (FC) case studies. The data collection strategy for the case studies included compiling and analyzing open source documents, and then conducting interviews with key informants. Our focus was on examining how local, street-level intelligence is managed and brought into the intelligence process to prevent terrorist incidents and to address a variety of criminal threats.

Although there are a large number of important findings discussed in this report, there are several highlighted here. First, although significant progress has been made post-9/11 installing fundamental policy and procedures related to building the intelligence capacity of law enforcement, there is significant room for improvement and a need to move agencies forward to be consistent with key requirements. Second, fusion centers are farther along instituting policies and practices than individual law enforcement agencies, most likely because there has been an extensive focus on developing fusion center operations and expertise by both the Department of Homeland Security and Department of Justice. Third, both samples of respondents stressed that they have worked at building relationships with a diverse range of agencies, but they also indicated that they are not completely satisfied with these relationships. Fourth, there is an overwhelming amount of information going into and out of these agencies, and it is likely, without having enough analysts within the organization or analysts not effectively trained to process this information, that there are missed opportunities for strategic and tactical understanding of homeland security and criminal threats. Fifth, assessing performance of analysts is quite difficult but respondents highlighted the need to focus on the quality of strategic and tactical products produced. Sixth, an analysis of the types of products produced and analytical procedures used on a daily basis also highlighted some of the differences in the intelligence mission of state, local, tribal law enforcement agencies and fusion centers. Specifically, fusion centers were more likely to be fostering information sharing connections, conducting a greater range of different types of analysis, and working with public health and other hazards-related data on a daily basis. Seventh, the SLT and FC respondents noted

considerable variation in access to formal communication systems. Because of the DHS and DOJ explicit focus on developing fusion centers, it should not be surprising that the centers have more access to data bases and networks than do individual law enforcement agencies. Finally, the case studies provide valuable insights into some of the best practices of fusion centers, but also indicated that these centers are works in progress constantly having to adapt to rapid changes in their external environment.

Table of Contents

"Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies"

Executive Summary

Purpose

The September 11th attacks impacted society generally, and law enforcement specifically, in dramatic ways. One of the major trends has been changing expectations regarding criminal intelligence practices among state, local, and tribal (SLT) law enforcement agencies, and the need to coordinate intelligence efforts and share information at all levels of government. In fact, enhancing intelligence efforts has emerged as a critical issue for the prevention of terrorist acts. An increasing number of SLT law enforcement agencies have expanded their intelligence capacity, and there have been fundamental changes in the national, state, and local information sharing infrastructure. Moreover, critical to these expanding information sharing expectations is the institutionalization of fusion centers. Despite these dramatic changes, an expanding role, and the acknowledgement that local law enforcement intelligence is critical to the prevention and deterrence of terrorist acts, very little research exists that highlights issues related to the intelligence practices of SLT law enforcement agencies and fusion centers. It is important to identify best practices for enhancing the flow of good intelligence into the intelligence process by documenting the current experiences of these agencies in building an intelligence capacity. There is a critical need for describing what these agencies are doing to build an intelligence capacity, assessing the state of information sharing among agencies, identifying various barriers that impede collaborative partnerships, and developing innovative ways to measure performance in these areas, although not much is known and government and law enforcement officials are seeking solutions.

This project addresses these gaps. Specifically, a national survey was developed to examine the experiences of SLT agencies and fusion centers for building an intelligence capacity, to understand critical gaps in the sharing of information regarding intelligence, and to identify obstacles related to other key intelligence issues, such as measuring performance and communication between agencies. In addition, the activities of three fusion centers were examined to identify strategies that appear to be successful in increasing the information flow across agencies, the major obstacles of effective intelligence gathering and information sharing, and to identify the best practices for integrating domestic intelligence into the information sharing environment and overcoming these obstacles.

Research Design

In sum, there are two elements to the research design. In the first element, the research team conducted a national survey on the intelligence practices with two different samples of key personnel. The first sample consisted of personnel from fusion centers and has been involved in the development of the state-level intelligence infrastructure. The second survey sample consists of line-level officers and other individuals charged with building an intelligence capacity for individual agencies. The second element of the research design was to conduct three case studies at fusion centers to better understand how they have managed important intelligence issues.

In order to provide an overview of the major issues facing law enforcement agencies and fusion centers, the research team distributed Institutional Review Board (IRB) approved questionnaires via a web-designed survey to two groups of law enforcement personnel. The first group included individuals who had attended training programs designed and delivered by the School of Criminal Justice at Michigan State University, and funded by the Department of Homeland Security. For the most part, those individuals selected to attend the training generally

were assigned to develop or re-engineer the intelligence capacity within their agency. Most had little previous experience in law enforcement intelligence and were seeking guidance, through the training, on how to develop their intelligence capacity. This sampling strategy, which includes personnel from significantly different sized police agencies in all geographic regions of the country, was chosen for three reasons. First, in attending this training, these officers were identified by their respective SLT agency as a representative of the intelligence function within the agency. Second, as such this sample includes law enforcement personnel who have a working understanding of key issues tied to building an intelligence capacity, and thus will be able to address specifically the problems with putting knowledge into practice. Third, their awareness of the contemporary intelligence structures, requirements, and formal communication networks increases the likelihood that they will have direct knowledge about the strengths and weaknesses of these issues. Although not all agencies are represented in our sample, the diversity of agencies and personnel that have attended the training, representing all types of agencies from all levels of these organizations, ensures that the sample includes personnel that will have crucial information for understanding the problems of information sharing, performance measurement, and formal communication networks as viewed by state, local and tribal law enforcement personnel.

The second group was attendees at the 2007 and 2008 National Fusion Center Conferences. The research team decided to survey the participants at these conferences rather than sending surveys directly to fusion centers for two reasons. First, participants in the conference will not only be fusion center staff (including possibly having multiple respondents from the same center), but include others from various levels of government and a range of key disciplines. Thus, the research team assumed the sample would include a broad range of

individuals critical to effective intelligence practices in the United States. Second, the research team assumed that since most fusion centers would send multiple personnel, there would be multiple indicators on key measures for each fusion center.

The intent behind the decision to administer a web-based survey instead of a mail survey was to simplify the response process for informants and to reliably capture the data they submitted. The final drafts consisted of 103 (law enforcement survey) and 125 (fusion center survey) structured, semi-structured, or open-ended questions. Although the survey instruments were long, the research team opted for breadth and providing opportunities for the respondents to engage a variety of critical intelligence issues. In general, the surveys captured their intelligence experiences, issues related to information sharing and strategies that could promote better information sharing, how intelligence practices are assessed and what metrics are being used to measure performance, and identify the communication networks that exist for information sharing. The research team also collected several indicators on the type of agency, role of intelligence in the agency, and characteristics of the respondent.

The research team also completed three in-depth case studies of fusion centers. The data collection strategy for the case studies was to select two that were using innovative strategies to address these critical issues. These agencies were identified through the surveys, contacts with key staff, and in consultation with the grant program manager and subject matter experts. In addition, the third case study was chosen in order to interview personnel who were working in a fusion center in transition. The research team concluded that since fusion centers are at various points of development that it was critical to receive input from an emerging fusion center that was managing challenging issues (e.g., change in management and other personnel; developing

new policies and procedures; staff learning new job responsibilities, developing new information sharing partnerships).

For each fusion center that was selected, the research team began by compiling and analyzing open source documents regarding their efforts to address these issues. In addition, site visits were conducted to better understand their relationship and work in the intelligence area. The research team provides an overview of the structure, activities, and development of each fusion center, and discusses best practices for responding to critical issues examined in the survey. The primary focus of each case study was to better understand the issues addressed in the survey: intelligence practices, information sharing, performance measurement, and communication networks. Other issues examined include experience with terrorism incidents and the production of intelligence regarding the terrorist threat, organizational structures that are part of the law enforcement intelligence community, collection requirements and reasons for relying on particular types of raw information, coordination, and information sharing practices within an agency, key assessment and evaluation activities, the important legal, cultural, and political issues that impact these processes, the role of intelligence in overall law enforcement operations, and perspectives of cooperation internally and externally.

Findings

The research team surveyed state, local, and tribal law enforcement officers and fusion center personnel and conducted three case studies to better understand intelligence practices, information sharing, performance metrics, and communication networks. This section highlights some of the key findings.

1. It appears that significant progress has been made post 9/11 installing fundamental policy and procedures related to building the intelligence capacity of law enforcement and fusion center agencies. Both respondents from state, local, tribal law enforcement agencies and fusion centers indicated that they were familiar with intelligence guidelines and standards, had a good working knowledge of threats in their community, and have some working knowledge of intelligence-led policing. Personnel also indicated that they have attempted to take advantage of the wide range of training opportunities available for intelligence analysts.

2. Despite the progress that has been made, there is significant room for improvement and development. For example, although respondents indicated that they were familiar with national standards and guidelines, they also expressed the belief that the policies and procedures within their agency have yet to reconcile with these requirements. Similarly, the respondents noted they were aware of the threats, but identified a need to build a capacity to better identify these threats and noted shortages in resources and personnel in accomplishing these goals. Also, they were aware of key civil rights and privacy issues, but respondents reported there is considerable work that needs to be done in their agencies to ensure agencies are fully compliant.

3. Fusion centers appear to be farther along addressing many different issues, including instituting an intelligence-led policing philosophy, establishing and being compliant with privacy issues, and fostering relationships with other agencies. Not all fusion centers were fully functional at the time of the survey, but had plans and goals to provide them direction along with guidance available from their peers as well as federally-supported training and technical assistance.

4. Critical to prevention and response is the sharing of information. In addition, it is clear that a wide range of law enforcement, community, government and private businesses may have information that is important to the intelligence fusion process thus it is important to build relationships with a diverse range of agencies and organizations. Both SLT and fusion center respondents indicated that that they have worked at building relationships with different agencies especially other law enforcement agencies, but fusion centers had closer relationships with a more diverse range of agencies and were more likely to be working with National Guard, transportation, public health, homeland security, emergency management, fire marshal, and critical infrastructure personnel.

5. Although many information linkages have been established, the respondents also indicated that they were not completely satisfied with these relationships. That is, it appears that the personnel were working with other agencies and making connections, but they think the relationships need further development to ensure consistent, substantive and timely information sharing.

6. There is an overwhelming amount of information going into and out of these agencies, and it is likely, without having enough analysts within the organization or analysts not effectively trained to process this information, that there are missed opportunities for strategic and tactical understanding of homeland security and criminal threats.

7. Both SLT and FC respondents agreed that the quality of intelligence products produced should be critical to the assessment of performance by analysts. There was some variation when comparing the two samples of respondents Information sharing and the quality of products was somewhat more important to fusion center respondents while having intelligence that led specifically to arrests, investigations, and convictions was

more important to the SLT agency respondents. This difference may be indicative of a misunderstanding among SLT officers regarding the value and purpose of intelligence analysts as well as the responsibility of operational units to act on the intelligence products in order to interrupt threats and pursue investigations

8. An analysis of the types of products produced and analytical procedures used on a daily basis also highlighted some of the differences in the intelligence mission of state, local, tribal law enforcement agencies and fusion centers. Specifically, fusion centers were more likely to be fostering information sharing connections, conducting a greater range of different types of analysis, and working with public health and other hazards related data on a daily basis. This should be expected given the roles and national standards for fusion centers.

9. It is important to consider the formal communication patterns that support and impede the intelligence process. These systems are critical because they provide an additional way for homeland security and intelligence officials to promote a necessary understanding of the procedures that need to be followed for better information sharing. The findings that were presented indicated that both SLT and FC respondents think that they have access to key communication systems and other sources of information that might be used to enhance intelligence products. Fusion center respondents were however somewhat more critical when asked whether RISS.net, LEO, HSIN, ATIX, and FBINET meet their intelligence and information sharing needs. Not surprisingly, the results also indicated that a higher percentage of fusion center respondents noted that they had access to various critical sources of intelligence information, including HSIN, RISS.net, FBINET, LEIU, and Health Related data.

10. The case studies of fusion centers are valuable in that they provide in-depth coverage of structural, policy, and strategic approaches that have been successful. The organizations studied were guided by a litany of formal policies and comprised of multiple task-specific units. These formalities allow for a strategic division of labor for specialized persons to perform specialized tasks – thus improving effectiveness and efficiency.

11. Each of the case studies also revealed that the fusion centers were "works in progress" and that the agencies had to update and embrace changes motivated by shifts in their external environment. For example, the Florida Fusion Center conducted an assessment of information sharing gaps between law enforcement agencies within the state of Florida. One of the findings from this gap analysis was that local law enforcement was not engaging in information sharing as a result of poor, or nonexistent, commitment to the intelligence-led approach. At the Southern Nevada Counter-Terrorism Center, a strong administrative commitment to an intelligence-led approach was established when Sheriff Doug Gillespie announced (multiple times) that the Las Vegas Metro Police Department (the primary agency of the SNCTC) was going to fully embrace this new philosophy.

Policy Implications

The status of law enforcement intelligence in SLT agencies appears to be similar to the early development of community- and problem-solving policing during the early 1990s. Law enforcement officers and executives recognize the importance of intelligence yet the implementation of law enforcement intelligence remains uneven a decade after 9/11. Several factors may contribute to this. First, the philosophical underpinnings of law enforcement

intelligence was significantly changed and broadened, hence a resocialization process among intelligence personnel had to occur. Second, while the 9/11 attacks remain as the benchmark for change, in reality new standards – such as the National Criminal Intelligence Sharing Plan and training programs did not emerge until 2003. Moreover, new standards and directions continue to evolve even at the time of this writing. Third, it simply takes time to develop new organizations such as fusion centers and get them at an operational level. Similarly, training and developing new policies in America's 16,000 law enforcement agencies is a massive task, particularly when new processes – such a participating in a fusion center – must be marketed and sold to the agencies as wise investment in resources.

Uneven development and evolution is even more the case when considering the intelligence-led policing philosophy and practice. Although respondents were familiar with the term ILP, the results suggest that most agencies are at an early stage of implementation. Indeed, there are different conceptual understandings of ILP and different visions of the role ILP should hold in law enforcement organizations. Like the community policing movement, these results reveal clear needs for training and commitment of resources and for addressing the tension between specialization and generalization. Additionally, the goal of increasing intelligence capacity and adopting ILP comes at a time that SLT agencies operate under significant budgetary constraints. Finally, the results suggest the potential for fusion centers to serve a critical role in continued development of the law enforcement intelligence capacity in local agencies.

Although the results of this study point to clear progress in the development of law enforcement intelligence capacity, they also reveal challenges. Clearly, there is a need for the commitment of resources in the form of personnel and training. Given the federated and decentralized structure of law enforcement in the U.S., it is critical that mid- to large agencies

have analysts who can conduct local level analysis as well as push information and intelligence to Fusion centers.. Small agencies need to have intelligence liaison officers who can serve as "nodes" in the intelligence network. This requires commitment of resources at a time that many agencies are not hiring or even cutting personnel. Law enforcement executives as well as policymakers at local, state, and federal levels will need to consider the implications of these budgetary issues. While many executives acknowledge that the use of analysts make the agency "work smarter" thereby having a great effect on crime and community order, it remains a difficult concept to sell to the public and politicians.

It is also clear that there is a need for continued and expanded training. This includes specific training for analysts, fusion center personnel, and intelligence managers. It also, however, means more general training for all SLT personnel on ILP and the role of SLT officers in the intelligence process to include what types of information can be shared, the process for sharing information, and the application of guidelines to protect privacy, civil rights and civil liberties.

Law enforcement executives also need to seriously consider and resolve several issues related to specialization and generalization. At one level is the issue of whether the intelligence capacity is viewed as specifically focused on homeland security and the threat of terrorism or whether it is viewed as building "all-crimes, all-hazards" capacity. On the one hand, the need to develop capacity and expertise focused on terrorism can justify a more specialized focus. As the commander of a local police department intelligence unit told us, "what keeps me awake is missing a tip or lead suggesting an Al Qaeda-type attack." On the other hand, the results of this study, combined with prior studies, suggests the potential power of the "all-crimes, all-hazards" focus. Prior research demonstrates the high level of involvement of terrorist groups in a variety

of criminal activity that brings these individuals in contact with SLT agencies (Damphouse and Smith, 2004; Smith et al. 2002; Hamm, 2005). The present study indicates a high proportion of Suspicious Activity Reports involving all-crimes. These results suggest that the continued development of the network of SLT agencies, linked to fusion centers and federal law enforcement and ultimately linked to the Intelligence Community (with appropriate firewalls and privacy safeguards) will be best served through the all-crimes, all-hazards information flow. Additionally, it strikes us that the costs of the investment in intelligence capacity will yield the greatest benefits for SLT agencies when the capacity equips such agencies to address not only terrorism but a range of criminal threats (e.g., organized crime, gangs, violent crime, drugs).

A parallel question of specialization/generalization relates to training and responsibilities within SLT agencies. On the basis of these findings, it appears that most agencies to date have developed intelligence capacity through training of officers and analysts dedicated or at least focused on intelligence assignments. Thus, the respondents to our surveys indicate a fairly high level of knowledge and expertise themselves but report much lower levels of familiarity throughout the organization. Again, this is similar to early stages of community- and problem-oriented policing when specialist officers were tasked with implementation but the majority of officers and supervisors focused on so-called "real policing." The danger is that the intelligence function becomes a specialized function divorced from the larger organization, what Toch and Grant (1991) once referred to as an "innovation ghetto." The risk is that information flow from street-level officers and investigators to analysts does not occur. Similarly, analysts do not fully understand the needs of officers and investigators. This, too, suggests the need for broad training on the intelligence function, the role of analysts, and ILP.

The development of a national network of 72 fusion centers (as of this writing) represents a monumental undertaking and achievement. Yet, there has been criticism of the fusion centers in two broad areas: Fusion center operations and the protection of civil liberties. The results of the current study suggest that the fusion centers are playing a critical role in the nation's domestic intelligence capacity and could play an even more important role in the future. The co-location of personnel from SLT, federal law enforcement and, in some cases, the private sector appears to mitigate some of the historic, cultural, and organizational barriers to information sharing. Consequently, the fusion center's occupy an organizational or network "space" that is "closer" to both federal law enforcement and the SLTs. They appear to be a critical network "node" for the movement of information and intelligence "up-from" and "back-to" the local level. Further, the survey results and case studies reflect the specialized expertise in terms of both human capital (analysts) and technology that many SLT agencies will never attain (with the exception of large metropolitan departments). The fusion centers are already displaying an impressive range of information sources and high frequency actionable intelligence products. Based on these findings, the loss of these fusion centers would result in both a loss of analytic capability and a disconnect between SLT and federal law enforcement and ultimately the intelligence community. Consequently, these results appear to call for continued investment and development of the network of fusion centers.

Perhaps the most critical point for successful intelligence is the quality of the analysis. The need for continual training of analysts, particularly in the area of critical thinking, and the recognition that analysts are practicing professionals – not simply "civilians in the intelligence unit" – are among the factors which need to be recognized and address by law enforcement

leaders. Greater attention by management needs to be provided for the professional development of intelligence analysts in order to increase the quality and utility of analytic outputs.

"Understanding the Intelligence Practices of State, Local, and Tribal Law Enforcement Agencies"

Chapter 1: Introduction

The September 11th attacks impacted society generally, and law enforcement specifically, in dramatic ways. One of the major trends has been changing expectations regarding criminal intelligence practices among state, local, and tribal (SLT) law enforcement agencies, and the need to coordinate intelligence efforts and share information at all levels of government. In fact, enhancing intelligence efforts has emerged as a critical issue for the prevention of terrorist acts. An increasing number of SLT law enforcement agencies have expanded their intelligence capacity, and there have been fundamental changes in the national, state, and local information sharing infrastructure.[1] Moreover, critical to these expanding information sharing expectations is the institutionalization of fusion centers. Despite these dramatic changes, an expanding role, and the acknowledgement that local law enforcement intelligence is critical to the prevention and deterrence of terrorist acts, very little research exists that highlights issues related to the intelligence practices of SLT law enforcement agencies and fusion centers.[2] It is important to identify best practices for enhancing the flow of good intelligence into the intelligence process by documenting the current experiences of these agencies in building an intelligence capacity. There is a critical need for describing what these agencies are doing to build an intelligence capacity, assessing the state of information sharing among agencies, identifying various barriers that impede collaborative partnerships, and developing innovative ways to measure performance

[1] Many of these changes are a product of the Intelligence Reform and Terrorism Prevention Act of 2004 which created the Information Sharing Environment (ISE). The ISE has had a significant influence on the development of fusion centers and intelligence-related programming of SLT law enforcement agencies, such as the Nationwide Suspicious Activity Reporting Initiative (NSI).

[2] Since many of the changes in law enforcement intelligence did not occur until 2003 or after, the true growth of fusion centers did not begin until around 2004-05, it is not surprising that there is little scientific research.

in these areas, although not much is known and government and law enforcement officials are seeking solutions.

This project addresses these gaps. Specifically, a national survey was developed to examine the experiences of SLT agencies and fusion centers for building an intelligence capacity, to understand critical gaps in the sharing of information regarding intelligence, and to identify obstacles related to other key intelligence issues, such as measuring performance and communication between agencies. In addition, the activities of three fusion centers were examined to identify strategies that appear to be successful in increasing the information flow across agencies, the major obstacles of effective intelligence gathering and information sharing, and to identify the best practices for integrating domestic intelligence into the information sharing environment and overcoming these obstacles.

Relevant Literature

Since the terrorist attacks of September 11th, there has been a considerable investment of resources in many different government sectors to better prepare, respond, and recover from terrorism. One critical investment area has been in improving the law enforcement intelligence capacity at all levels of government. The changes in the intelligence practices for state, local, and tribal agencies has been particularly pronounced. Many law enforcement agencies had eliminated their intelligence units, starting in the late 1960s, in reaction to a proliferation of civil rights lawsuits alleging systemic practices of collection and retaining information about people where there was no articulable nexus between the individual and criminal activity. In the 1980s there was some significant restructuring of state and local law enforcement intelligence as a result of several factors:

- Structural and policy changes to intelligence units, predominantly in major cities and states, that were built on the precedence set in civil rights cases relating to law enforcement intelligence practices.
- The implementation of 28 CFR Part 23 by the Justice Department's Office of Legal Policy which established guidelines for the collection, retention, review, dissemination and purging of information in federally funded, multijurisdictional criminal intelligence records systems that were managed by state or local law enforcement agencies.
- The articulation of the Law Enforcement Intelligence Unit (LEIU) File Guidelines which made 28 CFR Part 23 more "policy-based" and, as a *de facto* effect, set the standard that the guidelines should be used by all law enforcement agencies, whether or not they received federal funds.
- The expansive growth (and reach) of the drug trade, largely driven by the Columbian drug cartels, required a different approach to drug investigations, relying on intelligence and information sharing.[3]

Following the September 11th attacks, and more specifically following the March 2002 IACP/COPS[4] Intelligence Summit, it was recognized that to provide an effective and comprehensive barrier to future terrorist attacks law enforcement agencies had to re-engineer their current intelligence capacity and, in many cases, they had to build an intelligence capacity from the ground up. The concept and application of law enforcement intelligence was beginning a metamorphosis at that time, driven by new concepts and standards, largely being driven by the

[3] The High Intensity Drug Trafficking Area (HIDTA) Intelligence Centers are one of the best examples of this.
[4] International Association of Chiefs of Police (IACP) and Office of Community Oriented Policing Services (COPS).

Global Intelligence Working Group (GIWG) and the Criminal Intelligence Coordinating Council (CICC). (Many of these changes are currently ongoing). New resources and training opportunities were becoming available and change was occurring comparatively fast. Among the challenges were that agencies were having difficulty accepting the changes, both conceptually and from a staffing perspective.

One significant factor that occurred was that the GIWG developed the National Criminal Intelligence Sharing Plan (NCISP) which recommended, among other things, that every law enforcement agency, regardless of size, develop an intelligence capacity. The purpose was to "understand the implications of information collection, analysis, and intelligence sharing," and "must have an organized mechanism to receive and manage intelligence as well as a mechanism to report and share critical information with other law enforcement agencies" (Carter, 2009: 1). The development of this capacity has resulted in a significant expansion of the intelligence function in law enforcement agencies, the institutionalization of intelligence units, and a significant need for providing intelligence training to all levels of law enforcement.

The growth of intelligence practices in SLT agencies has coincided with an increasing acknowledgement within various levels of government of the importance of SLT law enforcement for enhancing the value of intelligence related to terrorism (see Cilluffo, Clark and Downing, 2011). Congress made it generally clear in the Homeland Security Act of 2002 that state and local information was critical for preventing and preparing for terrorist events, and that federal, state, and local entities should work to embrace strategies that would dramatically increase the sharing of information (see General Accounting Office, 2003; 2007; President's National Strategy for Information Sharing, 2007). Perhaps more importantly, the Information Sharing Environment Implementation Plan, a product of the *Intelligence Reform and Terrorism*

Prevention Act of 2004, placed significant responsibilities on state and local law enforcement agencies for collecting and sharing information for purposes of countering terrorism (PM-ISE, 2006.) This conclusion highlights the recognition that each level of government has unique information sources within its specific environment and is in a position to harness its various assets in the most effective way to accomplish the broad goals of the counterterrorism mission.

The importance of SLT's contribution to the intelligence process can be highlighted in several ways. First, the National Strategy for Information Sharing (2007) highlights the importance of sharing threat information with many sectors of society, and specifically highlights the need for SLT law enforcement agencies to foster a culture of fusing information on crime and terrorist related incidents, support efforts to detect and prevent attacks, and develop training and awareness programs on terrorism. Second, although the Federal Bureau of Investigation is the lead agency for the investigation of terrorism, the types of information provided by various sources and the sheer number of cases and leads requiring follow-up, highlights the importance of involving local law enforcement in terrorist investigations (Davis et al., 2004). Third, it is critical to note that terrorism is a local event, and as such SLT law enforcement agencies are in a unique position to contribute important raw information based on their knowledge about the criminal activities of individuals, groups, and organizations operating in local communities. One report states, "The 800,000 plus law enforcement officers across the country know their communities most intimately and, therefore, are best placed to function as the 'eyes and ears' of an extended national security community. They have the experience to recognize what constitutes anomalous behavior in their areas of responsibility and can either stop it at the point of discovery (a more traditional law enforcement approach) or follow the anomaly or criminal behavior, either unilaterally or jointly with the Federal Bureau of Investigation (FBI),

to extract the maximum intelligence value from the activity (a more intelligence-based approach)" (Masse, O'Neil, and Rollins, 2007). In addition, there is evidence in both cases of international and domestic terrorism where state and local law enforcement officers have encountered terrorists through such activities as traffic stops, yet did not know the threat these individuals posed because of information barriers. This clearly highlights the need for SLT law enforcement agencies to have access to timely and actionable intelligence which may lead to the prevention and response to terrorist acts (see Cilluffo, Clark and Dunning, 2011; Cooney, Rojek, and Kaminski, 2011; 9/11 Commission Report). Fourth, critical infrastructures and high-value targets are dispersed widely in the United States, and many of these potential targets are located in rural and less-populated areas. Local law enforcement agencies in these communities are in the best position to recognize when suspicious situations occur near these critical targets. Fifth, survey research, supported by extensive anecdotal experience of the research team, indicates that the terrorism experiences and expectations regarding intelligence work of state and local agencies increased after September 11th (Davis et al., 2004).

Terrorism scholarship examining the behaviors and patterns of terrorists operating on U.S. soil also supports the conclusion that there are significant opportunities for SLT law enforcement agencies to significantly enhance the amount, quality, and reliability of both critical sensitive information and intelligence. Brent Smith and colleagues' American Terrorism Study is one of the most important domestic terrorism data collection efforts to date (Smith, 1994). This project, conducted in cooperation with the FBI's Terrorist Research and Analytical Center, includes persons under federal indictment as a result of an investigation under the FBI's Counterterrorism Program. These researchers were provided lists (1980-1989; 1990-1996; 1997-2002) of persons indicted, and then traveled to federal courthouses to collect data from trial

transcripts and docket information. These data have been used by various principal investigators to answer a variety of important questions, including the prosecution and punishment of international and domestic terrorists (Smith, Damphousse, Jackson and Sellers, 2002), prosecutorial strategies in terrorism cases (Smith and Orvis, 1993), and the empirical validation of the growth of leaderless resistance tactics (Damphousse and Smith, 2004). These data highlight that the base of operations for domestic right-wing groups is rural areas and left-wing groups operate generally in urban areas. Similarly, Smith and colleagues found that terrorists are much more likely to engage in planning activities and to commit preparatory crimes compared to traditional criminals, and importantly the patterns of preparatory conduct vary by type of terrorist group (Smith, Damphousse, & Roberts, 2006). For example, they found that right-wing terrorist groups are more mobile than international terrorists, and tend to commit crimes farther from their home. Smith and colleagues concluded that this may either be evidence that far-right groups have broader support networks which allow them to freely to move around the country or it could reflect that far-right terrorists tend to reside in rural locations (p. 46). It was found that left-wing and international terrorist groups committed many more preparatory crimes compared to right-wing and single issue terrorist groups and were more likely to separate their acts from their targets (pp. 36; 52). Findings such as this can be an important source of information used in strategic intelligence analysis. It can help refine the parameters of the threat picture and provide direction for the development of investigative leads.

Similarly, Hamm (2005) compared the types of crimes committed by international and domestic terrorist groups. His analysis of data from the American Terrorism Study found that international terrorists were statistically more likely to commit aircraft violations, motor vehicle crimes, violations of explosions, and some types of firearms violations. In contrast, domestic

terrorists were more likely to commit mail fraud, racketeering, robbery, burglary, and violations of destructive devices. He stressed that both international and domestic terrorists come into contact with law enforcement in the normal course of crime investigations because of their failures, the types of crimes they commit, and their preparatory activities. Hamm concluded that his study provides "strong empirical support for the notion that terrorist-oriented criminality has distinguishing features" (p. 22), and that these "different crimes require different skills and opportunities and identifying these differences may take law enforcement a step closer to prevention" (p. 19). Once again, the value of these findings can be useful for giving direction to the types of information that should be collected for both strategic and tactical intelligence analysis.

These research studies clearly show the great potential of strengthening intelligence capabilities and enhancing the information sharing among agencies in different geographic locations and in other branches/jurisdictions of government. But not much is known about the status of SLT intelligence practices. It is critically important to first describe how law enforcement personnel have responded to the need to build an intelligence capacity. Are they familiar with national intelligence standards? Intelligence-led policing? Fusion center resources and capabilities? Terrorism/Intelligence Liaison Officer programs? Constitutional standards and restrictions unique to the intelligence process? Have they been trained to national standards and do they feel as though there agency is prepared to effectively contribute to the intelligence enterprise of the Information Sharing Environment?

In addition to describing the current state of intelligence practices among SLT law enforcement agencies, this study also examines the fusion center perspective on these critical intelligence issues. One of the important roles that state fusion centers is intended to play in the

information sharing environment is to act as a conduit between SLT agencies and both the federal law enforcement agencies and the intelligence community. It is thus important to highlight the status of several issues critical to building an intelligence capacity in both SLT agencies and fusion centers. This study highlights issues related to information sharing, the evaluation of performance in intelligence agencies, and how and what information is being shared across intelligence networks. A better understanding of these issues and the identification of innovative ways that they might be better addressed, could significantly enhance the effective use of intelligence practices to define threats and ultimately enhance public safety. These specific areas of this project are discussed in more detail below. In addition, this report highlights how these issues have been addressed by specific agencies in order to provide insights into how to address critical issues in collecting substantive information for the intelligence process.

Information Sharing

There have certainly been specifically directed efforts to implement initiatives to address concerns about information sharing. For example, the creation of the Global Intelligence Working Group (GIWG) and their first product, the National Criminal Intelligence Sharing Plan (NCISP), has been critically important for developing an effective intelligence capacity among state, local, and tribal law enforcement agencies and, consequently enhancing information sharing at all levels of government. In addition, the number of Joint Terrorism Task Forces (JTTF) has increased dramatically since 9/11 which, while investigative bodies, utilize the products of the intelligence process as well as aid in collecting information that meets intelligence requirements. The development of state and major urban area fusion centers has also

had a significant effect on intelligence production and information sharing. While the seventy-two officially recognized fusion centers are under the control of their respective state or local jurisdiction, they comply with federal standards, serve as a clearinghouse of information for DHS and generally provide opportunities for federal, state, and local law enforcement to share and disseminate information about terrorism and criminal threats. Finally, the *Intelligence Reform and Terrorism Prevent Act of 2004* mandates that the President establish an Information Sharing Environment (ISE). The implementation plan for this ISE, which was released in November 2006, states that "This environment will create a powerful national capability to share, search, and analyze terrorism information across jurisdictional boundaries and provide a distributed, secure, and trusted environment for transforming data into actionable information. The resulting environment will also recognize and leverage the vital roles played by State and major urban area information fusion centers, which represent crucial investments toward improving the nation's counterterrorism capacity" (p. xiv).

While this responsibility has developed more slowly, there have been significant strides in the last two-three years. While there has been a significant void in empirical research that attempts to examine issues related to information sharing among law enforcement agencies, there is some work that provides a general understanding of relatively recent concerns, but only one is a national study that specifically focused on state, local, and tribal law enforcement agencies.

First, the General Accounting Office (2003) reviewed critical documents related to information sharing, interviewed officials from various agencies, and surveyed 29 federal law enforcement agencies, all 50 home security offices, all cities with a population of 100,000 or greater (N=485), and a random sample of smaller cities (N=242). The surveys were sent to the mayor who either completed the survey or delegated the completion to the chief of police, an

assistant, or other emergency management personnel. There were many important findings highlighted in this report, but several concern information sharing limitations. Among these findings were that: 1). Officials from federal, state, and local governments do not think the process of sharing information is "effective" or "very effective;" 2). They do not routinely receive the information they need to protect the homeland; 3). The information received is not timely; 4). Opportunities are routinely missed to obtain and provide information to the federal government; and 5). Law enforcement agencies are not receiving the types of information they need to effectively prevent terrorist attacks. Importantly, it should be noted that when these data were collected in 2003, virtually none of the currently available information sharing tools were in place, including fusion centers.

The Major Cities Chiefs Association (MCC) examined the intelligence and information sharing needs between major city law enforcement agencies and federal law enforcement. Some of the observations in the MCC position paper are particularly important for the current project. The chiefs conclude that the federal government must better integrate local law enforcement to take full advantage of their capabilities (p. 17), and they also stated that with background on terrorists and timely intelligence, "law enforcement would have the background from which it could take seemingly random or unconnected events—such as minor traffic violations—and place them into a larger context, thereby being able to perceive a bigger picture of potential attack or recognize the need to pass the information to an appropriate homeland security partner agency" (p. 22).

The RAND Corporation has conducted two national surveys related to domestic preparedness and intelligence (Riley and Hoffman, 1995; Riley, Treverton, Wilson, and Davis, 2005). The 1995 survey focused on preparedness issues for state and local law enforcement.

The important conclusion of the study was that there was very little intelligence and strategic assessment capability and poor information sharing between federal and state law enforcement officials. Of course, the significant changes that were produced in the post-9/11 era, largely under GIWG leadership were intended to address these problems.

Prior to the establishment of the Department of Homeland Security, RAND did a second survey and several case studies to examine issues related to local and state intelligence efforts. The study concludes that SLT law enforcement agencies have played an increasingly important role in responding to and preventing terrorism. Law enforcement agencies wanted better intelligence sharing, needed improvements in communication interoperability, and thought that training improvements were necessary. In addition, even small agencies, if assessing their threat risk as high, were very proactive in focusing their preparedness efforts.

Recently, the Homeland Security Policy Institute published a research brief that highlighted the results of a survey that was administered to individuals attending the Intelligence Unit Commanders Group of the Major Cities Chief Association (Cilluffo, Clark and Downing, 2011). Forty-two surveys were completed. Several of the findings highlighted in the research brief relate to the issues examined in this study. First, they found that all respondents had a working relationship with their local fusion center, and the respondents thought there was value in maintaining that relationship. Second, the respondents were willing to share information through key channels, such as the FBI's National Data Exchange and Nationwide Suspicious Activity Reporting Initiative. Third, they noted that they preferred to share information locally first, then regionally, and then finally federally. Fourth, the respondents indicated that their best source of terrorism information was the FBI's Joint Terrorism Task Forces followed by the local fusion centers.

Although it is generally understood that intelligence must be shared widely, there has been very little empirical research that identifies key obstacles to information sharing. The studies discussed above provide valuable background information and highlights some of the key obstacles in effectively using state and local intelligence in the war of terrorism. However, the GAO study does not specifically focus on law enforcement efforts and the RAND study was conducted in 2002 prior to the establishment of the Department of Homeland Security and before the GIWG had issued any of its standards, recommendations or best practices. The brief by the Homeland Security Policy Institute is based on surveys completed by only respondents from major cities. The field of intelligence has changed incredibly since 2002, and it is important to examine current issues specific to law enforcement efforts in the area of intelligence. In addition, these studies do not focus on the efforts to improve intelligence flow and there has not been a systematic attempt to examine how fusion centers strategically fuse intelligence and what promising strategies exist to enhance information sharing.

Performance Measures and Intelligence

There is clearly a need for the development of performance standards related to information collection, intelligence analysis, and information sharing. A key maxim of organizational behavior is that what gets measured gets done (Osborne and Gaebler, 1992). The absence of performance measures and metrics for law enforcement intelligence makes it impossible for policymakers to assess progress towards enhancing the Information Sharing Culture, and leaves fusion centers and individual agencies vulnerable to intelligence gaps.

In general, the accurate measurement of performance related to intelligence has several potential benefits (see General Accounting Office, 2006; Johnson, 2005). First, these measures

are valuable for the improvement of programs and strategies. Second, change is most likely to occur in iterative steps, and thus accurate performance measures can help an organization monitor improvement steps, highlight problem areas, and suggest approaches for accomplishing goals. Third, such measures would be valuable in making personnel allocation, training needs and allocating resources within the organization. Fourth, such measures can hold organizations and individuals accountable for accomplishing goals. Finally, according to a GAO report (2006, p. 11), "in a risk management process, agencies can use performance measurement to assess progress towards meeting homeland security goals. The intended effect of assessing such progress, when coupled with other aspects of the risk management process, is the reduction of risk." Beyond these organizational factors, an overarching measure important for law enforcement intelligence is ensuring that all information collection, retention and dissemination activities are consistent with constitutional standards.

There is very little evidence that intelligence performance and the products of information sharing are being consistently and empirically measured in any meaningful way. Intelligence leaders and analysts, however, have provided anecdotal support for the conclusion that there are significant limits to both the amount and quality of information shared, and have voiced frustrations about the inability to accurately assess performance. The problem may not be a lack of data and information, but just the opposite: state fusion centers and analysts have been overwhelmed with data but are only receiving limited actionable information. This problem is significant because such information still has to be processed, thus leaving little time to focus on producing helpful analytic products and distributing reports. In many instances, it also appears that intelligence products disseminated by fusion centers may simply be a "re-packaging" of intelligence products, not new information. According to Treverton et al. (2006: 14), "the United

States has been obsessed with data, and that has come at the expense of judgment. Rather than maintaining the ideal of speaking truth to power, intelligence has focused on gathering information. In many ways, this is a function of wealth—a big budget can buy lots of gadgets. The problem is that with all these so-called added capabilities, technologists assert we can collect everything."

Communication

A final, but related issue to the research areas discussed above, concerns our examination of how SLT law enforcement agencies communicate information about intelligence issues, the formal communication systems, the general understanding and ratings of usefulness of the technical systems that exist for information sharing, and identifying best practices to address issues related to communication and user acceptance. Communications in the intelligence process has three broad elements: technology, policy and human.

Communication is a challenge for all organizations, but the autonomy of each law enforcement agency and fusion center functionally equates to a fragmented structure of law enforcement intelligence in the United States that increases the difficulties in communicating effectively. The flow of communication across the ISE is thus dependent on the capacity of SLT, their ties to fusion centers, and the links to federal agencies and the private sector. Consequently, regardless of agency size, law enforcement needs timely and reliable information to conduct criminal inquiries and respond effectively in crisis situations. Of particular importance are how important procedures and policies about intelligence are understood and practiced by SLT law enforcement agencies and what mechanisms exist to enhance the sharing of these ideas in the current environment.

Research Design and Methods

In sum, there are two elements to the research design. In the first element, the research team conducted a national survey on the intelligence practices with two different samples of key personnel. The first sample consisted of personnel from fusion centers and has been involved in the development of the state-level intelligence infrastructure. The second survey sample consists of line-level officers and other individuals charged with building an intelligence capacity for individual agencies. The second element of the research design was to conduct three case studies at fusion centers to better understand how they have managed important intelligence issues.

Surveys of Key Personnel

In order to provide an overview of the major issues facing law enforcement agencies and fusion centers, the research team distributed Institutional Review Board (IRB) approved questionnaires via a web-designed survey to two groups of law enforcement personnel. The first group included individuals who had attended training programs designed and delivered by the School of Criminal Justice at Michigan State University, and funded by the Department of Homeland Security. For the most part, those individuals selected to attend the training generally were assigned to develop or re-engineer the intelligence capacity within their agency. Most had little previous experience in law enforcement intelligence and were seeking guidance, through the training, on how to develop their intelligence capacity. This sampling strategy, which includes personnel from significantly different sized police agencies in all geographic regions of the country, was chosen for three reasons. First, in attending this training, these officers were identified by their respective SLT agency as a representative of the intelligence function within the agency. Second, as such this sample includes law enforcement personnel who have a

working understanding of key issues tied to building an intelligence capacity, and thus will be able to address specifically the problems with putting knowledge into practice. Third, their awareness of the contemporary intelligence structures, requirements, and formal communication networks increases the likelihood that they will have direct knowledge about the strengths and weaknesses of these issues. Although not all agencies are represented in our sample, the diversity of agencies and personnel that have attended the training, representing all types of agencies from all levels of these organizations, ensures that the sample includes personnel that will have crucial information for understanding the problems of information sharing, performance measurement, and formal communication networks as viewed by state, local and tribal law enforcement personnel.

The second group was attendees at the 2007 and 2008 National Fusion Center Conferences. The research team decided to survey the participants at these conferences rather than sending surveys directly to fusion centers for two reasons. First, participants in the conference will not only be fusion center staff (including possibly having multiple respondents from the same center), but include others from various levels of government and a range of key disciplines. Thus, the research team assumed the sample would include a broad range of individuals critical to effective intelligence practices in the United States. Second, the research team assumed that since most fusion centers would send multiple personnel, there would be multiple indicators on key measures for each fusion center.

The intent behind the decision to administer a web-based survey instead of a mail survey was to simplify the response process for informants and to reliably capture the data they submitted. A group of state, local, and tribal law enforcement intelligence leaders, who constitute the Advisory Board of the Michigan State University Intelligence Program, served as

subject matter experts and scrutinized preliminary drafts; a separate group of law enforcement officials then took part in a pretest of both surveys to identify ambiguous or poorly worded questions, issues that were overlooked, and items that could be potentially difficult to answer correctly. The final drafts consisted of 103 (law enforcement survey) and 125 (fusion center survey) structured, semi-structured, or open-ended questions. Although the survey instruments were long, the research team opted for breadth and providing opportunities for the respondents to engage a variety of critical intelligence issues. In general, the surveys captured their intelligence experiences, issues related to information sharing and strategies that could promote better information sharing, how intelligence practices are assessed and what metrics are being used to measure performance, and identify the communication networks that exist for information sharing. The research team also collected several indicators on the type of agency, role of intelligence in the agency, and characteristics of the respondent.

The surveys were administered using software purchased by Michigan State University that is ideal for web-based survey design and data collection (see SnapSurvey.com). Prior to the data collection phase, it was necessary to ensure no individuals appeared in both sampling frames. In early June 2009 an e-mail was sent to each addressee outlining the purpose of the study and inviting them to complete a self-administered, online questionnaire. The research team recorded replies that took the form of automated server notifications telling us the source addresses were invalid and formal refusals, and then corrected the sampling frame by removing individuals who could not be contacted in addition to those who declined to participate.

Invitation e-mails were sent to the law enforcement sample of 2,882, followed by 2395 e-mails with a unique identifier and one of two URLs a respondent could use to access the appropriate survey a week later. In the case of the fusion center sample, 872 invitations and 772

follow up emails were transmitted. As e-mail replies and survey submissions appeared, the research team readjusted the sampling frames so subsequent requests targeted only those who had not communicated with us. Further follow up e-mails were issued a second, third, and fourth time at approximately monthly intervals; the fifth and final reminders were sent at the end of March 2010 and the collection window closed a month later.

Table 1.1: Numbers of responses by intelligence workers.

	Group	
Responses	Law enforcement	Fusion centers
Valid	414	88
Undelivered email	313	52
Declined	57	31

Table 1.1 shows the response totals the research plan elicited. Using the formula of valid responses / (first phase invitations - undelivered invitations - declined invitations), the response rate for individual respondents was 20.4 percent for the law enforcement sample and 12.8 percent for the fusion center sample.

The response rate was lower than expected. In order to learn why the response rates were not higher, the research team conducted follow up telephone interviews with 100 randomly selected participants in the law enforcement sample. Among the key reasons that were consistently reported for not responding were:

1. Job responsibilities. A number of individuals stated that they had been reassigned or promoted and no longer worked in the intelligence function. As a result they either felt the survey no longer applied to them or they were not familiar with current activities in the intelligence function.
2. The survey length. In order to fully explore the nature of and challenges to law enforcement intelligence work, both surveys asked respondents more than 100 questions.

Feedback suggests individuals were uncomfortable committing to this task, especially when they were at work. As one informant remarked, "Thirty minutes is too long, there's no way I have time to take a survey for half an hour – we're under massive pressure as it is."

3. One response per agency. Several individuals declined because they knew a colleague from the same agency had already responded. One person even indicated his work group had instituted an informal policy whereby they only respond to one survey per week and this task is rotated around the group. While it is possible to control for a limited number of responses when departments are small, it becomes problematic in the case of larger organizations and fusion centers.
4. Security. A handful of individuals were concerned about the security implications of sharing information about intelligence activities outside of the law enforcement community. This was a somewhat surprising finding since the study aims to inform public policy by identifying general, not agency specific, trends about law enforcement intelligence work. However, even though the study was funded by the National Institute of Justice of the U.S. Department of Justice, there was skepticism about the legitimacy of the data collection exercise.

Demographic information

Table 1.2 provides information regarding the position of the respondents and their tenure in the agency. Mean figures suggest 47.1 sworn officers (n=247, SD=346.8), 77.4 professional staff (non-sworn and not analysts) (n=210, SD=966.6), and 13.6 analysts (n=133, SD=30.3) make up the law enforcement sample's intelligence workforce. The large measures of dispersion

indicate there was considerable variation and it was evident that some data points reflected the belief that all agency workers service the intelligence function.

Unsurprisingly, respondents indicate fusion centers employ fewer workers. On average, there are 10.0 sworn officers (n=68, SD=15.7), 18.8 professional staff (non-sworn and not analysts) (n=61, SD=21.7), and 12.0 analysts (n=66, SD=13.3) working in these organizations. However, as Table 1.2 illustrates, most fusion center workers (48.0%) have held their position for between one and three years, in marked contrast to law enforcement workers (21.9%) who tend to have remained in the same role for more than ten years.

Table 1.2: Position and Tenure within their Agency.

	Law enforcement		Fusion centers	
	N	Percent	N	Percent
Role				
Administrator	119	30.3	46	57.5
Supervisor	90	22.9	18	22.5
Investigator	116	29.5	6	7.5
Analyst	68	17.3	10	12.5
Tenure				
Less than a year	3	0.8	10	13.3
1-3 years	27	6.9	36	48.0
4-9 years	78	19.9	24	32.0
10-15 years	86	21.9	3	4.0
More than 15 years	199	50.6	2	2.7

Table 1.2 also displays categorical counts for the job roles and intelligence career tenure of study participants. Most law enforcement (30.3%) and fusion center workers (57.5%) serve as administrators. The next largest groups for the SLT sample include law enforcement investigators (29.5%) and supervisors (22.9%). Analysts represented 17.3 percent of the SLT sample. Over 22 percent of the FC respondents were supervisors, 12.5 percent were analysts, and 7.5 were investigators.

Case Studies

The research team completed three in-depth case studies of fusion centers. The data collection strategy for the case studies was to select two that were using innovative strategies to address these critical issues. These agencies were identified through the surveys, contacts with key staff, and in consultation with the grant program manager and subject matter experts. In addition, the third case study was chosen in order to interview personnel who were working in a fusion center in transition. The research team concluded that since fusion centers are at various points of development that it was critical to receive input from an emerging fusion center that was managing challenging issues (e.g., change in management and other personnel; developing new policies and procedures; staff learning new job responsibilities, developing new information sharing partnerships).

For each fusion center that was selected, the research team began by compiling and analyzing open source documents regarding their efforts to address these issues. In addition, site visits were conducted to better understand their relationship and work in the intelligence area. The research team provides an overview of the structure, activities, and development of each fusion center, and discusses best practices for responding to critical issues examined in the survey. The primary focus of each case study was to better understand the issues addressed in the survey: intelligence practices, information sharing, performance measurement, and communication networks. Other issues examined include experience with terrorism incidents and the production of intelligence regarding the terrorist threat, organizational structures that are part of the law enforcement intelligence community, collection requirements and reasons for relying on particular types of raw information, coordination, and information sharing practices

within an agency, key assessment and evaluation activities, the important legal, cultural, and political issues that impact these processes, the role of intelligence in overall law enforcement operations, and perspectives of cooperation internally and externally.

Structure of the Final Report

The research team presents the results of this study in eight chapters. Chapters 2 through 4 present the survey results. In Chapter 2, information is presented about the organizational policies and staff knowledge of intelligence issues, Chapter 3 engages issues on information sharing, and Chapter 4 discusses performance metrics and communication networks. Chapter 5 provides additional survey results from the fusion center personnel, and discusses the results of the Michigan Intelligence Operations Center case study. Chapter 6 provides a detailed description of the Florida Fusion Center and Chapter 7 discusses the Southern Nevada Counter-Terrorism Center. The final chapter provides a summary of the results and discusses implications for policy, practice, and future research.

Chapter 2: Organizational Policies and Worker Knowledge of Key Intelligence Issues

The September 11th attacks fundamentally changed the structure, expectations, and requirements of law enforcement intelligence operations. Although there have been significant changes and challenges facing the federal law enforcement community, this project focuses on what has occurred at state, local, and tribal levels. The most significant changes have been the development of new national standards and initiatives promulgated by the Global Intelligence Working Group as well as the widespread development of fusion centers. There were only a few fusion centers – typically called Regional Intelligence Centers -- that existed prior to 9/11. This expansion and its impact on local law enforcement is noted in a report recently released by DHS documenting progress made towards implementing recommendations from the 9/11 Commission. Specifically, it was stated that "While fusion centers did not exist ten years ago, today there are 72 recognized fusion centers throughout the country…that are uniquely situated to empower front-line law enforcement, public safety, fire service, emergency response, public health, critical infrastructure protection, and private sector security personnel to understand local implications of national intelligence, thus enabling local officials to better protect their communities" (U.S. Department of Homeland Security, 2011:12). One of the underlying reasons for the creation of these fusion centers was to establish an information sharing clearinghouse for state, local, and tribal law enforcement agencies as part of the Information Sharing Environment. Such centers were designed to help tear down "silos of information" by building trust and communication channels among and between law enforcement agencies, and developing nationwide criminal information connectivity. Technology provides opportunities to collect and share mass amounts of information, but managing and making sense of the data that is available

is a great challenge. The development of fusion centers were designed to help manage a growing amount of two-way SLT information sharing more effectively and efficiently.

Critical to responding to terrorism and other multi-jurisdictional crimes is local information collected from state, local, and tribal law enforcement agencies. There are documented cases of criminal extremists having routine contact with SLT law enforcement officers that led to prevention of an attack, but there have also been some missed opportunities, most notably 9/11. For example, evidence has shown that terrorists commit precursor crimes that put them in contact with various law enforcement officers. One concern, however, is that potentially relevant and important information is not shared and thus an opportunity to prevent a potential serious act may be missed. The new intelligence structure was designed to fix some of these gaps in information sharing. State, local, and tribal agencies have been urged to develop an intelligence capacity so that they may effectively share threat information across jurisdictions as well as provide information to analysts who may more effectively define the threat picture. A significant challenge, however, is that SLT agencies must absorb the costs of building an intelligence capacity as "an unfunded mandate." The lack of dedicated resources makes the building of an effective intelligence capacity particularly challenging.

This chapter provides an introduction that relates to this changing intelligence structure on six survey issues. First, staff attitudes toward preparedness for terrorist and other types of criminal events are examined. Second, staff knowledge of key intelligence mandates are assessed. Third, the knowledge and understanding of the intelligence-led policing concept is discussed. Fourth, attitudes about civil liberties are examined. Fifth, training programs the respondents have taken, as well as intelligence training priorities, are discussed. Sixth, formal policies and practices are examined that support the building of an intelligence capacity. Where

applicable, the results compare the fusion center respondents to all other law enforcement respondents, as well as by the administrator, supervisor, investigator and analyst results.

Attitudes Toward Agency Preparedness

Table 2.1 provides information about agency preparedness. The first two items focused on understanding the threats existing in their region as well as their preparation in responding to these threats. The results are insightful. A majority (63.4%) of the SLT respondents thought to be either very aware or aware of the threats facing their region with little variation when comparing the responses by position within the agency (e.g., administrator, supervisor, investigator, and analyst). However, over 94 percent of the fusion center (FC) respondents said that they were very aware or aware of such threats facing their region. Similarly, nearly 43 percent of the SLT respondents stated that their agency was very prepared or prepared for the threats in their region (an almost equal number stated that they were somewhat prepared), but over 67 percent of the FC respondents said they were very prepared or prepared for homeland security threats. In addition, when comparing the SLT responses by position in the organization, the responding analysts were much more likely to say that the organization was very prepared or prepared. Over 66 percent of the analysts said that the organization was prepared or very prepared compared to 46 percent of administrators, 33 percent of supervisors, and 36 percent of investigators. Thus, although the FC respondents and analysts thought that they were prepared for the threats in their region; other SLT personnel did not feel as strongly about their preparation.

Table 2.1 Attitudes Towards Agency Preparedness

Question	SLT	Fusion Center	Administration	Supervisor	Investigator	Analyst
Agency						

aware of threats[1]	63.4%	94.1%	68.9%	63.2%	57.3%	70.5%
Agency prepared for threats[2]	42.7%	67.4%	46.2%	32.6%	35.7%	66.1%
Far along is agency in having an intelligence capacity[3]	9.2%	14.1%	8.4%	6.7%	7.0%	16.2%
Agency has sufficient staff[4]	2.9%	1.2%	1.7%	1.1%	4.3%	3.0%
Agency has capacity to identify threats[4]	13.3%	19.2%	14.5%	16.9%	7.3%	18.6%
Agency provides timely intell[4]	16.7%	17.9%	16.2%	19.0%	12.7%	24.1%
Fusion center products have content to aid in prevention of crime[4]	16.8%	NA	17.8%	20.0%	12.9%	18.0%

[1] Very aware/aware; [2] Very prepared/prepared; [3] Very far; [4] Strongly Agree

The results in Table 2.1 also show that there is widespread agreement that the law enforcement community has a long way to go in building an intelligence capacity—a conclusion indicated by the respondents taking both surveys. Less than ten percent of the SLT respondents thought that their agency was far along in developing and maintaining a criminal intelligence capacity, 13 percent strongly agreed that they had the capacity to identify the characteristics of events that represent the indicators or precursors of threats, and only 17 percent thought their agency provides actionable intelligence in a timely manner. Only 14 percent of the FC

respondents thought that they were very far along in developing and maintaining an intelligence capacity, 19 percent strongly agreed that they had the characteristics of events that represent indicators and/or precursors, and nearly 18 percent strongly agreed that the center provides intelligence in a timely manner. It is not surprising, but very few SLT respondents and FC respondents thought they had a sufficient number of staff to achieve their agency's intelligence capacity mission.

Knowledge of Key Intelligence Mandates

Table 2.2 presents knowledge of key intelligence mandates. The results from this table also support the conclusion that building an intelligence capacity for both FCs and SLT agencies is a work in progress and very few respondents think their agency has reached optimum levels. The state, local, and tribal respondents were very familiar or somewhat familiar with the National Criminal Intelligence Sharing Plan and the intelligence-led policing concept, but they were much less familiar with the Department of Homeland Security's Target Capability List. There was not much variation in the responses to this general awareness of these mandates when comparing the different levels of the organization. Fusion center respondents were more likely to be very or somewhat familiar with the National Criminal Intelligence Sharing Plan, the Target Capability List, and the intelligence-led policing concept compared to the SLT respondents.

Table 2.2. Respondent Knowledge of Key Intelligence Mandates

Question	SLT	Fusion Center	Administrator	Supervisor	Investigator	Analyst
Familiar with NCISP[1]	63.7%	88.6%	65.5%	57.8%	68.1%	60.3%
Familiar with TCL[1]	37.8%	72.7%	40.3%	44.8%	31.0%	34.4%

Familiar with ILP[1]	70.3%	86.2%	70.6%	65.9%	68.1%	79.1%
Agency follows NCISP recs[2]	9.4%	19.0%	3.6%	11.8%	10.0%	15.3%
Agency aligns with TCL[2]	6.0%	7.6%	3.8%	5.1%	6.8%	4.2%

[1]Very familiar/familiar; [2]Completely

It is interesting that the respondents agreed that, although they were generally familiar with the National Criminal Sharing Plan, the Target Capability list, and Intelligence-Led Policing, they have yet to put these mandates into practice. Only nine percent of the SLT respondents said that their agency's intelligence function follows the National Criminal Sharing Plan and just six percent said it aligns with the Target Capability list. Nineteen percent of the FC respondents said that their agency's intelligence function followed the NCISP recommendations and over seven percent said that it aligns with the Target Capability list.

Intelligence-Led Policing

The adoption of intelligence-led policing (ILP) is gaining momentum among state, local, and tribal law enforcement agencies. The International Association of Chiefs of Police (IACP) intelligence summit in 2002 recommended the adoption of ILP by America's state, local and tribal law enforcement agencies in the post-9/11 era (IACP, 2002). This was reinforced by a recommendation in the National Criminal Intelligence Sharing Plan (NCISP) to adopt ILP and has been echoed broadly by law enforcement leaders as well as reflected in new programming by the U.S. Department of Justice (DOJ) and the U. S. Department of Homeland Security (DHS) (Carter, 2009). The demand for intelligence-led policing has come from a variety of government

recommendations, reports, and mandates. Moreover, government funding has provided incentives for agencies to adopt intelligence-led policing to explore its different applications– such as the Bureau of Justice Assistance's "Targeting Violent Crime Initiative" (TVCI).

Very few of the agencies surveyed, however, have implemented intelligence-led policing. Table 2.3 presents these results. On average, only 18.7 percent of the SLT respondents said that their agency had adopted intelligence-led policing. Analysts were somewhat more likely than administrators, supervisors, and investigators to believe their organization had adopted ILP. In contrast, over 29 percent of the FC respondents indicated that their agency had adopted ILP. Not only did a larger percentage of FC respondents indicate that their agency had adopted ILP, they were also somewhat more likely to indicate that it was very effective. Over 38 percent of the FC respondents indicated that ILP was very effective in their agency. Although investigators and analysts were somewhat more optimistic about the effectiveness of ILP in their agency, under 30 percent of all SLT respondents thought that ILP functioned very effectively in their agency.

Table 2.3. Understanding Intelligence-Led Policing

Question	SLT	Fusion Center	Administrator	Supervisor	Investigator	Analyst
Agency Adopted ILP	18.7%	29.1%	16.8%	14.8%	20.0%	26.5%
ILP effective in agency[1]	28.0%	37.5%	20.0%	25.0%	36.4%	33.3%
Agency chief exec supports ILP[2]	23.3%	51.2%	28.0%	21.2%	17.3%	31.7%
Analysts in agency familiar with ILP[2]	13.8%	28.4%	10.5%	13.3%	14.4%	20.0%

Personnel in agency familiar with ILP[2]	3.2%	18.5%	2.5%	2.3%	3.5%	6.2%

[1] Very Effective; [2] Strongly Agree

A recent study of Intelligence-Led Policing implementation found that both familiarity with, and commitment to, the ILP concept increased the likelihood of successful implementation (Carter, 2011). The respondents from both surveys indicated that most analysts and other personnel in their organization were not familiar with the ILP concept. Only 14 percent of the SLT respondents strongly agreed that analysts were very familiar with the ILP concept and just over three percent said that other personnel in the organization were very familiar with this concept. Although the percentages were somewhat higher when examining the FC responses, just over 28 percent strongly agreed that the analysts in the fusion center were familiar and over 18 percent strongly agreed that others in the agency were familiar with the ILP concept.

Critical to the promotion of this concept is the attitudes of the chief executive about the adoption of ILP—without commitment from command staff it is unlikely that ILP will have much of an impact on organizational processes. It appears that the FC respondents thought that the chief executives were much more supportive of the ILP concept. Over 51 percent of these respondents strongly agreed that their chief executive supports ILP. In contrast, just over 23 percent of the SLT respondents strongly agreed that the chief executive supports ILP.

Civil Liberties

Table 2.4 provides data on perceptions of civil liberties. Most of the SLT respondents and FC respondents indicated that suspicious activity reports include personal identifying information of suspicious persons. Nearly 78 percent of the SLT respondents and 75 percent of

the FC respondents said that suspicious activity reports include such information. Only 17 percent of the SLT respondents and 27 percent of the FC respondents said that these reports are entered into an information system outside of their agency, but the SLT analysts were much less likely to indicate that such reports were entered into other information systems.[5]

The remaining results presented in Table 2.4 represent more general issues related to privacy and protection of civil liberties. As a precursor discussion, 28 CFR Part 23, is a federal regulation prescribing guidelines for the collection, retention, review, dissemination and purging of "criminal intelligence information". The regulation stipulates it only applies to law enforcement agencies that operate a federally funded multijurisdictional criminal intelligence records system. However, as a new national standard, the National Criminal Intelligence Sharing Plan (NCISP) provides broader application, recommending that all law enforcement agencies that have criminal intelligence records adhere to 28 CFR Part 23, whether or not they receive federal funding. As a result, the research team included these questions as a benchmark to measure adoption of the NCISP recommendations. Just over half of the SLT respondents indicated that their criminal intelligence records system was 28 CFR Part 23 compliant, but over 82 percent of the FC respondents indicated such compliance. The surprising aspect of this finding is that since one responsibility of fusion centers is to serve as repositories for "criminal intelligence information" and virtually all of them receive some type of federal funding (although that funding may not specifically be to support the "criminal intelligence records system") one would assume that all fusion centers were 28 CFR Part 23 compliant.[6] As a caveat,

[5] It should be noted that at the time of these surveys, the Nationwide Suspicious Activity Reporting Initiative (NSI) had been developed but was still in the Evaluation Environment (EE) phase. While there had been widespread discussion of the initiative, its implementation was still in progress. The question was addressed in this survey because there had been some vocal concern about the NSI expressed by the American Civil Liberties Union (ACLU).

[6] Beyond the NCISP recommendation, the Fusion Center Guidelines also explicitly recommend that fusion centers also adhere to the regulation.

some of the fusion centers were still in development at the time of the survey – if surveyed again today this percentage would most likely be higher.

Further on the question of 28 CFR Part 23 compliance, it is very interesting to compare the SLT analysts' responses to the administrator, supervisor, and investigator results. Specifically, the analysts were much more likely to indicate that the agency's criminal intelligence records system were compliant with 28 CFR Part 23 compared to others in the organization. For example, over 72 percent of the analysts said they were compliant compared to 48 percent of the administrators, 42 percent of the supervisors, and 55 percent of the investigators. An explanation for this is that the analysts' training typically focuses more on the 28 CFR Part 23 guidelines and the analysts tend to work with the criminal intelligence records on a more consistent basis than other than other staff members. As a result, the analysts' responses may simply reflect a more informed response to the question.

Less than half of the SLT and FC respondents said that their privacy policy meet federal policy standards, although most of the remaining respondents indicated that their policy was in the process of being modified. In the last two years there has been a concerted effort, including federal technical assistance, to ensure that the fusion centers have a privacy policy in place that meet the privacy standards of the Information Sharing Environment. Once again, if the survey was taken today, the percentage of fusion centers with a privacy policy meeting these standards would likely be higher.

Similarly, less than half of the SLT respondents and 63 percent of the FC respondents indicated that their agency distinguishes between permanent and temporary intelligence files within their intelligence records policy. It should be noted that the distinction between temporary and permanent intelligence records are not part of the 28 CFR Part 23 guidelines, but

simply a policy mechanism employed by many law enforcement agencies to deal with "tips and leads" that have not yet met the criminal predicate standard. Those agencies and fusion centers not reporting the use of both types of files may have simply opted to not retain any criminal intelligence records unless the criminal predicate has been established.

Table 2.4. Attitudes on Civil Liberties

Question	SLT	Fusion Center	Administrator	Supervisor	Investigator	Analyst
SARs have identifying information	77.9%	75.0%	78.8%	76.2%	88.2%	73.0%
SARs entered into outside info system	16.7%	27.1%	18.8%	16.3%	21.2%	7.9%
Agency distinguishes perm. and temp. intel files	47.4%	62.7%	46.2%	39.5%	50.4%	58.8%
Privacy policy meets federal standards	47.4%	45.9%	50.4%	43.2%	45.2%	54.4%
Crim. intel records system are 28 CFR Part 23compliant	52.7%	82.4%	47.9%	42.0%	55.3%	72.1%

Training

A critical mechanism for building an effective intelligence capacity is providing training to staff in all levels of the organization on policies, procedures, civil rights, and organizational change issues. Indeed, the *Minimum Criminal Intelligence Training Standards* produced by the GIWG emphasize the need and minimum training content for Chief Executives, commanders and supervisors, analysts and line officers. Some funding agencies have supported the creation

of training programs related to building an intelligence capacity and some other programs are available from specific law enforcement agencies. For example, all of the SLT members have attended MSU's Intelligence Toolbox Training in order to be in the sample, and beyond this, approximately 30 percent of the fusion center sample attended this training. Table 2.5 presents whether SLT respondents, SLT analysts, and fusion center personnel have attended other types of training programs. Of the training programs considered, training provided by State and Local Anti-Terrorism Training (SLATT) was most likely to be attended by the analysts in these agencies. Fifty-three percent of all SLT respondents, 58 percent of SLT analysts, and 73 percent of FC personnel indicated that their analysts had attended SLATT training. A relatively high number of respondents indicated that their analysts attended the Fundamentals of Intelligence Analyst Training (FIAT) and 28 CFR Part 23 training. Approximately 35 percent of SLT respondents and analysts indicated that their analysts attended FIAT training, and 35 percent of all SLT respondents and 47 percent of SLT analysts indicated that their analysts attended 28 CFR 23 training[7]. Nearly 77 percent of FC respondents indicated that their analysts attended FIAT training and 76 percent indicated they attended 28 CFR 23 training. Over 20 percent of the SLT respondents indicated that their analysts attended the Federal Law Enforcement Training Center analyst training and the National White Collar Crime Centers Analyst training. A somewhat higher percentage of SLT analysts and FC respondents indicated that their analysts attended these two trainings. In general, a smaller percentage of respondents indicated that their analysts attended the other trainings considered, including the FBI's Center for Intelligence Training[8], the DEA's Federal Law Enforcement Analyst Training (FLEAT), Regional

[7] The Bureau of Justice Assistance provides 28 CFR Part 23 training both as an "in class" model and an online where there is testing a certificate issued. The survey did not distinguish between the training delivery methods.
[8] This has recently been renamed the Intelligence and Analysis Training Unit (IATU).

CounterDrug Training Academy (RCTA), and the Department of Homeland Security's DHS Report Writing workshop.

Table 2.5. National Training Participation

Training	SLT	Fusion Center	Analyst
FIAT Analyst Training	33.9%	77.2%	35.9%
FLETC Analyst Training	22.6%	44.3%	34.4%
FBI Center for Intel Training	8.6%	15.2%	9.4%
FLEAT Analyst Training	12.5%	26.6%	21.9%
NWCCC Analyst Training	21.1%	40.5%	25.0%
SLATT Analyst Training	53.0%	73.4%	57.8%
28 CFR 23	35.1%	75.9%	46.9%
Regional CounterDrug Intel Training	14.3%	22.8%	10.9%
DHS Report Writing	13.1%	NA	23.4%

Beyond the training programs attended, the research team wanted to document training priorities by asking what type of training, in general, analysts were required to complete and whether the agency provided any specific training on intelligence issues. Table 2.6 provides the responses for SLT and FC respondents. Fusion centers, in general, had a much higher number of training priorities. For example, over 78 percent of the fusion respondents indicated that analysts were required to receive training on the agency's privacy policy and 68 percent indicated that analysts were required to receive training on precursor activities of terrorists.[9] Over 31 percent of the FC respondents indicated that analysts were required to receive specific training on intelligence-led policing. Forty-one percent of the SLT respondents indicated that analysts were required to receive training on precursor activities of terrorists, 39 percent indicated that they

[9] It should be noted this training is largely related to the Nationwide Suspicious Activity Reporting Initiative.

received training on the agency's privacy policy, and 82 percent said they received specific training on ILP. These results are consistent with earlier findings presented that compared general awareness of ILP issues and concerns about civil rights organizations across the two samples of respondents.

A relatively large number of respondents indicated that their agency was attempting to train others in different ways to assist with the collection of suspicious activities and intelligence requirements. Over 87 percent of the FC respondents and 82 percent of the SLT respondents indicated that line level officers were trained to identify and report information related to suspicious activities. Eighty-three percent of the FC respondents indicated that they trained other partners (e.g., businesses, community organizations) and 43 percent indicated they trained citizens to identify suspicious activities in their community. In comparison, 40 percent of the SLT respondents indicated they trained other partners and 28 percent indicated they trained citizens to identify suspicious activities. Almost half of the SLT respondents indicated that they provided academy training on the role and function of intelligence in their agency and 77 percent of the FC respondents indicated they provided such training. Approximately one-third of both samples of respondents indicated that they train other law enforcement officers on privacy and civil rights issues. Prior to the law enforcement intelligence initiatives that were products of the 9/11 attacks and the subsequent creation of the Global Intelligence Working Group, there was virtually no intelligence related training for law enforcement personnel who were not assigned to a dedicated intelligence unit, gang unit or drug unit. As a result, the percentages of agencies reporting intelligence-training to non-intelligence staff represent significant progress.

Table 2.6. Agency Training Priorities

Training	SLT	Fusion Center

Specific training on ILP	19.0%	31.7%
Agency's privacy policy	38.8%	78.3%
Precursor activities of terrorists	41.1%	68.7%
Suspicious activities	81.6%	87.1%
Trained non-traditional partners	40.1%	82.9%
Trained citizens	27.9%	42.9%
Provided academy training	49.3%	77.1%
Provided training on civil rights issues	35.7%	38.6%

Formal Policies and Procedures

Table 2.7 documents the formal policies and procedures that are in place related to building an intelligence capacity. Most of these policies and procedures represent the building blocks critical to achieving a mature intelligence capacity, and in general, about half of the respondents indicated that their agency had put most of these policies and procedures in place. Nearly 46 percent of the SLT respondents and 59 percent of the FC respondents indicated that the agency had a policy designed expressly to guide their intelligence function, and 34 percent of the SLT respondents and 62 percent of the FC respondents indicated that their agency has an intelligence capacity mission statement. Over 60 percent of the SLT respondents and 79 percent of the FC respondents indicated that their agency had a formal approval process for entering into a Memorandum of Understanding for information and intelligence sharing with other law enforcement agencies/entities, although only 44 percent of the SLT respondents said their agency had defined goals and objectives for collecting, analyzing, producing and sharing information compared to over 81 percent of the FC respondents. While these data reflect significant growth of intelligence-related policies and procedures, a caveat is that the survey was sent to a purposive

sample of individuals working in an intelligence-related assignment-- in the universe of American law enforcement agencies, the proportions would be smaller.

Several of the survey items relate to the management of potential intelligence sources. Nearly 39 percent of the SLT respondents indicated that their agency has a suspicious activity reporting policy, and 74 percent said their suspicious activities reports are for all crimes. In comparison, 49 percent of the FC respondents said their agency had a suspicious activity reporting policy, and 73 percent indicated that they had these reports for all crimes. Over half of the SLT respondents and over 60 percent of the FC respondents said that their agency had either or both a Terrorism Liaison Officer and Intelligence Liaison Program. New initiatives and guidelines were developed for Fusion Center Liaison Officers after the survey data were collected. Once again, a survey administered today would likely see this number increase significantly. Nearly 68 percent of the SLT respondents indicated that the agency has a formal policy for managing informants and 47 percent indicated that the agency deconflicts information in their intelligence records system. A somewhat smaller percentage of FC respondents said that they had an articulated policy and procedures for managing informants, but a higher percentage stated that their agency deconflicts information in their intelligence records system.

Several of the questions build on the earlier discussion of responding to privacy and civil rights concerns. For example, 32 percent of the SLT respondents indicated that their agency regularly audits their intelligence function and records, nearly 52 percent indicated their agency has a policy to handle both sensitive but unclassified information and classified information, 41 percent indicated that legal counsel has reviewed and approved all procedures related to building an intelligence capacity, and 62 percent indicated that the information stored in criminal intelligence files is evaluated according to source reliability and content validity before being

included in a criminal intelligence files. Thirty percent of these respondents, however, indicated that their privacy policy has never been updated to be aligned with new or revised laws or court decisions. The FC respondents were somewhat more likely to indicate that such policies were in place. For example, 46 percent said they audit their intelligence function and records, 67 percent said they have a policy to handle sensitive but unclassified and classified information, 67 percent indicated that legal counsel had reviewed and approved all policies and procedures, and nearly 80 percent indicated that the information stored in criminal intelligence files was evaluated according to source reliability and content validity. One would expect the fusion centers to report higher percentages on these variables because there has been a more directed training and technical assistance effort directed toward fusion centers by the Department of Homeland Security (DHS) because of the DHS obligations to establish functional two-way information between DHS (in particular) and state, local and tribal law enforcement agencies.

Table 2.7. Summary of Policies and Formal Practices

Question	SLT	Fusion Center
Policy to guide intel function	45.9%	59.3%
Regularly audits intel function and records	32.1%	46.5%
TLO/ILO program	51.2%	67.7%
Policy for sensitive info	51.7%	67.4%
SAR policy	38.7%	49.4%
SARs for all crimes	74.0%	72.9%
Intel capacity mission statement	34.0%	61.6%
Policies & procedures for managing informants	67.5%	60.0%
Formal approval process for MOU for info & intel with other law enforcement entities	61.2%	78.8%
Legal counsel has approved all policies & procedures of intel	41.3%	66.7%

capacity		
Agency NEVER updates privacy policy	29.2%	8.9%
Agency has goals for collecting, analyzing, producing, & sharing info	44.3%	81.0%
Agency established process to identify/track reports of suspicious activity	56.1%	78.2%
Agency deconflicts info in intel records system	47.0%	67.9%
Crim. intel files is evaluated for reliability & validity before put in intel file	62.0%	79.5%
Agency developed collection requirements based on risk assessment results	34.6%	55.7%

Chapter 3. Information Sharing

One of the key elements to the successful use of intelligence for prevention is widespread information sharing. According to the Information Sharing Environment Implementation Plan, "Strengthening our nation's ability to share terrorism information constitutes a cornerstone of our national strategy to protect the American people and our institutions and to defeat terrorists and their support networks at home and abroad" (McNamara, 2006: xiii). Similarly, the President's National Strategy for Information Sharing (2007, p. 1) states, "Our success in preventing future terrorist attacks depends upon our ability to gather, analyze, and share information on intelligence regarding those who want to attack us, the tactics they use, and the targets that they intend to attack." Agencies and individuals must know how to identify relevant threat information, collect it without violating civil liberties, know who the information should be shared with, and must be willing to share it. Although there are many agencies that will provide information that will have to be shared to be successful in preventing terrorist attacks, SLT law enforcement agencies play a particularly important role for identifying and intervening in domestic threats. Moreover, although state and major urban area fusion centers have provided a vehicle to perhaps enhance the flow of local intelligence, these centers are still in development with little empirically known about their information sharing relationships with other agencies. Considering that information sharing among law enforcement agencies has historically been a problematic issue, there is reason to suspect that it will be necessary to develop innovative strategies to promote information sharing across SLT law enforcement agencies and with the Department of Homeland Security, the Federal Bureau of Investigation, and state fusion centers. While both the Global Intelligence Working Group and the Program Manager for the Information Sharing Environment are providing important standards and guidelines for sharing

intelligence and information among fusion centers, SLT agencies and federal law enforcement, a scientific assessment of information sharing practices has not occurred. The research team reminds the reader that the data collected in this study represents information sharing practices at the time the survey was completed by respondents – new initiatives and practices have occurred in the time interval between data collection and this report of the findings. Nonetheless, this data provide an important empirical benchmark that was not previously available.

Although the 9/11 attacks did not initiate the call for better information sharing among government agencies, the attacks did enhance the urgency to take action. There are many examples that can be taken from congressional hearings, reports, and legislative initiatives that demonstrate the widespread conclusion that the sharing of information must be improved. For example, the USA PATRIOT ACT specifically cites the need to improve information sharing and that the "wall" between the intelligence and law enforcement communities must be torn down. The 9/11 Commission report highlights multiple information sharing failures and missed opportunities to prevent the attacks, and importantly concludes: "The culture of agencies feeling they own the information they gathered at taxpayer expense must be replaced by a culture in which the agencies instead feel they have a duty to the information—to repay the taxpayers' investment by making that information available" (National Commission on Terrorist Attacks Upon the United States, 2004: 417). Other examples of government commission reports that highlight the problems with information flow and the need to improve information sharing include the Senate Select Committee on Intelligence, *The National Strategy for Homeland Security* and *The National Security for the Physical Protection of Critical Infrastructures and Key Assets*, the General Accounting Office's 2003 and 2007 reports on strengthening information sharing, and the report from The Weapons of Mass Destruction Commission 2005

report. Perhaps, however, one of the most significant factors was the Intelligence Reform and Terrorism Prevention Act of 2004 which created the Information Sharing Environment.

This chapter focuses on how state, local, tribal and fusion center personnel think about law enforcement intelligence sharing practices. The research team examines who the respondents consult on intelligence issues and their satisfaction with their relationship with various federal, state, and local agencies. Similarly, the study examines how these individuals rate their closeness to other law enforcement agencies, but also how well they are intersected with other community, political, and government agencies. In addition, information sharing inputs and outputs, and the methods used to share information are examined.

The Nature of Relationships with Other Agencies

Table 3.1 provides the results from asking about the likelihood that respondents would contact various agencies for intelligence and threat-related information. The results are provided for all SLT respondents, FC respondents, and SLT administrators, supervisors, investigators, and analysts. Both SLT and FC respondents were likely to rely heavily on others within their own agency when having questions about intelligence issues. Over 66 percent of the SLT respondents and over 75 percent of the FC respondents indicated that they were very likely to consult other staff in their own agency. Close to or more than half of both SLT and FC respondents were very likely to consult the FBI, state or local law enforcement agencies, and experts in the field. Both SLT and FC respondents were less likely to consult government officials and government attorneys. Table 3.1 is interesting for two additional reasons. First, in general, similar percentages of SLT and FC respondents were very likely to consult the same sources when they have intelligence-related questions, although FC respondents indicated that

they were very likely to use a few sources more frequently. For example, a higher percentage of FC respondents indicated that they were very likely to consult the FBI, state law enforcement agencies, experts in the field, and other state fusion centers. Only about 30 percent of the SLT respondents were very likely to consult other fusion centers on intelligence issues compared to over 61 percent of the FC respondents. This makes sense but it also provides evidence related to the structure of intelligence sharing, and that fusion centers appear to have open lines of communication and thus would be expected to, in turn, push any intelligence received from other fusion centers throughout their states. Indeed, this empirically supports the rationale on which the development of fusion centers was based. Second, SLT administrators, supervisors, investigators, and analysts appeared to use these sources similarly with just one exception. State, local, tribal analysts were somewhat less likely to say that they would consult the FBI on intelligence issues compared to supervisors and investigators and much less likely compared to administrators. Since analysts tend to be non-sworn, it is likely that this finding reflects organizational culture as much as information sharing practices.

Table 3.1. Consults Other Agencies on Intelligence Issues

Agency	SLT	FC	Administration	Supervisor	Investigator	Analyst
FBI	47.9%	57.7%	60.7%	48.8%	40.4%	35.6%
State FC	45.1%	NA	50.4%	41.0%	39.3%	50.8%
Other State FC	28.7%	61.5%	28.9%	32.1%	22.5%	32.8%
Other Fed LEA	42.5%	46.8%	47.0%	40.5%	42.7%	34.5%
State LEA	53.9%	60.8%	56.9%	54.1%	52.8%	50.0%
Other Local LEA	59.6%	56.6%	64.7%	60.2%	57.7%	52.5%
Other Staff in Agency	66.2%	75.6%	71.2%	67.9%	60.4%	65.5%

Govt Officials	33.1%	31.2%	37.4%	31.7%	28.7%	34.5%
Govt Attorneys	22.9%	32.5%	26.1%	21.3%	22.0%	18.5%
Experts in Field	45.9%	63.2%	49.1%	39.2%	48.5%	45.5%

Table 3.2 explores these relationships in a somewhat different way as respondents were asked to reflect on the closeness of the relationship with various agencies. In addition, the research team asked respondents to not only reflect on the closeness of their relationship with other federal, state, and local law enforcement agencies, but also with a number of government and community agencies, the national guard, and the private sector. The results are similar to the discussion presented above. Both SLT and FC respondents similarly rated the closeness of their relationship with other law enforcement relationships, although more FC respondents rated the relationship with state law enforcement as being very close. Approximately 39 percent of SLT and FC respondents rated their relationship with the FBI and other federal law enforcement agencies as very close, 64 percent rated their relationship with local law enforcement agencies, and 10 percent rated their relationship with tribal agencies as being very close. Fifty-three percent of the SLT respondents thought their relationship with state law enforcement agencies, but 68 percent of FC respondents rated their relationship as very close. This difference makes sense as state fusion centers and state police think similarly about the geographic boundaries of their work, and in many states (like Michigan discussed below), the state police are either the lead or one of the lead agencies responsible for fusion center operations. When comparing the SLT responses by position in the agency, analysts were less likely to define their relationship with the FBI, local law enforcement, and hospitals, but more likely to define their relationship

with the state fusion centers, Department of Corrections, and the National Guard as being very close.

Table 3.2. Working Relationship with Other Agencies

Agency	SLT	FC	Administration	Supervisor	Investigator	Analyst
FBI[1]	39.1%	39.0%	46.6%	34.5%	39.1%	33.3%
Other Fed	37.3%	40.7%	39.7%	29.1%	42.2%	38.7%
State LE	53.0%	67.9%	60.5%	46.0%	51.8%	54.0%
Local LE	64.4%	63.8%	71.7%	63.5%	60.2%	61.3%
Tribal LE	10.7%	10.5%	6.3%	8.0%	8.5%	28.6%
State FC	37.1%	NA	36.0%	31.8%	36.9%	50.8%
Other FC	18.9%	48.8%	20.9%	13.8%	17.2%	25.9%
State Govt Officials	19.6%	31.7%	23.3%	9.9%	23.2%	21.1%
Infrastructure Security Rep	21.6%	39.5%	23.6%	23.1%	15.5%	29.1%
Dept of Corrections	31.1%	41.3%	25.0%	30.1%	35.6%	40.0%
Emergency Mgmt	36.0%	48.8%	41.9%	31.0%	32.0%	41.4%
Fire Marshal	30.9%	39.5%	30.4%	30.5%	29.6%	36.2%
Homeland Security	29.2%	54.9%	34.5%	23.2%	25.0%	37.3%
IRS	11.2%	13.8%	9.6%	7.5%	15.3%	14.0%
Hospitals	22.2%	13.6%	25.2%	23.2%	22.2%	16.4%
Private Sector	15.8%	16.3%	19.8%	9.9%	16.0%	18.2%
Public Health	22.4%	35.8%	26.8%	18.3%	22.3%	23.6%
Public Works	28.7%	20.0%	29.2%	32.1%	26.3%	25.9%
Transportation	22.7%	29.6%	25.4%	20.5%	20.2%	25.5%
National Guard	25.2%	58.4%	23.9%	20.5%	24.0%	38.9%

[1]Very Close

The results presented in Table 3.2 also indicate that fusion centers have closer relationships with a wider variety of institutions and agencies. Again, this would be expected as most fusion centers have adopted an "all crimes all hazards" approach, which fundamentally requires the building of diverse relationships. Fusion center respondents were more likely to say that their relationship with other fusion centers, state government officials, critical infrastructure representatives, Department of Corrections, emergency management, fire marshals, homeland security, public health, transportation, and the National Guard was very close. For example, only 25 percent of the SLT respondents noted that there relationship with the National Guard was very close compared to nearly 60 percent of the FC respondents who define this relationship as being very close. Similarly, 30 percent of the SLT respondents but 55 percent of the FC respondents defined their relationship with homeland security as being very close. Only 22 percent of the SLT respondents but 40 percent of the FC respondents said that their relationship with critical infrastructure representatives was very close. These findings support some successes have been achieved on the conceptual foundation of fusion centers with respect to developing diverse information sharing partners.

Satisfaction with Relationships

Table 3.3 presents the results on respondents' evaluation of their satisfaction with how their agency relates to other agencies. These results are interesting especially when contrasted with the findings from the previous two tables. In general, only a modest number of SLT and FC respondents were very satisfied with their relationship with the agencies noted and there was not much variation when comparing the two groups. For example, approximately 20 percent of

SLT and FC respondents were very satisfied with their relationship with the FBI, other federal law enforcement agencies, and emergency management personnel. A somewhat higher percentage of both SLT and FC respondents were very satisfied with their relationship with state and local law enforcement agencies. Approximately 28 percent of SLT respondents and 35 percent of the FC respondents were very satisfied with their relationship with state law enforcement agencies, and over 38 percent of the SLT and FC respondents indicated that they were very satisfied with their relationship with local law enforcement agencies. Both SLT and FC respondents were not very satisfied with their relationship with tribal law enforcement, public health, and private sector agencies.

Table 3.3. Satisfaction with Relationship

Agency	SLT	FC	Administration	Supervisor	Investigator	Analyst
FBI[1]	20.6%	20.0%	28.8%	18.4%	15.6%	16.9%
Other Fed LEA	16.4%	19.0%	21.8%	9.3%	12.5%	20.0%
State FC	22.4%	NA	24.1%	18.8%	21.9%	25.8%
State LEA	27.9%	35.0%	29.7%	28.9%	22.2%	34.8%
Local LEA	38.0%	38.8%	44.3%	32.6%	35.8%	36.8%
Tribal LEA	4.9%	3.9%	6.1%	1.3%	2.8%	10.9%
Private Sector	7.0%	10.5%	9.4%	8.4%	4.5%	6.3%
Public Health	9.6%	15.2%	18.5%	4.8%	6.4%	6.3%
Emergency						

Mgmt	17.6%	22.8%	29.7%	9.6%	14.8%	11.1%

[1] Very Satisfied

There was some variation in satisfaction with the relationship comparing across position in the SLT agencies. For example, supervisors, investigators, and analysts were less satisfied with their relationship with the FBI compared to the administrators in the sample, and supervisors and investigators were less satisfied with their relationship with other federal law enforcement compared to administrators and analysts. Supervisors, investigators, and analysts were also less likely to be satisfied with their relationship with local law enforcement, public health agencies, and emergency management agencies.

There are a wide variety of factors that are going to affect satisfaction with different agencies – historical experiences, organizational culture and even personalities are among these factors. Thus, closer examination of these variables will provide more insight into the true nature of satisfaction in these relationships.

Information Sharing Practices

In this section, we look more deeply at information sharing practices. Both fusion centers and SLT agencies have significant amounts of information coming into the organization that has to be managed, assessed, processed, and determined if it is indicative of a criminal threat. If there is a requirement or a need for the information to be shared, it will be packaged and distributed within the organization or shared with the appropriate external constituencies. Although much of this information might have little value from an intelligence perspective, some of it might be considered critical – such as suspicious activity -- and thus there is the need to ensure that the right information gets shared with the people and agencies who are likely to need

to know the information. Since organizations have information both coming in and being disseminated, the research team included a series of questions that speak to the inputs and outputs of the organization. These results are presented in Tables 3.4 and 3.5.

Table 3.4 includes the results on some of the types of data, information, and intelligence that are brought into the organization. The results indicated that the agencies surveyed are overwhelmed with information. Although there is some variation in the sources of information, analysts from both SLT and FCs receive significant amounts of information on a daily basis. For example, 35 percent of the SLT respondents said their agency receives suspicious activity reports, 41 percent said they receive crime reports, 62 percent said they receive news reports, 55 percent receive open source information, 37 percent receive 9-1-1 calls data, 34 percent receive human intelligence, and 27 percent receive TIPS line data on a daily basis. Other information that comes into the organization daily includes threat assessments (20.6%), witness/suspect statements (15.7%), and crime maps (15.0%). Similarly, fusion center respondents also indicated that a significant amount of information comes into the organization on a daily basis. Specifically, 45 percent said that suspicious activity reports, 50 percent said crime reports, over 80 percent said that news reports and open source information, 43 percent said TIPS line data, and 32 percent human intelligence comes in on a daily basis. Although not coming into the organization as frequently, fusion centers still receive crime maps, witness/suspect statements, threat assessments and 9-1-1 call data.

Table 3.4. Information Sharing Practices (Input)

Question	SLT	Fusion Center
Frequency of intel analysts receiving information from:[1]		

Suspicious Activity Reports	35.3%	45.8%
Crime Reports	40.5%	50.0%
Crime Maps	15.0%	23.5%
Witness/Suspect Statements	15.7%	14.7%
Threat Assessments	20.6%	16.9%
News Reports	61.9%	84.3%
Open Source Information	55.0%	81.2%
Human Intelligence	33.6%	31.9%
TIPS Line	27.2%	42.6%
9-1-1 Calls	36.9%	20.6%
Frequency of receiving actionable intelligence from:		
DHS	42.7%	56.0%
FBI	40.4%	46.6%
DEA	33.2%	33.8%
DOD	20.1%	23.0%
State Fusion Centers	50.1%	NA
Other Fusion Centers	31.1%	72.3%
Coast Guard	18.2%	30.1%
ICE	32.1%	35.6%
Border Patrol	22.3%	25.0%
NDIC	15.0%	26.4%
US Attorneys	24.6%	35.6%
State Police	50.8%	75.0%
DOC	37.2%	56.1%
State Health Department	20.0%	36.9%
State Attorney General	22.9%	26.8%
National Guard	17.7%	41.9%

Local/Tribal Police	39.7%	54.7%
Sheriff	55.6%	73.0%
Fire Services	34.5%	27.0%
Private Businesses	24.0%	30.1%
Critical Infrastructure Security Representatives	20.2%	39.7%

[1]Daily [2]Very Frequently/Frequently

Other data presented in Table 3.4 relates directly to the amount of actionable intelligence that is being received by the agencies in the study. Similar to the conclusion from above, the agencies in this study are clearly being provided a significant amount of intelligence that needs to be processed by the organization for some type of operational response or awareness. A large number of organizations appear to be sharing information very frequently or frequently with these agencies, and as would be expected, the fusion center respondents indicated that the amount of actionable intelligence was even greater. In fact, a higher percentage of FC respondents stated that their agency very frequently or frequently received actionable intelligence from every agency listed except fire services. More than half of the FC respondents noted that their agency receives actionable intelligence very frequently or frequently from state police, sheriffs, other fusion centers, department of homeland security, department of corrections, and local and/or tribal law enforcement. At least 30 percent of the FC respondents said that very frequently or frequently receive actionable intelligence from the FBI, DEA, Coast Guard, ICE, United States Attorneys, the State Health Department, the National Guard, private businesses, and critical infrastructure staff. Although a smaller percentage of SLT respondents note that they thought their agency received actionable intelligence frequently or very frequently compared to the FC respondents, SLT agencies are receiving significant amount of actionable intelligence and the distribution of responses is quite similar to the fusion center results.

Respondents from state, local, and tribal agencies were most likely to state that their agency very frequently or frequently received actionable intelligence from the sheriffs, state police, the state fusion center, Department of Homeland Security, the FBI, and the Department of Corrections. While not collected in the data, interviews and anecdotal evidence indicates that a notable portion of intelligence assessments and situational awareness bulletins are duplicative in that law enforcement personnel are often on multiple notification lists and reports, such as an FBI/DHS Joint Intelligence Bulletin, which may be sent to an individual from more than one source.

The many post-9/11 information sharing initiatives appear to be producing results since respondents reported considerable output and information sharing from both SLT and FC agencies. These results are presented in Table 3.5. Although 60 percent of the SLT agencies said their agency never provided specific intelligence briefings to federal law enforcement, 42 percent said they never provided briefings to other law enforcement agencies, and 21 percent said they never attended intelligence sharing meetings in a typical month, SLT respondents did indicate that they were very frequently or frequently sharing actionable intelligence with a number of organizations. For example, 61 percent of the respondents indicated that their agency very frequently or frequently provide actionable intelligence to other local law enforcement agencies, 55 percent did so for state law enforcement agencies, 38 percent said they did so for the FBI, and 44 percent they shared information with other federal law enforcement agencies.

As would be expected, the FC respondents were much less likely to note that their agencynever had intelligence briefings with federal law enforcement agencies, state, local, tribal law enforcement agencies, or intelligence sharing meetings. In addition, at least half of the FC respondents indicated that that were very frequently or frequently sharing information with federal, state, and local law enforcement, the FBI, other fusion centers, state government

officials, critical infrastructure security representatives, Department of Corrections, Emergency Management, fire marshals, homeland security, and the National Guard.

Table 3.5. Information Sharing Practices (Output)

Question	SLT	Fusion Center
# monthly intel briefings to federal LEA (% indicating never)	59.4%	28.2%
# monthly intel briefings to state, local, & tribal LEA	41.7%	12.7%
#monthly intel sharing meetings attended by staff	23.4%	6.2%
Frequency of providing actionable intel to FBI[1]	37.7%	63.7%
Frequency of providing actionable intel to other federal agencies[1]	43.5%	55.2%
Frequency of providing actionable intel to state law enforcement[1]	54.8%	84.0%
Frequency of providing actionable intel to local law enforcement[1]	60.5%	77.3%
Frequency of providing actionable intel to tribal law enforcement[1]	14.7%	22.5%
Frequency of providing actionable intel to state fusion centers[1]	36.2%	NA
Frequency of providing actionable intel to other fusion centers[1]	24.4%	63.0%
Frequency of providing actionable intel to state government officials[1]	25.8%	52.0%
Frequency of providing actionable intel to critical infrastructure security representatioves[1]	26.4%	57.5%
Frequency of providing actionable intel to Department of Corrections[1]	34.9%	52.7%

Frequency of providing actionable intel to Emergency Management[1]	35.9%	60.5%
Frequency of providing actionable intel to Fire Marshalls[1]	30.6%	50.0%
Frequency of providing actionable intel to Homeland Security[1]	33.9%	68.0%
Frequency of providing actionable intel to IRS[1]	16.7%	25.7%
Frequency of providing actionable intel to Hospitals[1]	21.3%	21.7%
Frequency of providing actionable intel to Private Sector Agencies[1]	19.1%	35.6%
Frequency of providing actionable intel to Public Health Agencies[1]	21.2%	41.3%
Frequency of providing actionable intel to Public Works[1]	24.3%	24.4%
Frequency of providing actionable intel to Transportation[1]	23.6%	45.4%
Frequency of providing actionable intel to National Guard[1]	22.5%	56.0%
Agency has processes for sharing terrorism info with public (Yes)	42.8%	58.0%

[1]Frequently/Very Frequently

The Distribution of Intelligence Products

Table 3.6 provides data related to how information is shared with others. These results support the conclusion that both SLT and FC agencies distribute intelligence products using a variety of different outlets. The most common way that both SLT and FC responses indicated that their products were distributed was email distribution lists. A large number of fusion center

respondents also indicated that their agencyshared intelligence products through personal contacts, memorandums, formal reports, via national intelligence communication systems (e.g., RISS.net, Law Enforcement Online), and other secure portals. Although smaller percentages of SLT respondents noted that their agency distributed products using these different mechanisms, 50 percent indicated that they distribute through personal contacts, 43 percent used memorandums or formal meetings, 40 percent used formal reports, and 38 percent said that distribute via national intelligence communication systems.

Table 3.6. Distribution of Intelligence Products

Method	SLT	Fusion Center
Formal Reports[1]	40.3%	64.9%
Periodic Memorandums	43.3%	66.2%
Formal Meetings	42.5%	64.9%
Secure Portal	35.9%	54.5%
Email	65.5%	79.2%
Telephone	35.1%	40.3%
Personal Contact	50.1%	71.4%
Website	20.0%	36.4%
Video Teleconference	7.7%	20.8%
Roll Call	22.5%	16.9%
National Intel Systems	38.1%	61.0%
Fax	17.8%	19.5%

[1]Distributed

In some, it appears policies and technologies have contributed to a substantial amount of information sharing among and between law enforcement agencies and fusion centers. Anecdotal evidence suggests that this information is being used by recipients, however, the extent and effects of usage represent a different set of metrics.

Chapter 4: Performance Metrics and Communication Networks

It has been documented previously that there have been significant changes within SLT law enforcement agencies regarding understanding the contemporary (i.e., post-9/11) law enforcement intelligence function, building an intelligence capacity, and meeting the demands for information sharing. The intelligence environment is changing at a rapid pace, and thus it has been difficult to assess the impacts of these changes. How can we measure intelligence reliably to know if it has prevented terrorist acts? Do we know if SLT law enforcement agencies have actually developed an operational "intelligence capacity"? How do we assess the quality of intelligence? How can the quality be improved? How do we know how well SLT agencies coordinate with federal intelligence access points? State level access points? Do SLT law enforcement agencies understand the types of information that should be collected and shared?

It is important to note that there is not widespread agreement about whether performance measurement in the intelligence arena is even possible or desirable (Treverton, et. al, 2006). This would appear to be an important empirical question that is worth pursuing in future research. It would be difficult for this research to proceed, however, without a foundational understanding of how law enforcement agencies currently decide what information is shared and why, and how key analytic hubs, like state fusion centers, effectively manage the massive amounts of information, make decisions about the quality of information, and are assessing performance among their personnel. What are the performance priorities? Is there concern with quantity or quality of products produced? Are there concerns about how intelligence impacts investigations? What other strategies are used to impact investigations? What analytic tools are being utilized to analyze raw information? Such critical information gathered from the key

producers and consumers of law enforcement intelligence can serve as the foundation for current and long-term assessment of our intelligence capabilities and the ISE in particular.

Assessing Analyst's Performance

Table 4.1 provides a listing of potential items related to assessing the performance of analysts. The results reveal that the first priority in assessment is the quality of items produced by the analyst. Over 70 percent of the FC respondents said the quality of strategic and tactical products were critical for assessment. Over 51 percent of the FC respondents said that the quality of risk assessments were critical for assessment. Forty-one percent of the FC respondents said making contacts with others outside the agency, and 31 percent said making contacts within the agency were critical for assessment. The quantity of products produced and whether the intelligence work was linked to investigations, actions, or convictions was much less critical for assessing analyst performance according to FC respondents. The logical reason for this finding is that the role of the analyst is to produce actionable intelligence. It is the role of operational units to use this information to decide whether and how to use the intelligence. Since the analyst has no influence on operational activities, assessing an analyst's performance based on outcomes would hold limited value unless there was feedback from operational units that the information from a given analyst consistently had limited or no value.

Table 4.1. Assessing Analyst's Performance

Factors	SLT	FC	Administration	Supervisor	Investigator	Analyst
Strategic Products	20.3%	27.0%	19.1%	23.3%	21.4%	13.2%
Tactical Products	17.3%	25.7%	17.0%	23.3%	15.5%	13.2%
Risk Assessments	13.3%	13.5%	10.6%	21.7%	14.3%	5.7%
Quality of Strategic Products	32.3%	71.6%	31.9%	36.7%	23.8%	41.5%

Quality of Tactical Products	30.3%	70.3%	33.0%	35.0%	19.0%	39.6%
Quality of Risk Assessments	23.3%	51.4%	22.3%	26.7%	19.0%	32.1%
Actions led to Investigation	19.7%	14.9%	22.3%	21.7%	19.0%	11.3%
Actions led to Arrest	20.0%	9.5%	21.3%	23.3%	21.4%	13.2%
Actions led to Conviction	11.0%	8.1%	11.7%	16.7%	11.9%	1.9%
Contacts with Personnel in Agency	21.3%	31.1%	24.5%	20.0%	17.9%	20.8%
Contacts with Personnel Outside Agency	22.7%	40.5%	26.6%	23.3%	19.0%	18.9%

In comparison, the SLT respondents also emphasized the quality of products produced but a lower percentage of respondents thought it was critical for assessing performance. Over 32 percent said that the quality of strategic products, 30 percent said the quality of tactical products, and 23 percent said that the quality of risk assessments was critical. The contacts made by analysts and the quantity of products produced were not thought to be particularly important for assessing performance. State, local, and tribal respondents were somewhat more likely to think that the work of analysts should led to investigations and arrests compared to the FC respondents. The SLT analysts had a similar view of assessment compared to administrators, supervisors, and investigators, although a higher percentage of the analyst respondents thought that the quality of products was critical for assessment and a lower percentage thought that is was critical that their work led to investigations, arrests, and convictions.

The research team wanted to look more closely at the performance priorities of the agencies by asking respondents to identify the top three factors critical to assessing performance by analysts. These results are provided in Table 4.2. Both FC and SLT respondents agree that

the quality of strategic and tactical products, as well as risk assessments, is critical to assessing the performance of analysts. These factors were the top three items for both samples and when comparing all positions in the agency. However, there was some variation when comparing the rank order of the rest of the items. In general, FC respondents indicated that information sharing activities and the quantity of products produced were somewhat more important, and having analysts' work lead to arrests, investigations, and convictions is somewhat less important compared to the rank ordering of items provided by the SLT respondents.

Table 4.2. Rank Order of Importance in Assessing Performance

Factor	SLT	FC	Administration	Supervisor	Investigator	Analyst
# Strategic Products	7	6	8	7	8	7
# Tactical Products	10	7	11	8	11	7
Risk Assessments	11	9	10	10	12	7
Quality of Strategic Product	1	1	1	1	1	2
Quality of Tactical Products	2	2	2	2	3	1
Quality of Risk Assessments	3	3	3	3	3	3
Actions led to Investigation	5	8	4	4	5	4
Actions led to Arrest	4	10	5	4	2	4
Actions led to Conviction	9	11	9	9	9	7
Contacts with Personnel in Agency	8	5	6	10	9	7

Contacts with Personnel in Other Agencies	6	4	6	6	6	6

Creation of Intelligence Products

Another way to think about performance is to document the types of intelligence products that analysts are being frequently asked to be produced. Table 4.3 presents data related to the creation of several intelligence products, and whether these products are never produced or produced every single day. Thirty-two percent of FC respondents said their agency produces bulletins every day, 24 percent of the FC respondents said they produce alerts every day, 21 percent said they produce warnings every day, 19 percent said they produce advisories every day, and 17 percent said they produce briefings every day. The SLT respondents indicated that such products are not as frequently produced every day and between 20 and 25 percent noted that most of products were never produced by the organization. Twenty-six percent of the SLT respondents said their agency never produces risk assessments, 24 percent said they never produce warnings or alerts, 22 percent said they never produce reports or briefings, and 17 percent said they never produce bulletins. It should be recognized that these are exploratory questions in order to develop a baseline for the types of products that may be available. In some agencies and fusion centers, staffing limitations likely require that a fairly narrow list of product types be developed based on the perceived priority of the organization's constituents. In other cases, the strategic priorities of an organization may not include all types of products – for example some organizations may never produce a risk assessment because it is not part of their charter.

Table 4.3. Creation of Intelligence Products

Product		SLT	FC
Bulletin	Never	17.0%	1.3%
	Daily	21.6%	32.9%
Risk Assessment	Never	25.5%	6.4%
	Daily	6.2%	2.6%
Advisories	Never	21.5%	2.7%
	Daily	13.8%	19.2%
Alerts	Never	17.8%	1.4%
	Daily	15.9%	24.3%
Warnings	Never	23.8%	4.3%
	Daily	14.2%	21.4%
Reports	Never	31.7%	10.5%
	Daily	6.6%	7.9%
Briefings	Never	21.7%	7.1%
	Daily	16.6%	17.1%

Table 4.4a and Table 4.4b provide a more detailed accounting of the types of products produced by the agencies in a typical month. SLT respondents (4.4a) and FC respondents (4.4b) were asked to identify within a range starting from 0 through over 50. The research team asked respondents to estimate the number of analytic products, intelligence briefs made to federal law enforcement, intelligence briefs to state and local law enforcement, intelligence sharing meetings, the number of permanent intelligence files opened, and the number of temporary intelligence files opened. Several findings can be observed based on their estimates. First, the SLT respondents were more likely to not produce any of these products in a typical month. Twenty-three percent said that their agency did not produce any analytic products, 60 percent reported they do not provide intelligence briefs to federal law enforcement, 42 percent said they do not provide intelligence briefs to local and state law enforcement, 23 percent said they do not

attend information sharing meetings, 45 percent said they do not produce permanent intelligence files, and 37 percent do not produce temporary intelligence files in a typical month. In contrast, only 3 percent of the fusion center respondents said their agency do not produce analytic products, 28 percent said that they do not brief federal law enforcement, 13 percent said they do not brief local and state law enforcement, 6 percent do not attend intelligence sharing meetings, 18 percent do not open a permanent intelligence file, and 16 percent do not produce a temporary intelligence file in a typical month. While one would expect the fusion centers to be much more active in information sharing activities as the data indicate, the findings pose some questions. For example, one would expect all fusion centers to produce intelligence products, provide briefings for SLT agencies, attend intelligence sharing meetings, and open intelligence files. Indeed, these activities are at the core role of fusion centers. One possible explanation is that fusion centers have been developed at an inconsistent pace across the country. Perhaps at the time these data were collected some of the responding fusion centers had been created but were simply not fully functional. Future research should explore this issue closely.

Table 4.4a. Number of Products Produced in a Typical Month (SLT)

Number	# Analytic Products	Intell Brief to Feds	Intell to Local/State	Intell Sharing Mtgs	Permanent Intell File	Temp Intell File
0	23.3%	59.4%	41.7%	23.4%	44.6%	37.3%
1-3	28.4%	30.5%	39.9%	46.0%	26.9%	27.6%
4-6	12.8%	4.4%	8.7%	20.8%	10.2%	10.0%
7-10	7.7%	2.3%	5.1%	5.7%	8.6%	11.1%
11-20	12.5%	2.3%	3.3%	2.6%	4.2%	6.2%
21-50	8.2%	0.8%	0.8%	1.0%	3.0%	5.1%
51+	7.2%	0.3%	0.5%	0.5%	2.5%	2.7%

Table 4.4b. Number of Products Produced in a Typical Month (Fusion Centers)

Number	# Analytic Products	Intell Brief to Feds	Intell to Local/State	Intell Sharing Mtgs	Permanent Intell File	Temp Intell File

0	2.6%	28.2%	12.7%	6.2%	17.6%	16.2%
1-3	15.4%	50.0%	46.8%	22.2%	27.0%	20.3%
4-6	21.8%	15.4%	21.5%	39.5%	14.9%	12.2%
7-10	19.2%	2.6%	8.9%	17.3%	18.9%	9.5%
11-20	11.5%	2.6%	6.3%	8.6%	13.5%	18.9%
21-50	24.4%	1.3%	3.8%	6.2%	1.4%	12.2%
51+	5.1%	0.0%	0.0%	0.0%	6.8%	10.8%

Both SLT and FC respondents reported that the agency typically produces between one and ten products each month, although, as one would expect, a higher percentage of the fusion center respondents reported that they produced between one and ten products for all categories considered. Overall, however, both SLT and FC respondents indicate that their agencies are actively engaged in producing intelligence products in a typical month. Nearly 49 percent of the SLT respondents said their agency produced between one and ten analytic products, 37 percent said they have between one and ten meetings with federal law enforcement, 54 percent said they have between one and ten meetings with state or local law enforcement, 73 percent had between one and ten intelligence sharing meetings, and 46 percent said that opened between one and ten permanent and temporary intelligence files in a typical month. Eighty percent of the FC respondents said that their agency had between one and ten intelligence sharing meetings, 77 percent said that they had intelligence briefings with local or state law enforcement, 68 percent said that they had between one and ten intelligence briefs with federal law enforcement agencies, 61 percent opened between one and ten permanent intelligence files, 42 percent opened between one and ten temporary intelligence files, and 56 percent said they produced between one and ten analytic products in a typical month.

Table 4.5 provides the results for questions related to some of the impacts of the intelligence products produced as well as the types of analysis and methodologies being used to process intelligence. Only 25 percent of the SLT respondents and 33 percent of the FC respondents said that intelligence products contribute to arrests frequently or always. Fewer respondents indicated that these products had an impact on assets seized. For context, the reader should recall that the intelligence function is designed to identify threats. As a result, operational activities based on the intelligence product may interrupt a threat before an actual crime occurs. It should also be noted that the standard to open an intelligence case file is a "reasonable suspicion" of a crime. While there may be a criminal nexus with an intelligence target's behavior, operational units may not be able to develop sufficient evidence to meet the more rigorous "probable cause" standard for an arrest. The point to note is that whether an intelligence product results in an arrest or seized assets is not a conclusive measure of effectiveness.

The rest of Table 4.5 provides a listing of different types of analysis that might be used to further the intelligence process. In general, a small and similar percentage of both SLT and FC respondents indicated that their agency used many of these analyses on a daily basis. For example, about 20 percent of SLT and FC respondents said their agency uses crime pattern analysis, 18 percent used crime mapping, 15 percent used hot spots analysis, and 10 percent used traffic analysis on a daily basis. There were some substantial differences when comparing some of the analytic techniques which really show how FC and SLT agencies have some different needs and priorities in terms of analysis. For example, it appears that sharing of products with others within the agency and across agencies is a higher priority in fusion centers. Sixty percent of the FC respondents said that shared intelligence within their agency on a daily basis and 48

percent said they share it with other agencies on a daily basis. In contrast, 40 percent of the SLT respondents said their agency shared intelligence within the agency on a daily basis and 34 percent said they shared intelligence with other agencies on a daily basis. In addition, the FC respondents indicated that analysts were involved in different types of analysis. For example, they indicated that their analysts were more likely to do visual investigative analysis, link analysis, social network analysis, telephone toll analysis, and flow charting analysis. Finally, the results show some evidence of the broader "all hazards" focus guiding fusion center practice as they were more likely to complete public health trend analysis on a daily basis. These are findings that one would intuitively expect.

Table 4.5. Impact of Intelligence Products & Nature of Intelligence Activities

Product/Operation	SLT	FC
Contribute to Arrests[1]	24.6%	33.3%
Contribute to Assets Seized	14.2%	16.9%
Crime Pattern Analysis[2]	20.2%	19.1%
Crime Mapping	16.0%	19.4%
Geographic Profiling	10.1%	13.6%
Hot Spots Analysis	13.5%	19.4%
Traffic Analysis	7.9%	12.7%
Produce Analytic Products	20.4%	26.9%
Analyze Suspicious Activity Reports	25.8%	43.3%
Critical Infrastructure Risk Assessment	8.3%	11.6%
Criminal Commodity Vulnerability Assessment	7.1%	8.2%
Statewide/Regional Risk Assessment	8.0%	11.1%
Shared Intelligence with Agency	40.3%	59.4%
Shared Intelligence with Others	33.7%	47.8%
Identify Criminal Enterprises	15.4%	18.8%

Identify Threats	25.1%	30.3%
Criminal Investigation Support	48.1%	58.5%
Proactive Strategic Analyses	18.4%	18.8%
Visual Investigative Analyzes	20.5%	31.7%
Alerts & Notifications	31.7%	46.3%
Deconfliction	21.2%	43.8%
Public Health Trend Analysis	3.8%	15.4%
Criminal Background Information	42.7%	57.8%
Case Correlation	31.0%	38.5%
Link Analysis	21.7%	39.4%
Social Network	16.3%	40.0%
Telephone Toll	14.0%	30.2%
Flow Charting	14.1%	32.8%
Table Tops	2.4%	1.5%
Live Trainings	2.4%	1.6%

[1]Frequently/Always [2]Daily

Communication Networks

Two issues regarding communication appear to be particularly important to examine. There is value to understand more about connectivity to current technical systems that were constructed to promote information sharing, such as FBI's Law Enforcement Online (LEO), the Regional Information Sharing System Network (RISS.net), the Homeland Security Intelligence Network (HSIN), and also know more about access to other sources of information. These advanced technical systems are critical to the success of the information sharing environment, the ability of law enforcement to prevent and solve crimes, and meeting the larger goals of the homeland security community. The analytic pieces of the intelligence puzzle will come from multiple sources, and the intelligence process must be supported by useful information technologies. Similarly, local investigations are significantly enhanced when officers have easy

access to timely and precise information, as well as when they are well connected with other law enforcement agencies. For these reasons, scholars have discussed how law enforcement is an area where "applications of information systems and practice are appealing and increasingly important" (Hu, Lin, and Chin, 2005: 235).

Table 4.6 provides information on whether the agencies surveyed were members of various advanced communication systems and whether several of these systems met their intelligence and information sharing needs. Most of the FC respondents indicated that their agency was a member of a regional RISS center, and a registered user of RISS.net, LEO, and HSIN. In fact, at least 85 FC respondents indicated that they were registered users of these systems. Less than half of the FC respondents indicated they were registered users of Automated Trusted Information Exchange (ATIX) and the FBI Network (FBINET). Fewer SLT respondents indicated that they were registered users of each of these communication systems. Nearly 83 percent of the SLT agencies were registered users of LEO, approximately 63 percent were members of a regional RISS center or had registered users of RISS.net, but only 40 percent of the SLT agencies were registered users of HSIN, 15 percent were registered users of ATIX, and 21 percent were registered users of FBINET.

Table 4.6. Access to Advanced Communication Systems

Question	SLT	FC
Agency is a member of regional RISS center	64.6%	85.4%
Agency personnel registered users of RISS.net	63.4%	85.5%
Agency personnel registered users of LEO	82.5%	96.4%
Agency personnel registered users of HSIN	39.7%	96.4%

Agency personnel registered users of ATIX	15.0%	42.0%
Agency personnel registered users of FBINET	20.6%	45.2%
RISS.net meets intell & info sharing needs[1]	28.8%	16.9%
LEO meets intell & info sharing needs	26.7%	17.3%
HSIN meets intell & info sharing needs	25.0%	23.8%
ATIX meets intell & info sharing needs	17.7%	11.1%
FBINET meets intell & info sharing needs	33.3%	25.6%

[1]Definitely

The FC respondents were also somewhat more critical of these communication systems in terms of meeting their intelligence and information sharing needs. That is, a lower percentage of FC respondents said that RISS.net, LEO, HSIN, ATIX, and FBINET met their intelligence and information sharing needs. Twenty-nine percent of SLT respondents said RISS.net definitely meets their intelligence and information sharing needs, 27 percent said that LEO meets these needs, 25 percent said that HSIN meets these needs, 18 percent said ATIX meets these needs, and 33 percent said FBINET meets these needs. Only 16 percent of FC respondents said RISS.net definitely meets, 17 percent said that LEO definitely meets, 24 percent said that HSIN definitely meets, 11 percent said that ATIX definitely meets, and 26 percent FBINET definitely meets their intelligence and information sharing needs. These findings are somewhat surprising since these are the primary portals for law enforcement agencies and fusion centers to share

sensitive but unclassified information. Future research should explore this issue by more explicitly defining the meaning of "meeting needs". In light of these results, there are likely many different interpretations of this – the research team cautions the reader from drawing any definitive conclusion about the value of these systems based on these findings alone.

Table 4.7 provides the results related to SLT and FC respondents access to various sources of information. Access here implies that there is opportunity to pull data into the intelligence process for analysis. In general, a large percentage of SLT and FC respondents indicated that they had access to motor vehicle reports, driver license records, correctional databases, National Law Enforcement Telecommunications System (NLETS), National Criminal Information Center (NCIC), Sex Offender Registries, and LEO. There were some substantial differences observed, however, when comparing the FC and SLT results. In fact, a higher percentage of FC respondents indicated that there their agency had access to IntelLink, Infragard, health-related data, Law Enforcement Information Network (LEIN), Law Enforcement Intelligence Unit (LEIU), HSIN, RISS, Open Source Information System (OSIS), the FBI's Regional Data Exchange (R-Dex) and National Data Exchange(N-Dex)), FBINET, High Intensity Drug Trafficking Areas (HIDTA), and the Homeland Secure Data Network (HSDN). For example, 20 percent of the SLT respondents but 42 percent of the FC respondents said they had access to IntelLink, 19 percent of SLT respondents but 63 percent of the FC respondents said they access to Infragard, and 34 percent of SLT respondents but 92 percent of the FC respondents said that they had access to HSIN. Both because of cost and mission, one would expect fusion centers to have access to a greater array of data systems.

Table 4.7. Access to Sources of Information

Source	SLT	FC

Motor Vehicle Records	92.9%	97.4%
Driver License Records	92.6%	97.4%
Correctional Databases	75.6%	85.5%
NLETS	73.0%	90.8%
NCIC	88.6%	93.4%
IntelLink	20.2%	42.1%
Infragard	19.3%	63.2%
Sex Offender Registries	88.6%	93.4%
Health-Related Information	23.3%	50.0%
LEIN	19.3%	36.8%
LEIU	18.2%	55.3%
HSIN	34.9%	92.1%
RISS	65.9%	93.4%
OSIS	11.6%	31.6%
LEO	74.4%	92.1%
R-Dex N-Dex	13.1%	48.7%
FBINET	22.4%	52.6%
HIDTA	44.0%	71.1%
HSDN	17.3%	57.9%

Chapter 5: Introduction to Fusion Centers and Case Study #1: Michigan Intelligence Operations Center

A key component of the ISE, fusions centers serve to coordinate efforts to identify risks to people, communities, and assets that support daily routines. More specifically fusion center personnel collect, integrate, analyze, and communicate information from public and private sectors so that steps can be taken to prevent, mitigate, or respond to terrorist attacks. By design and through practice, fusion centers are conduits between homeland security and law enforcement organizations operating at the local, state, and federal level, as well as industry groups (General Accounting Office, 2007b).

The development of a network of actors to contribute information with a view to countering terrorist activities is not without challenges. Previous studies have highlighted fusion centers with different goals, stakeholders and sources of funding, along with concerns about the long-term feasibility of these entities (Masse, O'Neil, & Rollins, 2007). To investigate these issues further, we asked our FC respondents additional questions about the creation and maintenance of their center.

Becoming operational

More than half of participants (53.4%) reported the state fusion center attained operational status between 2005 and 2007. 24.7 percent of respondents indicated the center was operational prior to 2005, while 21.9 percent stated the center was operational between 2008 and 2009. Additionally, 78.8 percent of FC respondents said there were defined goals for collecting, analyzing, and sharing information; 76.3 percent also indicated there was a process in place to add or remove stakeholders.

Interestingly, 60% of the fusion centers responded that their agency had an all crimes/all hazards focus while only 6.3% indicated their focus was only on terrorism. This is interesting because fusion centers have been accused of "mission creep" for expanding beyond the terrorism focus. While beyond the scope of this study, suffice it to note that fusion centers, while information sharing partners with federal agencies, are nonetheless entities of states or major urban area collaborative operating under the authority and guidance of their parent jurisdiction(s). While terrorism is certainly a priority of state and local jurisdictions, their daily and most frequent threat is from crime. It is more efficient and operationally effective for fusion centers to take an all crimes/all hazards approach rather than the more narrow "terrorism only" focus. As a result, this finding is not surprising.

Table 5.1. Respondents' assessment of resources for fusion center development

Resource	%
Fusion Center Guidelines[1]	58.7
Baseline Capabilities[1]	58.1
NCISP[1]	51.4
ISE[1]	34.3
National Preparedness Guideline and TCL[1]	29.0
Annual Fusion Center Conference[1]	60.3
Meetings and contacts with other fusion centers[1]	70.3
Meetings and contacts with federal LE officials[1]	37.3
Meetings and contacts with state LE officials[1]	44.0
Meetings and contacts with local LE officials[1]	47.3

Other DHS provided materials[1]	43.3
Training programs[1]	54.2

[1] Very helpful

Table 5.1 summarizes findings about resources FC participants found "very helpful" to consider as their center moved towards operational status. Leading items include meetings and contacts with other fusion centers (70.3%), the annual National Fusion Center Conference (60.3%), the Fusion Center Guidelines (58.7%), the Baseline Capabilities (58.1%), and training programs (54.2%). It is interesting to note these resources are likely to involve interaction with colleagues working in a similar role (i.e. training sessions and meetings) or are publications written for fusion centers guidance (i.e. Guidelines and Baseline Capabilities). On the other hand, FC participants were less likely to value materials about the ISE (34.3%) and National Preparedness Guidelines and TCL (29.0%). A somewhat higher number of respondents viewed meetings and contacts with local law enforcement (47.3%) as being more useful with respect to the center becoming operational than those held with state (44.0%) or federal (37.3%) counterparts.

Thus the research team sees the fusion centers continuing to become operational and the majority of these are likely to handle information relating to crime, terrorism and natural threats. With a broader mission most fusion centers are therefore sufficiently nimble to develop interagency partnerships to reflect changing needs within their jurisdictions. Similarly, in terms of identifying resources that assisted in centers attaining operational status, respondents found it very helpful when they consulted with colleagues in a similar position (i.e. lateral communication) or when they examined materials designed explicitly for fusion centers.

Maintaining a fusion center

There are different ways to fund a fusion center's activities including the government appropriations process, grant funds, and support through partnerships. However, more than half of the FC respondents (59.6%) said the federal government provided 50 percent or more of their funds, and 17.3 percent of FC respondents indicated federal government provided all the funding for their center. Anecdotally, the research team believes these data do not reflect the fusion center funding sources in 2011. As a result of the financial exigencies faced by the U.S. there have been reduced available grant funds. Through various fusion center meetings and conferences attended by the research team as well as conversations with fusion center directors, state and local governments have increased their proportional funding to support fusion centers, although current empirical data are not available. .

Previous research indicates the agency responsible for directing fusion center operations is mostly likely a law enforcement or public safety organization with statewide jurisdiction (General Accounting Office, 2007b). Likewise almost two-thirds (64.3%) of FC respondents identified a state agency as their center's lead agency, whereas a fifth (21.4%) said a municipal department fulfills this role. State law enforcement agencies are also most likely to have management responsibilities (68.9%). The most logical interpretation of these findings is to recognize there are 72 officially recognized fusion centers – one in each state and 22 fusion centers in major urban areas. However, it is more complicated than that. The structure of state law enforcement agencies vary – some states have a comprehensive full service state police agency. Others have a more diversified approach with a state patrol for primarily traffic functions with a state bureau of investigation responsible for criminal law enforcement. Other

states have created a state office of homeland security where the fusion center is housed. Most fusion centers have an oversight by a Board of Directors, which have varying degrees of authority over fusion center operations. The director of a fusion center may also rotate between agencies, which is particularly true of major urban area fusion centers. Typically, fusion center leadership is idiosyncratic to the organizational structures, political factors, unique state legislation and even personality factors of the state or major urban area. The question of future research is to determine which model(s) work(s) most effectively.

Table 5.2. Assignment of personnel to fusion centers from other agencies.

	%
State LE representative	87.3
County LE representative	54.9
Muncipal LE representative	62.0
Tribal LE representative	0.0
FBI intelligence analyst	60.6
FBI special agent	36.6
Federal DHS intelligence analyst	63.4
State DHS intelligence analyst	26.8
DEA intelligence analyst	2.8
National Guard representative	63.4
Legal representative	9.9
Private sector representative	7.0
Emergency operations representative	23.9

Public health organization	21.1
Fire service representative	46.5
Department of Corrections	23.9
TSA representative	22.5

On average there are 12 analysts working at a fusion center. Over a fifth of respondents (22.4%) said there is an intelligence analyst on duty in their center 24 hours a day, every day. However, as Table 5.2 shows, assignments of personnel to fusion centers from other agencies are commonplace. The most frequent assignments include law enforcement representatives from state (87.3%) and municipal (62.0%) agencies, along with a FBI intelligence analyst (60.6%) and a federal DHS intelligence analyst (63.4%), and a member of the National Guard (63.4%). In contrast it appears workers from the private sector (7.0%) seldom work in fusion centers. There a several reasons for this but three are most prominent. Civil libertarians are significantly opposed to private sector personnel working in fusion centers because of fusion center employees access to sensitive personal information could violate privacy protections. Another significant reason is concern by the private sector is that proprietary information may be compromised through fusion center information sharing practices. Another concern is that assignment to a fusion center may give a particular corporation some form of competitive advantage, hence the provision that a private sector representative must represent a sector, rather than an individual company. Given these controversies, many fusion centers have opted to avoid the added challenges of a private sector appointment. Indeed, most respondents (77.0%) indicated they worked in law enforcement prior to joining their fusion center and, unsurprisingly

given the sensitivity of law enforcement intelligence work, all but one of the respondents (98.7%) reported background checks are performed on all center personnel. In light of the security requirements for fusion center personnel this single exception was likely a mistaken response.

Perceptions of fusion center activities

The research team asked several questions that asked respondents to assess the services their fusion center provides. Ninety-two percent of respondents said they were very or somewhat familiar with the baseline capabilities for fusion centers, targets the United States Departments of Homeland Security and Justice (via the Global Intelligence Working Group) deem important for centers to attain in order to effectively share threat information while also protecting the rights and liberties of citizens. Only a quarter (25.9%) believed their center is completely aligned with these priorities. The Fusion Centers Baseline Capabilities were developed only shortly before the survey was administered; hence this finding is not surprising. Since that time, technical assistance has been provided to fusion centers to aid them in aligning their performance with the baseline capabilities. At the time of this writing, all fusion centers are going through an assessment of their adherence to the Baseline Capabilities.

Less than half of the respondents strongly agreed their center's intelligence products have a consistent format (41.0%), are disseminated in a timely manner (21.8%), and are actionable (19.2%). There is no uniform model for intelligence products and in 2009 there was significant criticism of the products released by some of the fusion centers. As a result, while there is still no prescribed format, standards related to content validity and civil rights have been articulated

with training provided to fusion center directors. Timely and actionable intelligence comes with experience and leadership. Future research should explore these issues in greater detail.

Respondents reported they receive and provide feedback to constituents about the information they share. Over 40 percent of respondents indicated constituents offer feedback on a daily, bi-weekly, or weekly basis, while 30.3 percent said their fusion center offers feedback to collectors at a similar rate. To draw upon the feedback FC respondents have received, the research team asked how they thought different constituents view intelligence-related analysis. According to respondents local (36.1%) and state (34.3%) law enforcement are most likely to find this activity very helpful, though this assessment drops for community leaders (12.5%) and private business (12.1%).

Table 5.3. Respondents' top concerns regarding fusion centers and the intelligence function.

Concern	%
Funding	27.7
Sharing information	21.7
Sustainability	15.7
Staffing	12.0
Civil liberties and privacy	10.8
Focus is too broad	9.6
Development of timely, actionable products	8.4
Interagency cooperation and coordination	8.4
Security of information	6.0
Lack of understanding about intelligence needs and concepts	6.0

Another item in the FC survey asked respondents to detail their top concerns with respect to the intelligence function and how their fusion center operates. The research team examined the submissions to create categories and counted the number of responses that matched a category, and then summed the counts. Table 5.3 lists the top ten items that respondents discussed and the leading concerns relate to the future funding of their fusion center (27.7%) and information sharing practices (21.7%). More specifically respondents expressed doubts about the availability of funds in subsequent years and they questioned whether the current levels of funding will be sustained (which they have not). With respect to information sharing, respondents questioned how many agencies are willing to participate in intelligence activities and suggested trust between (and within) agencies at different levels of government is occasionally fragile. It appears while improvements have been, fragility remains in some locales between fusion centers and some federal agencies.

A limitation of a tally is that it treats concerns as discrete items when they are often interrelated. For example, concern about funding also has implications for other items like the sustainability and growth of future center activities (15.7%), as well as worries about the center's focus being too broad (9.6%); to the availability of trained staff (12.0%) and the timely development of intelligence products that are actionable (8.4%). As such an alternative interpretation of respondents' concerns is that they reflect a dynamic environment in which fusion centers are constantly evolving so that they can manage their environments and remain relevant to stakeholders. As one respondent remarked, "The further we get from 911, the more it seems that intelligence and information sharing are no longer a priority."

Michigan Intelligence Operations Center

As each fusion center is developed with the determined needs of a geographic region, case studies conducted from varying regions within the U.S. provide a valuable glimpse into the different approaches, styles, and best practices of fusion centers across the country. While there are certainly consistencies across different fusion centers, each state has differing policies, resources, and missions by which their fusion centers operate. While many concepts may seem repetitive, the distinguishable characteristics, even if they are few, are what make this case study approach beneficial to the law enforcement population. This chapter will explain the approach taken by the state of Michigan with the creation of the Michigan Intelligence Operations Center (MIOC).

In accordance with the *Fusion Center Guidelines*[10] published by the U.S. Department of Justice, Office of Justice programs, the state of Michigan identified a fusion center as an actual physical structure where government security and public safety partners collaboratively work together sharing information, developing intelligence, maximizing resources, streaming operations, and analyzing data to improve the ability to fight crime and terrorism. On December 20, 2007, Michigan Governor Jennifer Granholm signed Executive Order No 2007-47 which officially established the Michigan Intelligence Operations Center[11] (MIOC) as the sate fusion center for Michigan to enhance the state's ability to improve prevention and preparedness.

Housed in Lansing, Michigan, the MIOC is an "all threats, all hazards" fusion center. While it provides support for international and domestic terrorism, organized crime, identity theft, all gang types, narcotics and smuggling interdiction, financial crimes, crime mapping, and

[10] For the complete *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*" report visit: http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf
[11] Also referred to as the Michigan Intelligence Operations Centers for Homeland Security.

cybercrime, the MIOC also manages resources and information to best prepare for, and respond to, natural disasters. In order to meet its mission, to promote public safety by operating in a public-private partnership that collects, evaluates, analyzes, and disseminates information and intelligence in a timely and secure manner while protecting the privacy rights of the public, the MIOC provides 24-hours-a-day (every day of the year) statewide information sharing among all levels of public safety agencies and private sector organizations in order to facilitate the collection, analysis and dissemination of intelligence relevant to terrorism and public safety.

Composition of the MIOC

The Michigan State Police (MSP) and Michigan National Guard (NG) comprise the primary partnership which facilitates the MIOC. While also working closely with the State Emergency Operation Center (SEOC) during times of emergency response, the MIOC relies upon formal partnerships with multiple law enforcement organizations. Most notably, these organizations include, but are not limited to:

- Michigan State Police
- Michigan National Guard
- Federal Bureau of Investigation
- U.S. Department of Homeland Security
- Michigan Homeland Security
- Michigan State University Police Department
- Michigan Department of Corrections
- Michigan Department of Transportation
- U.S Coast Guard

Beyond these formal partners, the MIOC is also responsible for administering the State Information System (STATIS) and Michigan Intelligence Information System (MCIS) as well as being the state designated liaison for INTERPOL, the Financial Crimes Enforcement Network (FINCEN), the Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network

(MAGLOCLEN), and the Criminal Intelligence Service of Ontario (CISO). Furthermore, the MIOC is the state point of contact for the National Alert Warning Answering System and is responsible for reviewing Law enforcement Information Network (LEIN) requests by other law enforcement agencies and the Department of Energy. Lastly, the MIOC facilitates information sharing to the FBI's Joint Terrorism Task Force (JTTF) and the High-Intensity Drug Trafficking Areas (HIDTA) located in Detroit by assigning detective sergeants to these initiatives.

Given the private sector has a critical role in the protection of the state's critical infrastructure, as well as their desire to protect their assets, employees, and customers, the private sector is an integral member of the MIOC. Additionally, they provide important sources of information as private sector security often has better observation capabilities and knowledge of the activities occurring around their local facilities and around the world. This data is useful to the fusion center analysts in identifying emerging trends or threats related to preventing terrorism and criminality.

Advisory Board

The advisory board for the MIOC was developed to serve as an advisory body within the Department of State Police. Consistent with Executive Order 2007-47, and appointed by the governor of Michigan, advisory board members are represented by the following:

- Department of State
- Department of Military and Veteran Affairs
- Department of Civil Rights
- Department of Corrections
- An individual representing local police departments in the state of Michigan (likely from the Michigan Association of Chiefs of Police).
- An individual representing local sheriff's departments in Michigan (likely from the Michigan Sheriff's Association).
- An individual representing the office of a county prosecuting attorney (likely from the Prosecuting Attorneys Association of Michigan).

- Five Michigan residents representing federal homeland security or law enforcement agencies.
- Three non-law enforcement residents from the state of Michigan.

Functional Desks

Michigan's information sharing environment structure positions the MIOC to be the entity responsible for fusing threat information gathered for the purpose of providing early warning. As such, each functional desk must identify potential threats that impact public safety and provide timely alerts to appropriate liaisons. Similarly, each functional desk in the MIOC is designed based on a needs assessment (McDaniel et al., 2008). Michigan homeland security operations identified the need for the fusion of shared information on critical infrastructure networks, environmental risks, and international trafficking concerns. These conclusions were founded on an assessment in which the state of Michigan utilized an ethnographic study based on interviews and surveys of both the public and private sector. This ethnographic approach was used to determine the mission and objectives of the MIOC and set its security goals as well. The security goals were broadly stated as the protection of people and key facilities and institutions. A gap analysis yielded three fundamental operations to initially guide the MIOC. Surveys exploring efforts to collect and analyze information focused on three core mission areas; 1) critical infrastructure protection; 2) border security; and 3) environmental health and welfare protection (McDaniel et al., 2008).

Critical Infrastructure and Key Resources Protection Desk

Critical Infrastructure and Key Resources (CIKR) protection desk coordinates the collection, analysis, and dissemination of CIKR information and intelligence. The security partners in this desk include state agencies that share a common mission of protecting the state's CIKR. This mission could be achieved through these agencies working together by pooling their

resources and skills, as well as collaborating with the state's different CIKR owners. The CIKR desk is considered a baseline capability for the state fusion center[12]. The CIKR desk within the MIOC is the centralized location for all critical infrastructure information, warnings, reporting, dissemination, and program coordination. The desk provides critical interface between the private and public sectors. The roles and responsibilities of this desk are to conduct public and private sector outreach to promote capabilities of the MIOC, maintain and develop two way communications between the desk and the CIKR operators, and security mangers to encourage cooperation in information sharing and management, to work with MIOC analysts to collect and vet Suspicious Activity Reports (SAR), and finally to serve as the state link to the Department of Homeland Security (DHS) for CIKR programs and information sharing.

The CIKR desk was created in the MIOC to centralize all CIKR information. Within the MIOC, this desk is staffed by analysts from the state's National Guard (NG) and the Michigan State Police (MSP). They are the two state agencies participating in the MIOC homeland security initiative pertaining to the protection of the state's CIKR. In the future, other state public safety agencies with CIKR related functions may be assigned in the MIOC. The design and processes for the CIKR desk were designed to be consistent with the Department of Homeland Security's *National Infrastructure Protection Plan* (NIPP)[13]. This approach includes the "protection plan strategy" which was the framework for the mission of the CIKR desk.

Both the NG and MSP each bring unique expertise and resources to the CIKR desk. The NG analysts assigned to this desk maintain the ability to analyze risks and vulnerabilities. Furthermore, the NG's resources include equipment used in detecting gaps in the security

[12] For the complete "Baseline Capabilities for State and Major Urban Area Fusion Centers" report visit: http://it.ojp.gov/documents/baselinecapabilitiesa.pdf
[13] For the complete "National Infrastructure Protection Plan" report visit: http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

programs of critical infrastructures. MSP's current resources enable the desk to gather information and intelligence through both the law enforcement community as well as the patrol personnel on the streets. This network enhances the analytical capacity of the desk. Community members call the state police with suspicious activity reports which are then funneled to the MIOC. Law enforcement officers who encounter suspicious activities throughout their patrols call the MIOC for verification of the SAR information and cross reference criminal databases.

Given the majority of America's critical infrastructure is located within the private sector, their inclusion as members of the MIOC and CIKR desk further enhance the desk's capabilities. Though private sector liaisons are not integrated to the MIOC on a full-time basis, this desk shares intelligence analysis products with the private members. Appropriately classified information is forwarded to private members on a "need to know" basis under the auspice that in turn the MIOC expects the private sector to collaborate with them by sharing pertinent private sector information consistent with the memorandums of understanding (MOU) that facilitate the partnership. A pivotal aspect by which the CIKR desk collaborates with the private sector is the uniqueness of the analysts and any specific knowledge or subject matter expertise of sector operations they may bring to the desk that may be out of the MIOC analysts' purview. Most members of the private sector do not have the information capabilities to integrate threat information. Effective protection of the state's critical infrastructure requires the sharing of information and resources. This sharing approach is facilitated by connectivity to the DHS Homeland Security Information Network (HSIN) - a national, web-based communications platform that allows multi-jurisdictional law enforcement entities, and other security partners to obtain, analyze, and share information.

Proposed Functional Desks

While they have yet to materialize as of the writing of this report, the MIOC has had discussion about further enhancing their preparedness and intelligence efforts by implementing an Environmental Risk Desk as well as a Border Security Desk. Although not currently implemented, a brief discussion of these proposed functional desks is pertinent to the case study narrative as well as the intent of this report. The concept of each desk maintains potential for other fusion centers or agencies to develop a similar approach.

Conceptually the proposed environmental risk desk (ERD) would coordinate the collection, analysis, and dissemination of environmental and public health-related data relevant to terrorism and public health and welfare. Unlike the CIKR Desk, which has the NIPP serving as the blue-print for its operations and a long-term relationship between the NG and MSP, the planned EPD would engage in varying initiatives across sectors that will hopefully serve to create the structural foundation and formal collaboration between the participating agencies. Partners of this desk would include state agencies that share the common organizational purpose of protecting the public's health, whether focused on environmental, workplace, food supply, or water systems. These agencies have a common purpose to develop public health and environmental intelligence, a goal which could be achieved by sharing their resources and expertise and collaborating with the state's traditional private and public health-care providers. If the ERD were to come to fruition, it is expected that such a partnership would gradually evolve into a collaborative partnership, where formal arrangements would allow representatives from each security partner to serve as a liaison at the MIOC. Moreover, such a future partnership and physical presence in the fusion center of the state would enable the ERD to take

a leading cooperative role and strategic actions on environmental and health-related information and intelligence.

A second proposed functional desk is a Border Security Desk (BSD) which would be established by those agencies that have the common purpose of securing Michigan's international border with Canada. Whether the public or private agency mission is the prevention of the illegal introduction of humans or contraband into the state, or the agency mission involves regulation of the mode of transportation of contraband into the state, or the ownership of those transportation modes, the shared focus on the international border is becoming an increasingly important demand with respect to understanding and responding to security issues. Such participating agencies would need to share information and, more importantly, share their experience of the potential trends in border security issues. Thus, organizations whose core missions concern the identification of contraband can collaborate on their shared goal. In fact, some of the initial federal and state agencies that may work together in a planned BPD could be as disparate as the Department of Homeland Security's Customs and Border Protection (CBP), and the state's health and agricultural departments.

An additional concern to Michigan public safety/health is the danger of agricultural threats or agro-terrorism agents being introduced through the state's ports of entries – such as diseases that could have a direct impact on the state's economy. One of the challenges for the proposed BPD is the inherent difficulty in ascertaining intelligence on persons or goods attempting to enter illegally until the attempt to enter results in apprehension. Through the state and federal police agencies, the desk could expand its information capacity on people and goods illegally entering the state by collaboration with Canada. The complexity of border security should therefore encourage participating agencies to initially work together and share resources

through a different collaborative partnership. The starting arrangement would not be a full-blown collaborative undertaking, but an open-dialogue network established on trust and two-way communication.

The proposed BPD would likely work on a different continuum of collaborative effort. Agencies participating in this desk would have interactive contacts or exchange information, or they would conduct ad hoc activities between and among themselves to accomplish the shared purpose of detection of contraband. The whole point is for the different agencies to begin working together and sharing resources, such as exchanging ideas, news, and reports. It is hoped that this initial interaction would lay the groundwork for a future collaborative partnership, one that has a more formal arrangement where the different security partners of this desk detail analysts to the MIOC and collaborate in the detection and analysis of border security-related terrorism information.

Information Resources

In order to facilitate the MIOC's mission, the state of Michigan has identified standing information needs. These information needs, consistent with standing intelligence requirements – those pieces of disparate information needed to maintain awareness of ever-present threats to the state and the U.S. homeland - have been established to maintain constant information flow with respect to the on-going threats identified by the state. These standing information needs are as follows:

Overt threats to U.S. Homeland Security	HSEC-01-00000-ST-MI01-2010
Domestic extremism	HSEC-14-00000-ST-MI01-2010
Prison radicalization	HSEC-14-03000-ST-MI01-2010
International terrorism	HSEC-22-00000-ST-MI01-2010
Critical infrastructure protection and key resources	HSEC-02-00000-ST-MI01-2010
Illicit drugs and precursor chemicals	HSEC-05-00000-ST-MI01-2010

Air and marine interdiction	HSEC-13-00000-ST-MI01-2010
Fraud (individuals and organizations)	HSEC-07-00000-ST-MI01-2010
Alien smuggling and human trafficking	HSEC-08-00000-ST-MI01-2010
Customs and border security	HSEC-04-00000-ST-MI01-2010
Violent gangs and criminal organizations	HSEC-16-00000-ST-MI01-2010
Plans and preparations for cyber-attacks against Michigan	HSEC-20-00000-ST-MI01-2010

In order to maintain awareness with respect to these standing information needs, the MIOC maintains comprehensive, cross-indexed, information that is relevant and useful in identifying information related to these needs as well as criminal activities, suspects, and associates. MIOC personnel collect and analyze vast amounts of information. The MIOC uses this information to target specific criminal activity and terrorists/extremists to identify trends for proactive law enforcement planning. Personnel within this section of the MIOC provide a variety of intelligence products to alert all law enforcement agencies of common problems, current trends, and the identity and method of operation of fugitives. Specific sources – or connectivity – currently utilized by the MIOC include:

- Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network (MAGLOCLEN)*
- Law Enforcement Online (LEO)*
- eGuardian*
- E-Team
- Criminal Justice Information Network*
- I-Service Gateway
- Rapid Start
- Interpol
- State intelligence database
- Links to national databases
- Investigative databases
- Federal networks and databases
- Department of Defense networks
- Homeland Security Information Network (HSIN)*
- Homeland Security Data Network*
- Riverglass

*Denotes subscription to information sharing network

To manage this wide-range of information sources, the MIOC employs Memex intelligence software systems. Memex, a SAS Company, provides intelligence management and analysis solutions for law enforcement, military intelligence and commercial organizations that help to improve intelligence processes, enhance public safety, and prevent and deter criminal acts. Memex places a great deal of emphasis on information sharing, compatibility and compliance with existing law enforcement systems. Its intelligence platform provides a single-source portal for analyzing Records Management Systems (RMS), Computer-Aided Dispatch (CAD), intelligence files, Suspicious Activity Reporting (SAR), open source data collection, and a variety of other data sources – whether via data integration, federated access, or a hybrid approach. This compatibility enables the MIOC with the capability to seamlessly examine all the data in one place, using the same data mining tools and user interface, rather than having to log on and off different systems. To help ensure information is flowing efficiently via Memex, the MIOC employs an individual dedicated to managing Memex and serving as a trained liaison with the Memex company.

Fusion Liaison Officer Program (FLO)

In an effort to further enhance their information gathering and sharing capabilities, the MIOC has a formal Fusion Liaison Officer (FLO) program. FLO programs provide an effective way for fusion centers to engage with other law enforcement entities since FLOs serve as liaisons between their agency and the fusion center. These FLO personnel help to facilitate their agency's participation in regional information exchanges, ensuring their agency is a full partner in the fusion center and information-sharing processes. This program may offer part of the solution to effectively support information sharing between fusion centers and local agencies, in

coordination with other initiatives. As the time of this report, to be a member of the MIOC FLO program personnel must be an active sworn law enforcement officer, sworn firefighter, U.S. military, an analyst with a law enforcement agency, a member of a tribal law enforcement agency, or the Michigan Department of Corrections.

The basic functionality of FLO members is that they must have consistent interactions with the community through calls for service, be able to share time between both their regular duties and the MIOC, and have the ability to successfully complete a background investigation to obtain the necessary security clearance. Through these basic functions, FLO members are expected to be a conduit for criminal intelligence to and from their community, department, and the MIOC. Being a FLO member also requires personnel to perform threat vulnerability assessments, provide on-scene support, maintain a comprehensive point of contact list, and educate other law enforcement officials and their communities about information sharing initiatives – such as the Nationwide Suspicious Activity Reporting Initiative.

Typical activities for an FLO include reviewing information bulletins or intelligence products disseminated by the MIOC, receiving or providing terrorist or criminal indicators awareness training, and fielding inquiries from agency colleagues or the fusion center. The FLOs have the responsibility to develop the information-sharing network in their own agencies, broadening the reach of the program and increasing the benefit to all members of the agency. As noted, further responsibilities may include conducting outreach to contacts in their own agencies, making their colleagues aware of the MIOC and its role in the region, disseminating information from the MIOC, providing criminal and terrorism awareness resources or training to help field officers identify indicators and warnings, and serving as a resource for colleagues. Making this

program most effective is a coordinator at the MIOC, FLOs at a majority of local agencies, and a formalized plan and training program that describes the roles and responsibilities of the FLOs.

Figure 1 illustrates the complex flow of information to and from the MIOC, its partners, and its resources.

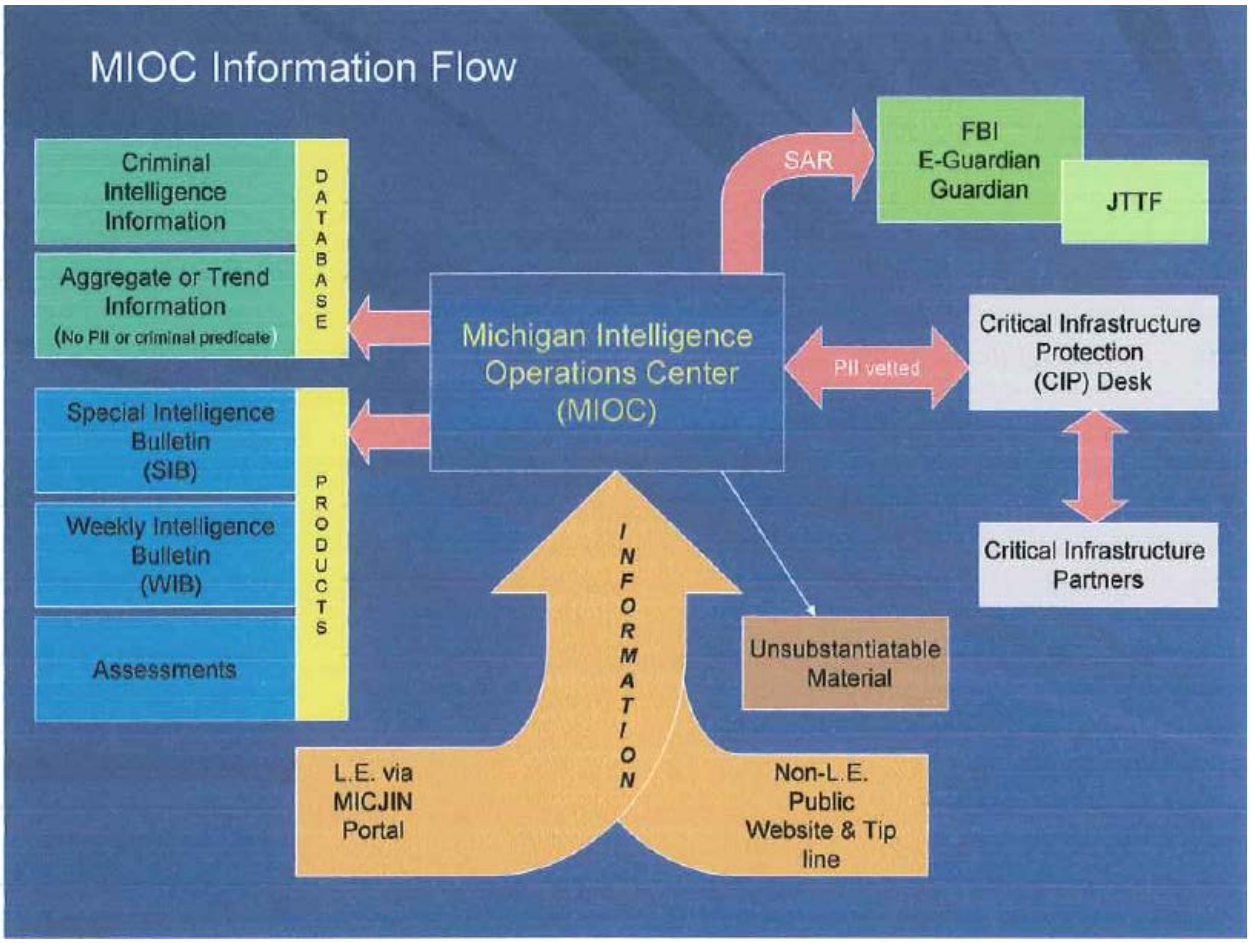


Figure 1. Information Flow to and from the Michigan Intelligence Operations Center

Analytic Capability

By managing the flow of information and turning intelligence into actionable knowledge, the MIOC supports law enforcement, public safety, and the private sector. By analyzing data from

different sources, the fusion center supports efforts to address immediate or emerging threat related circumstances and events. At the same time, it supports the implementation of risk-based, information driven prevention, response, and consequence management programs. Analyst personnel within the MIOC also provide investigatory assistance in the areas of telephone toll analysis, charting of complex criminal investigations to aid with presentations to prosecutors and juries, and Tip Center information analysis for major criminal cases. By assisting in these areas the MIOC is able to identify gaps in information needs across agencies and sectors. Furthermore, MIOC analysts process all requests for information received from public tips lines. This information is analyzed and disseminated to local and state agencies. These tip lines include the Help Eliminate Marijuana Planting (HEMP) initiative, arson, methamphetamines, suspicious activity reports, "Crime Stoppers", and reported school violence. Analysis of the multiple information and data types is communicated to MIOC partners through a variety of intelligence products. These products include, but are not limited to:

- Michigan Law Enforcement Bulletin
- Weekly Information Briefings
- Special Intelligence Bulletin
- Situational Awareness Bulletin
- Intelligence-Led Policing and Protection Plans

These analysis products are shared with partners and actively distributed (pushed) through secure information systems. Furthermore, these products are uploaded to sharing systems where they remain available to be accessed (pulled) via queries that may be related to the content of the product.

Privacy

The post-9/11 environment requires increased security needs that not only require enhanced information sharing, but also emphasize the need to balance the sharing of information with the rights of citizens. Ethical and legal obligations compel personnel, authorized users, and participating entities to protect constitutional rights, including privacy and other civil liberties, and civil rights throughout the information sharing process. To accomplish this, appropriate privacy and civil liberties protection policies must be in place. Like all fusion centers, the MIOC has developed and implemented a comprehensive privacy policy consistent with the *Fusion Center Privacy Policy Development*14 published by the U.S. Department of Justice.

The purpose of the privacy policy is to articulate within the MIOC, to external agencies that access and share information with the MIOC, to other entities, and publicly that the MIOC will adhere to legal requirements and MIOC policy and procedural provisions that enable gathering and sharing of information to occur in a manner that protects constitutional rights, including personal privacy and other civil liberties, and civil rights. The Michigan State Police has primary responsibility of the MIOC for the overall operation of its justice systems, operations, information collection and retention procedures, coordination of personnel, and the enforcement of the privacy policy.

Primary responsibility for the activities of the MIOC, its systems, operations, and coordination of personnel and the enforcement of the privacy policy is assigned to the MIOC Director within the MSP. The MIOC is guided by an agency-designated privacy committee that liaises with community privacy advocacy groups to ensure that privacy and civil rights are protected within the provisions of this policy and within the MIOC's information collection, retention, and dissemination processes and procedures. The MIOC privacy committee is guided

14 For the complete "Fusion Center Privacy Policy Development Privacy, Civil Rights, and Civil Liberties Policy Template" report visit: http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

by a trained privacy officer who is appointed by the Director of the MIOC who will select the most qualified individual to serve in this position. The MIOC Privacy Officer receives reports regarding alleged errors and violations of the provision of this policy, receives and coordinates complaint resolution under the MIOC's redress policy, and is the liaison to with the Program Manager's Information Sharing Environment (ISE), ensuring that privacy protections are implemented through efforts such as training, business process changes, and system designs that incorporate privacy enhancing technologies.

Training

Given the complex operations of the MIOC, such as the Critical Infrastructure and Key Resources Desk, Fusion Liaison Officers, comprehensive analytic strategies, and diverse partnerships, a wide-range of training is necessary to ensure consistency with MIOC policies. As many of the MIOC policies (e.g. privacy) are developed in concert with those established by the Department of Homeland Security (DHS), the MIOC utilizes training programs offered by DHS to train their own personnel as well as formal partners and local agencies engaging with the MIOC. While DHS-sponsored training programs for fusion centers are becoming less prevalent as a result of decreased budgets, fusion centers have to develop their own training programs. The MIOC is developing and recommending training programs for their partners. These efforts are important in building awareness, institutionalizing the importance of criminal intelligence, increasing the value of intelligence personnel, fostering relationships among the law enforcement community, and improving the ability to detect and prevent acts of terrorism and other crime. All MIOC personnel are required to review the federal fusion center guidelines published by the U.S. Department of Justice.

All persons holding manager/supervisor positions within the MIOC are required to review the following documents and attend the following training programs (while they remain available):

- Fusion Center Guidelines Executive Summary
- MSU Intelligence Toolbox Program
- Criminal Intelligence for the Chief Executive
- State & Local Antiterrorism Training (SLATT)
- 28 Code of Federal Regulation Part 23*15*
- Antiterrorism Intelligence Awareness Training Program (AIATP)

Executives at the MIOC acknowledged one of the major areas for enhancing the center's capabilities would be to market their resources and mission to their local law enforcement agencies. Executives noted a general awareness of the fusion center by local agency personnel, however many agencies lacked knowledge with respect to the MIOC's available resources and mechanisms for sharing information. In efforts to remedy this shortcoming, local law enforcement agencies engaged, or seeking to engage, with the MIOC, the following training programs are provided by the MIOC:

- Intelligence Liaison Officer (ILO) Training: The MIOC offers introductory intelligence liaison officer training geared towards the investigator and uniformed road officer. This training program includes modules on:
  - MIOC-Fusion Center Overview & MIOC Reporting & Contact Information
  - International Terrorism
  - Domestic Terrorism
  - Fraudulent Documents and Facial Recognition
  - Weapons of Mass Destruction Brief
  - Homeland Security Teams (Narcotics, Smuggling & Human Trafficking)
  - Organized Crime
  - Terrorism Screening Center (TSC) & Joint Terrorism Task Force (JTTF)
- MIOC Onsite Field Training: The MIOC offers opportunities for employees of local law enforcement agencies to work and train directly with investigators and analysts in the MIOC. Field training is determined on a case by case basis.

15 Codified as 28 CFR Part 23 "Criminal Intelligence Systems Operating Policies", this regulation governs inter-jurisdictional and multi-jurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies and that are funded by or receive federal funds.

Chapter 6: Case Study #2: Florida Fusion Center

The vast majority of state, local, and tribal law enforcement agencies in the U.S. are either unaware of, or struggling with, building an intelligence capacity. These ambiguities are compounded by implementation fidelity – best practices in one agency may not translate to another. Such a problem creates an obstacle for conducting case studies on law enforcement intelligence practices. A solution is to identify an environment where intelligence practices are most likely to be applied consistent with federal guidelines and recommendations and most generalizable to the broad law enforcement community. Fusion centers provide such an environment as they are law enforcement organizations specifically structured to engage in law enforcement intelligence practices. While the average fusion center has significantly different organizational characteristics as compared to the average local law enforcement agency, the principles of engaging in information sharing, establishing a system of performance metrics, and building communication networks are quite similar.

This chapter provides a case study from the Florida Fusion Center. The Florida Fusion Center is unique given a rich tradition of law enforcement intelligence within the state of Florida as well as the state's geographic and demographic composition. This case study is provided as a means to provide context for law enforcement intelligence practices. Moreover, little is known about the operations and administration of fusion centers and thus the narrative to follow provides a unique glimpse into the fusion center environment. Intersections between the case study and relevant constructs and the findings presented earlier will be discussed.

The Florida Fusion Center

The Florida Fusion Center (FFC) is physically located within the Florida Department of Law Enforcement's (FDLE) Office of Statewide Intelligence, located at FDLE headquarters in Tallahassee, Florida. Officially created in January 2007, the FFC operates under the authority of FDLE as recognized in the Florida State Statute 943[16]. The mission of the FFC is to protect the citizens, visitors, resources, and critical infrastructure of Florida by enhancing information sharing, intelligence capabilities and preparedness operations for all local, state and federal agencies in accordance with Florida's domestic security strategy. The FFC serves as the state node in that it provides connectivity and intelligence sharing among the regional fusion centers as well as the regional domestic security task forces.

For forty years the FDLE has operated a centralized intelligence unit that supported criminal investigative efforts of local, state and federal law enforcement agencies. This rich history of law enforcement intelligence practices within the state of Florida presents a unique environment in which FDLE was able to respond quickly to emerging initiatives and flourish in a dynamic intelligence environment where other agencies have endured struggles. This context provides a unique opportunity for this study to examine law enforcement intelligence practices within an intelligence environment that has evolved over time. As a result of this evolving intelligence environment, the structure of intelligence and information sharing among law enforcement agencies and other organizations within the state of Florida has also evolved and thus requires a step-by-step explanation of how the different entities of the information sharing structure have been established and communicate.

Structure of Law Enforcement Intelligence in Florida

[16] 943.0321 The Florida Domestic Security and Counter-Terrorism Intelligence Center and the Florida Domestic Security and Counter-Terrorism Database. This statute can be accessed at: http://www.leg.state.fl.us/Statutes/

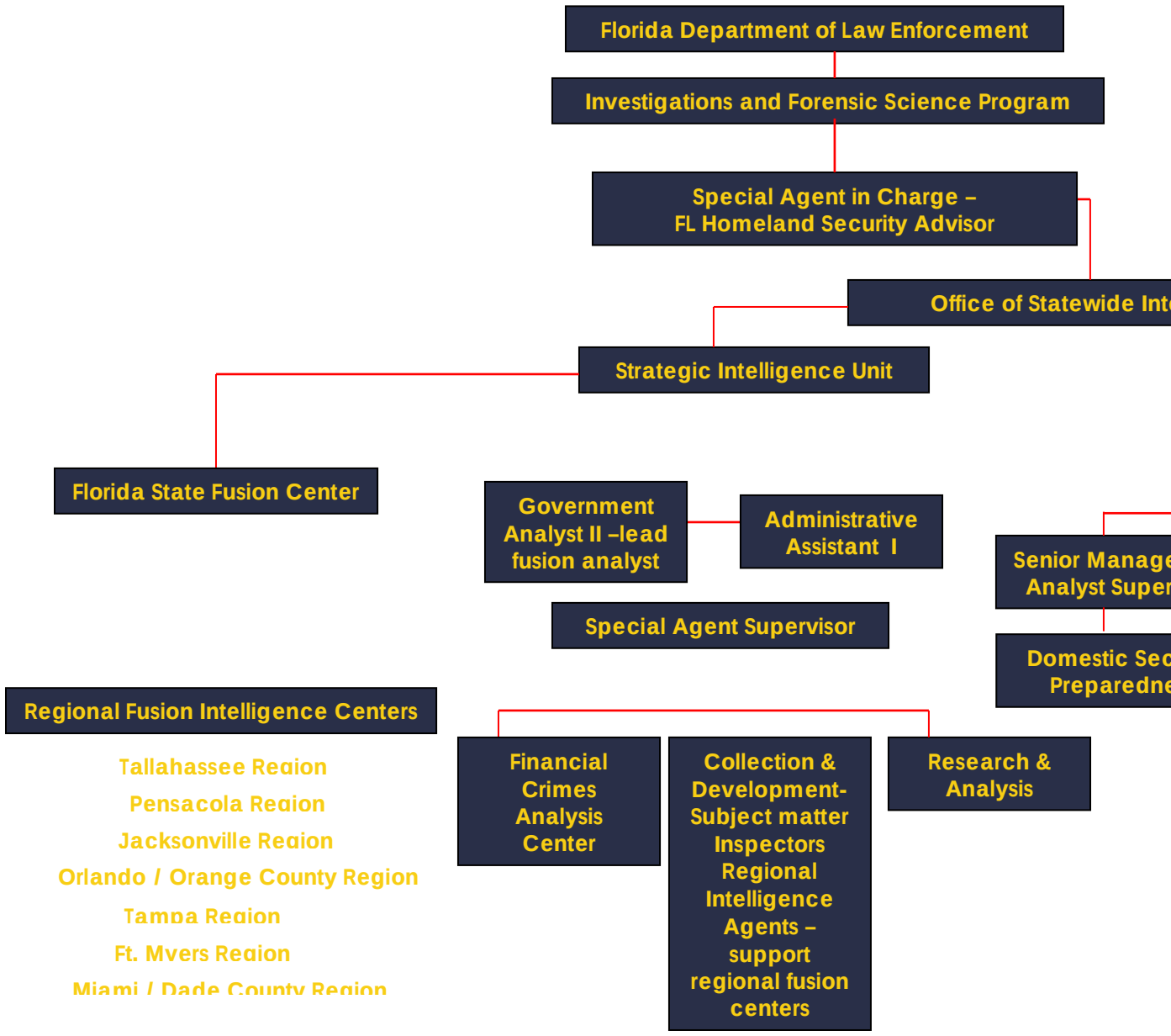
The Office of Statewide Intelligence and the Florida Fusion Center

While the state of Florida has been actively sharing information for decades, the heart of Florida's intelligence operations was established in 1996 with the creation of the Office of Statewide Intelligence (OSI). This new office within FDLE was designed to refine the analytical and investigative efforts of FDLE to be centered on an intelligence-led approach. The OSI is comprised of multiple intelligence divisions to support the over-arching function of intelligence practices and intelligence-led policing. To further enhance this intelligence-led approach adopted by FDLE, the Florida state fusion center was created in 2007 to expand information sharing to include a more broad "all-threats, all-hazards" approach to threat prevention. While the OSI and FFC are staffed by similar personnel and both serve as a threat-prevention function of FDLE, they are separate entities operating together, separated by a key distinction that will be discussed. Figure 1 illustrates the structure of FDLE's Investigations and Forensic Science portion of the organization – the other significant portion of FDLE is public safety[17].

The primary mission of the OSI is to provide FDLE leadership with sufficient information so that they may make informed decisions on the deployment of resources to best carry out FDLE's mission. The OSI plays a primary role in the planning and direction, analysis, reporting, and evaluation of FDLE intelligence products and serves as the core resource of the Florida Fusion Center. The OSI is responsible for the coordination of FDLE's intelligence efforts, analysis of intelligence and crime data information, and dissemination. Although other functions take place in OSI, its primary focus is to ensure timely information are available so critical decisions can be made based on the best available intelligence.

[17] For a complete FDLE organizational chart visit: http://www.fdle.state.fl.us/Content/getdoc/f3f99431-903b-4209-8d00-b3e0e4bc4be4/Org-Chart.aspx

Figure 1: Florida Department of Law Enforcement Organizational Chart – Investigations and Forensic Sciences



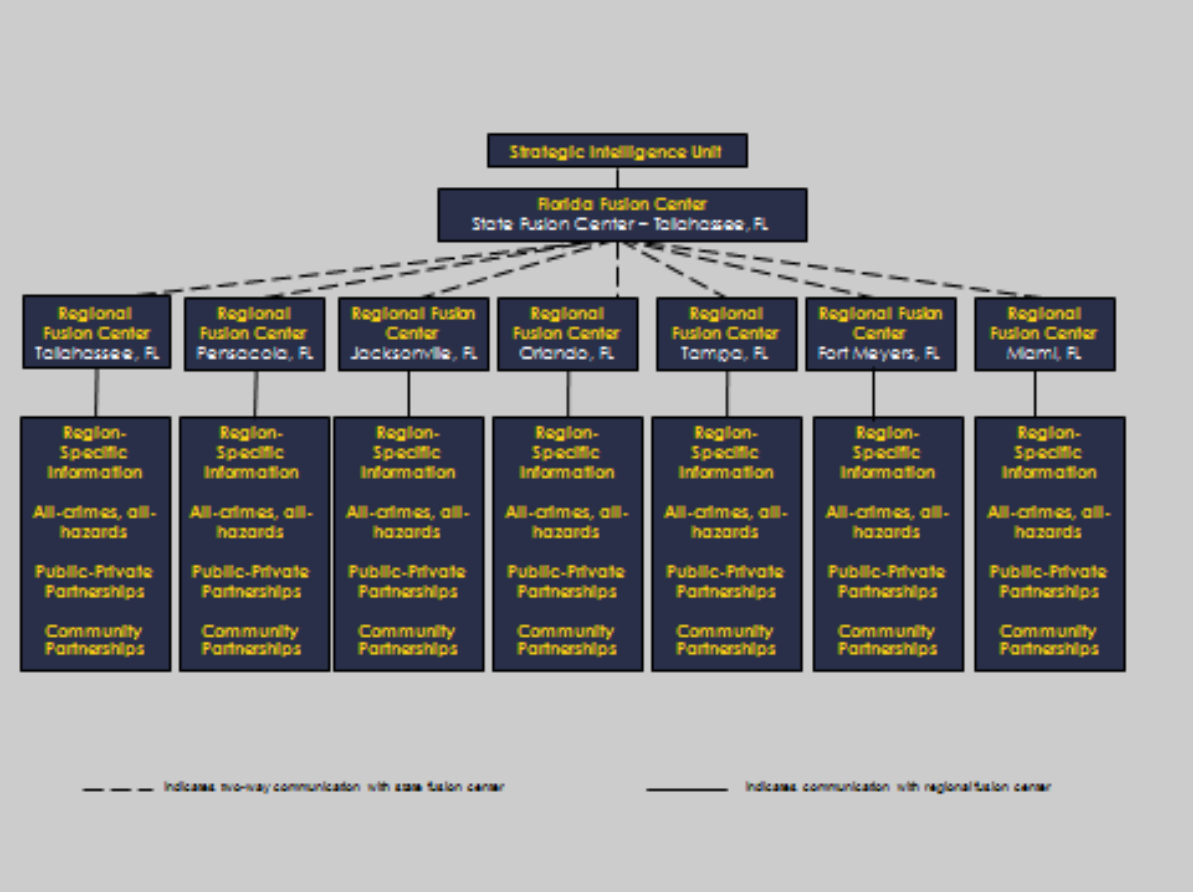
The OSI has had an all crimes approach since its inception that was reflective of FDLE's investigative strategy and focus areas. This approach was enhanced with the addition of a domestic security mission after the attacks of September 11th, 2001. Under the coordination of FDLE, seven regional domestic security task forces (RDSTFs) were created along with an

analytical unit within OSI to enhance domestic security and counter terrorism investigative efforts. Each task force is co-chaired by an FDLE Special Agent in Charge and a sheriff from the region. Beyond the RDSTFs, the OSI also contains strategic and operational focus teams that interact with and support regional intelligence centers as well as state, local, and federal agencies to monitor issues that could affect the state of Florida.

Seven Regional Fusion Centers

In 2007, FDLE conducted a gap analysis of the state of Florida's information sharing processes. The findings and recommendations from this gap analysis identified insufficient cooperation and information sharing with local law enforcement agencies within the state of Florida. While this gap analysis will be discussed in more depth to come, its importance to the information sharing structure of the state of Florida pertains to the creation of seven regional intelligence centers. An infrastructure and resources foundation for these regional intelligence centers had already been established in the seven critical regions of Florida with the RDSTFs and RIAs. Logistically, financially, and functionally it made sense to place the regional fusion centers in these same seven regions. The regional intelligence centers do not replace the existing RDSTFs or RIAs, they are separate entities that work along aside one another to enhance effectiveness across the board. Figure 2 illustrates the seven regional fusion centers and their relation to the state fusion center.

Figure 2: Florida Department of Law Enforcement - Regional Fusion Centers

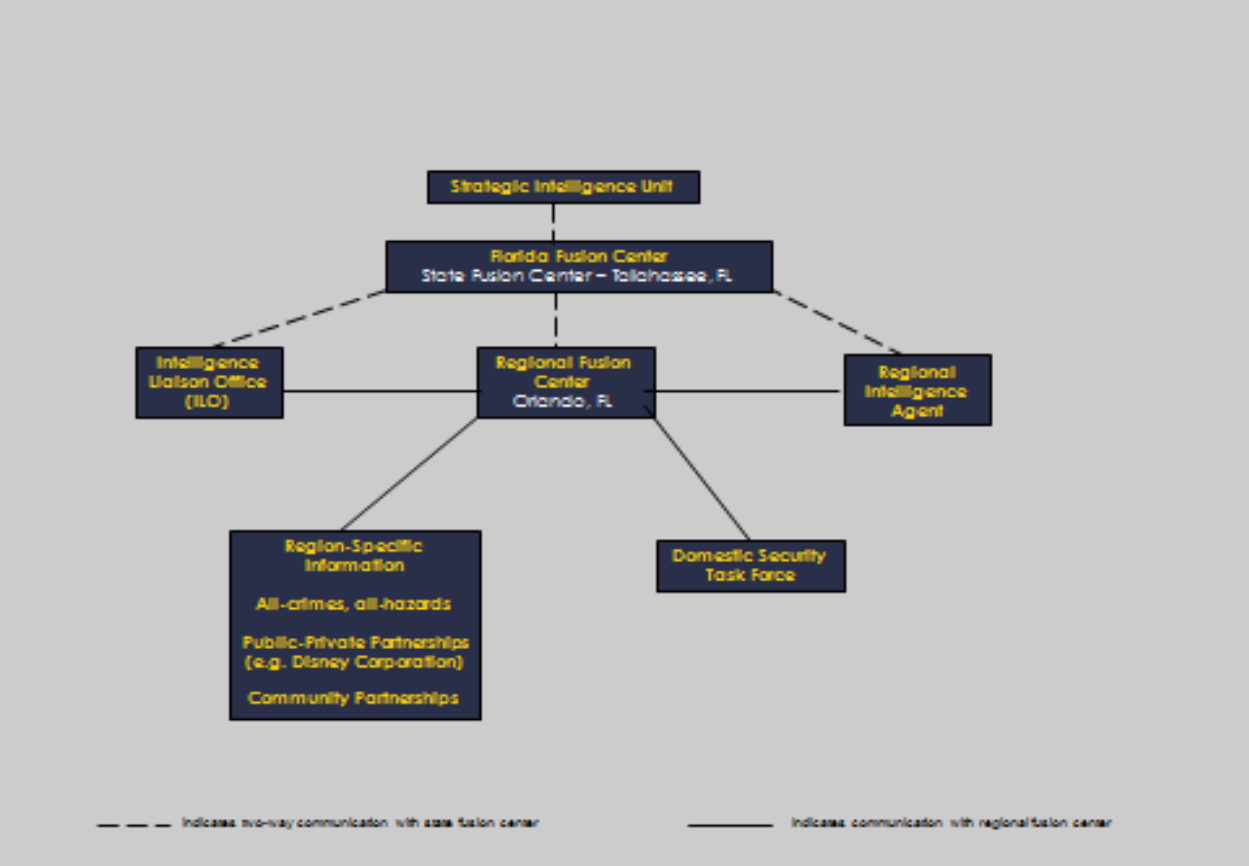


In March 2008, Florida Governor Charlie Crist designated the FFC to serve as Florida's primary fusion center. While the regional fusion centers are in the process of becoming operational, the FFC provides resource and instructional assistance. Regional fusion centers may provide operational support and situational awareness to local and state law enforcement agencies in their jurisdiction but only the FFC handles this function for the entire state. The FFC also has a 24/7 investigative support center for situational awareness and some after hours tactical support. It should be noted that while the primary state fusion center is in Tallahassee (the FFC) a regional fusion center is also located in Tallahassee. The RIAs serve as the primary communication mechanism between the FFC and regional centers. At the time of the site visit, the regional fusion centers in Miami Dade County and Orlando / Orange County were fully functioning with the other five centers becoming operational in the near future. The FFC has

begun to conduct quarterly meetings that include representatives (ILO's) from each of the regional fusion centers. Figure 3 illustrates the structure of the regional fusion centers and uses the Orlando center as an example. Each of the seven regional intelligence centers is structured in a similar fashion.

Information collection requirements and priorities are established through two-way communication between the FFC and regional centers. For purposes of protecting the state of Florida, the FFC establishes information collection requirements for the regional centers and requires information relative to the established requirements be pushed back to the FFC for further analysis and dissemination. For example, the FFC may have information relevant to a certain type of insurance fraud occurring throughout the state of Florida and pushes out requirements pertaining to these activities to the regional centers. Once the regional centers are aware of this emerging trend and identify information that may be relevant to the insurance fraud scheme, they push their intelligence products back to FFC for further analysis. Once all seven regions are functional they will begin pushing information back to FFC where it can be analyzed, the

Figure 3: Regional Fusion Center Structure – Orlando, FL Example



FFC can begin to create an entire state-wide picture of how insurance fraud is occurring in Florida and pushes this information back out to the seven regions for the officers and analysts to more accurately respond. Moreover, if information comes in from Miami on specific individuals involved with insurance fraud and this information matches closely or is specifically related to other information provided from another regional center, this information can be fused together and pushed back to each region to provide a more comprehensive understanding of the individuals and actions.

Beyond collecting information consistent with requirements established by the FFC, regional fusion centers are also tasked with the responsibility of collecting and analyzing region-specific information on all-crimes and all-hazards. Region-specific reports are then pushed on to

the FFC in order for the FFC to maintain a conscious awareness of crimes, individuals, and activities across the state of Florida as well as allocating necessary resources to specific regions when in need. Each regional center is responsible for establishing partnerships with the community and private sector within their respective region. For example, the FFC will not have an established formal partnership with the Disney Corporation directly – this would be the responsibility of the Orlando/Orange County regional fusion center. Information provided by or requested from Disney would be managed by the regional center and then pushed to the FFC in Tallahassee in the form of an intelligence product.

The Difference between the Florida Fusion Center and the Office of Statewide Intelligence

Once again, the OSI is responsible for providing intelligence products to FDLE executives to guide the planning and direction, analysis, reporting, and evaluation of FDLE operations. Even though all of the OSI assets support the FFC, the two entities have different missions. The OSI provides intelligence products to support FDLE cases and investigations – cases which are standard criminal investigations, especially those related to criminal enterprises. The FFC on rare occasions may lend support to FDLE cases; however the FFC mission is to provide strategic intelligence products related to terrorism, critical infrastructure and all-threats and all-hazards. This structure can be explained by FDLE's adherence to the Baseline Capabilities for State and Major Urban Area Fusion Centers (DHS, 2008). The guiding purpose of these baseline capabilities is fusion centers to establish operating procedures consistent with the Program Manager's Information Sharing Environment's (ISE) model.

According to the ISE model, fusion centers are responsible for terrorism, crimes that have terrorism nexus, and threats to critical infrastructure and key resources (GIWG, 2005). This ISE

context is the approach adopted by Florida to operate their fusion centers. From a functional perspective it is expected that there will be some investigation overlap between the OSI and FFC. This overlap is due to the fact that some crimes may or may not have a terrorism nexus and until the investigation can reach a sufficient point at which a terrorism nexus can be identified, both the OSI and FFC will continue to work the investigation simultaneously and in conjunction with one another. If the investigation indicates a terrorism nexus, the OSI will turn the investigation over completely to the FFC. Likewise, if the investigation indicates a lack of a terrorism nexus, the FFC will turn the investigation over completely to the OSI.

Information Sharing: Local Law Enforcement, Non-Law Enforcement Organizations, and Federal Agencies

Gap Analysis

As mentioned, in 2007 FDLE conducted a statewide assessment of their information sharing capabilities to identify gaps for improvement. The critical gap identified through this evaluation was the need for improvement in the relationship between the FFC and local law enforcement agencies; more specifically a gap in information collection provided via local agencies and local analyst products. Many of the local agencies tended to interpret intelligence-led policing as focused within their own agency (FFC, 2010a) as opposed to a broader philosophy of being part of the information sharing culture where locals think beyond jurisdictional boundaries. This is critical given the FFC's strong emphasis that for successful intelligence-led policing to occur, agencies must understand trans-jurisdictional responsibilities (FFC, 2010a). Less than optimal relationships with local law enforcement were not unanimous as FDLE experienced a variation across the regions with respect to these relationships. For

example, the FFC has a strong relationship with local law enforcement agencies in Pensacola developed though their collaborative experience managing natural disasters (hurricanes) and criminal investigations.

Relationships with local law enforcement seemed to hinge on two factors; 1) local agencies recognizing what information needed to be pushed to the FFC and, 2) a lack of awareness of what the FFC actually provides. This is not to say local agencies in Florida are opposed to developing consistent standards for information sharing, however, a gap existed with respect to understanding the intelligence-led policing philosophy and the resources available to assist them in achieving an operational intelligence capability. This lack of knowledge is coupled with a lack of commitment from local law enforcement executives. As mentioned by FFC personnel, the lack of support and buy-in at all levels of the organization is a key obstacle to effective information sharing. The sub-par commitment is not in the form of unwillingness to share information, but insufficient resources needed to meet the standards for information sharing outlined by the FFC that ensure quality, legality and effectiveness. Despite the identified gaps in communication with local agencies, many of them are involved in some form or fashion, be it having a formal ILO or simply an informal relationship to pass along information. In fact, information overload from local agencies is a challenge both in terms of the FFC managing this information but also communicating the importance to local law enforcement for the need to analyze and evaluate the information as it relates to their region. Similarly, the information overload issue arises as a result of needing a clearly defined dissemination strategy that has identified recipients and mechanisms are in place for appropriate two-way information flow.

In response to these concerns, the FFC recognizes the need to market their products and resources with local law enforcement to increase awareness of what the FFC can provide for

local law enforcement and vice versa. Currently this is being achieved through FFC personnel who meet continually with local law enforcement to provide region-specific information as well as keep them up to date on resources available to them through the FFC. The creation of the seven regional fusion centers is also at the heart of the solution to this issue. These regional centers are tasked with the responsibility of marketing their resources to local law enforcement within their region while developing and maintaining active information sharing channels. The seven regional centers build the grass-roots partnerships for two-way communication flow and the FFC relies upon these regional centers to provide information from the community-level. Although it was beyond the scope of this case study, it would be quite informative to study the variations in these regional centers and how those variations were developed and the positive and negative impacts they had on information sharing. This information flow allows the regional centers to identify region-specific or unique crime/hazard/terrorism trends and provide this information to the FFC in the form of an intelligence product that can be used to allocate resources to that region to respond to the identified needs. Moreover, the FFC can use this information to track crime/hazard/terrorism trends throughout the state of Florida and disseminate this information across the state and country.

Intelligence Liaison Officers (ILOs)

A critical component to the success of fusion centers across the country is the establishment of intelligence liaison officers (ILO). As noted earlier, over 50 percent of the SLT respondents indicated that the agency had a TLO or ILO program. An ILO is intended to be a communication channel of raw information from his or her agency/organization who can integrate that agency/organization-specific information into the collective body of information

for analysis. When the fusion center has intelligence requirements, the ILO is the communication channel back to the agency/organization to share, monitor, and process the new information needs (Carter, 2009). An ILO must ensure that analytic products and threat information are directed back to the parent agency for proper dissemination. The ILO's may be physically assigned to fusion centers, but a more common arrangement is for the ILO to perform his or her fusion center responsibilities simultaneously to those of their home agency/organization from that location.

The gap analysis conducted by FDLE in early 2007 identified the need to establish ILOs in the state of Florida. By December 2007, 12 state agencies formally committed to the FFC by signing memorandums of understanding (MOU) with FDLE to contribute members to serve on the Executive Advisory Board and to serve as ILOs to support FFC operations. All formal ILOs meet with FFC personnel each Wednesday of the week to maintain consistency of intelligence requirements and emerging issues. These ILOs represent multi-discipline partners from education, fire rescue, communications, law enforcement and emergency management. Below is a list of the agencies and entities which participate as ILOs in the FFC:

- Department of Agriculture
- Department of Business and Professional Regulation
- Department of Corrections
- Department of Education
- Division of Emergency Management
- Department of Environmental Protection
- Fish and Wildlife Conservation Commission
- Department of Financial Services
- Department of Health
- Department of Highway Safety
- Department of Transportation
- Office of the Attorney General
- National Guard
- Department of Homeland Security
- US Attorney's Office
- Federal Bureau of Investigation
- Drug Enforcement Administration
- Florida Chiefs of Police Association
- Florida Sheriffs Association
- Florida Fire Chiefs Association
- Agency for Enterprise Information Technology

To formally become an ILO with the FFC, agencies/organizations must enter into a MOU with FDLE. The MOU requires the ILO to recognize rules, regulations, and laws pertaining to

the disclosure of information as well as operating policies and procedures and performance expectations of FDLE/FFC. This MOU also requires a minimum time dedication of one ILO day per week. Additionally, ILOs must complete a background investigation, successfully obtain a secret-level security clearance (including civilian personnel), and complete a formal ILO training program set forth by the FDLE and the Fusion Executive Advisory Board. All FFC members (and FDLE members assigned to the FFC) must also complete these trainings requirements. These training requirements are supplemented by monthly training schedules that address emerging issues in information sharing – such as 28 CFR Part 23 reviews, information sharing systems and privacy concerns. Moreover, each ILO is responsible for an established benchmark for standard tasking that includes, but is not limited to: monthly encounters report (e.g. repeat offenders, traffic stops and tickets), review of their agency/organization databases[18], actively push information back to the FFC, and complete strategic assessments for monthly encounters.

Formal ILOs assigned to the FFC are expected to participate in a capacity deemed appropriate by the ILO's agency/organization and will have the ability to be virtually connected to the FFC via electronic information sharing systems. The intelligence system utilized by the FFC as well as other local, state and federal criminal justice agencies throughout Florida is known as the Statewide Intelligence Site - InSite. This system operates on the secure information portal administered by FDLE, the Criminal Justice Network (CJNet). InSite provides law enforcement agencies (federal, state and local) a secured computerized database of active criminal intelligence and active criminal investigative information to the legally authorized users across the state of Florida. The FDLE is responsible for system administration to include audits for both the use of CJNet and InSite. Access to the portal and the system

18 Florida Fusion Center personnel may ask for Intelligence Liaison Officers to run all the checks of their databases for persons which they are legally authorized to conduct. For example, a database search may identify a name from a terrorism watch list that also appears in the Department of Education or Public Health information systems.

requires MOUs, Agency Agreements and Individual User Agreements. All users of InSite are required to undergo additional background investigations and training before being granted access to the system. All agency executives and individual users of InSite must acknowledge in writing an adherence to the FFC Privacy Policy as well as all applicable federal or state laws. Individuals assigned to the FFC from agencies outside FDLE are also bound by the Non-Disclosure Agreement. Civilians may be provided access to the system on a case by case basis for those who have a need to know and a right to know the information contained within the system.

The ILOs not only provide additional terrorism information, but also enhance the all-hazards perspective adhered to by the FFC given their proximity to threats that can emerge outside of the traditional law enforcement purview. A unique example from the FFC of this all-threats approach was working with emergency management personnel for hurricane evacuation plans. Beyond the obvious threats posed by hurricanes, FDLE and emergency management planners has taken another step and are examining registered sex offenders living within the projected hurricane damage areas to determine an appropriate evacuation and contingent living options. Together, the FFC and emergency management personnel identified the increase of a potential threat involving registered sex offenders being evacuated during a hurricane and directed to shelters where there may be large numbers of children with minimal adult oversight – such as many schools that serve as evacuation shelters during hurricanes. As such, the FFC and emergency management personnel are working together to create appropriate hurricane evacuation plans for registered sex offenders living within high-impact hurricane areas in the state of Florida.

Threat Assessments, Intelligence Products, and Dissemination

Utilizing information and intelligence products received from other law enforcement agencies, fusion centers, and ILOs, the FFC has developed a comprehensive process for intelligence and information sharing in support of the completion of strategic assessments, criminal investigations and, as emphasized the most at the FFC, situational awareness. These processes are at the heart of the FFC function to plain and simply facilitate communication across organizations (FFC, 2010a). Within their first six months of operations, the FFC completed 12 strategic threat assessments and 53 requests for information. During 2009, approximately 250 intelligence assessments on subjects and topics of interest were produced.

As with any emerging initiative there has been improvement but issues still remain. For example, when the Super Bowl was held at Raymond James stadium in Tampa, FL in 2009, the FBI requested the FFC to conduct a threat assessment of possible threats, actors, targets, and methods that could impact the Super Bowl. Within this threat assessment, the FFC included a brief section on serious domestic threat groups in the Tampa area. Once the assessment was disseminated to the FBI it was decided this information should not be included in the final threat assessment for the Super Bowl given the FBI's threat prevention concerns were focused on international threat groups. Despite a significantly higher likelihood of potential attacks coming from domestic groups/crime, this information was not included in the threat assessment and thus resulted in a less comprehensive intelligence product for dissemination.

The FFC utilizes a "user-friendly, short and concise" (FFC, 2010a) format for their intelligence products and disseminates these products in multiple ways electronically. Intelligence products are posted to the Homeland Security Information Network Intelligence[19] (HSIN-Intel) website and Homeland Security State and Local Intelligence Community of

19 For more information visit https://government.hsin.gov/

Interest[20] (HS SLIC) website. Beyond these major Regional Information Sharing System websites, the FFC maintains an updated email distribution list for awareness products as well as an internal secure portal to share information with other law enforcement agencies on request. Moreover, the ILOs receive information on how to disseminate products during their ILO training program. However, maintaining a consistent and timely standard for disseminating intelligence products has its challenges. One primary obstacle faced by FFC personnel is that every 35-40 days the FFC's access to federal databases gets automatically deleted to particular system nodes. For example, HSIN has a variety of nodes that remove access on a regular basis for security purposes. After a couple of days the FFC's access is restored, but this becomes a routine inhibitor to information flow. Information sharing inhibitors are not only technical, but bureaucratic as well. The process of receiving timely products from federal agencies is an extremely complicated process due to the fact that there are so many layers of review and sign-off on intelligence products before they go out. This often results in stale information that is no longer applicable to current situations.

Relationships with the Private Sector

The importance of establishing public-private partnerships with fusion centers is reiterated in a variety of reports and recommendations. The extent of participation and format of these partnerships can vary greatly across fusion centers nationally. The approach taken by the FFC is unique given the structure of the information sharing system in the state of Florida. To begin with, active information sharing with the private sector occurs both at the state and regional fusion center levels. At the state level, the FFC administers a website specifically designed to facilitate information exchange with private sector entities. "Business Safe" is a

[20] For more information visit https://hsin-intel.dhs.gov/

program that includes an outreach program and website to the private sector. BusinesSafe is designed to involve local businesses in protecting the safety and well-being of Florida's residents and visitors from threats – both man-made and natural. Florida's seven RDSTFs have launched BusinesSafe to provide businesses with the necessary tools and resources to facilitate two-way communication with the regional fusion centers. BusinesSafe provides sector specific fact sheets for businesses to reference[21]. These sheets are categorized by the type of business and are patterned after a program that was created by the New York City Police Department after the attacks of September 11th – the NYPD Shield initiative[22]. More specifically, the information provided via BusinessSafe is designed to help local businesses identify suspicious activities which may result in a threat to those businesses. Private sector members can also sign up to receive electronic alert notifications via e-mail, cellular phones, and PDAs. These notices provide information about breaking news, possible threats, suspicious activity and specific preparedness techniques pertinent to the local businesses. Currently there are approximately 4,000 local businesses in the state of Florida connected to BusinessSafe (FFC, 2010a).

Additionally, businesses are able to register with a US Department of Homeland Security website[23] which provides vital information on how to better protect their business from threats. To register for this secure website, private sector members must apply via the website and identify their regional protective security advisor (PSA). The regional PSAs are representatives from the RDSTFs[24]. Beyond the US Department of Homeland Security secure website, local businesses may also register to become a member of multiple other websites designed for sharing

[21] For a list of specific sectors and fact sheets visit: http://www.fdle.state.fl.us/Content/getdoc/77cd6c85-8eed-4888-855c-715de12dcaef/Sectors-Key-Resource-Areas-(1).aspx
[22] For more information visit http://www.nypdshield.org/public/
[23] For more information visit http://cvpipm.iac.anl.gov/
[24] For more information visit: http://www.fdle.state.fl.us/Content/getdoc/5a336d9b-cf38-4979-bd03-d9bfe0f52738/DHS_Protective_Security_Advisor.aspx

threat information[25] – all of these websites can be reached via the BusinessSafe website. For example, the website "Business Owners Against Terrorism" (BOAT) provides local business owners connectivity with the North Florida Regional Domestic Security Task Force. The BOAT website allows business owners, managers or employees to anonymously report suspicious behavior or activities to local law enforcement authorities.

Consistent with the approach that local business must identify their protective security advisor – the representative from the RDSTF – to gain access to secure websites, regional fusion centers are responsible for establishing and sustaining active two-way information flow with the private sector within their region. The state fusion center (FFC) does not maintain partnerships with private sector companies – only the BusinessSafe website. The FFC relies upon the regional intelligence centers for these partnerships. The regional fusion center personnel push intelligence products from the private companies in their region to the FFC for further review and integration into other intelligence products. If additional information is needed from a private organization, the FFC will communicate with the regional center where the business is located and the regional fusion center will then reach out to the business where information is sought.

Intelligence Analysts: Performance Evaluation and Standards

Analysts at the Florida Department of Law Enforcement

Law enforcement intelligence is reliant upon the analysis of raw information and thus, intelligence analysts. The FDLE and the FFC are sensitive to the importance of quality intelligence products. The FDLE defines a law enforcement analyst as "any person who is

[25] To view a list of additional private sector sharing websites visit: http://www.fdle.state.fl.us/Content/getdoc/b46536cc-bd2d-4008-8023-4d27f427da63/Related-Links.aspx

employed or contract by a municipality, state or political subdivision thereof whose primary responsibility is to collect, analyze and disseminate data in the form of operational, strategic, investigative, intelligence and crime analysis to support, enhance and direct law enforcement missions (FFC, 2010a). When asked what character traits FDLE looks for in an intelligence analyst, the FFC personnel indicated the importance of credibility, excellent written and oral communication skills and the ability to think critically. Moreover, FDLE believes analysts are not just people who sit behind a desk and operate computer software, but have a genuine ability to reach out to others and be proactive about the case they are working on and how it may relate to other cases they are aware of but might not be assigned (FFC, 2010a).

Despite hiring analysts with these characteristics, FDLE is cognizant of the need for professional standards to train and evaluate analysts in order to achieve quality intelligence products. A critical issue facing FDLE and the FFC is that the regional fusion center structure presents challenges with respect to how to coordinate and ensure the quality of intelligence products throughout state. This challenge of coordination and quality control is the result of some of the regional fusion centers were developed by local agencies that are currently being incorporated into a state-wide regional structure. Moreover, regional fusion centers operate, for the most part, separate from the FFC and even though the FFC provides an FDLE analyst in all regional fusion centers, FDLE will not dictate to the regional centers.

Analyst Training

One way of addressing the analyst quality and standards challenge is through the development of a required analyst training academy. In 2003, the Florida Department of Law Enforcement developed the Florida Law Enforcement Analyst Academy (FLEAA). This

academy was the first of its kind in the nation. Analysts learn criminal and intelligence analysis skills that are used by law enforcement and other emergency responders to successfully prevent crime and conduct complex investigations. The FDLE's long-term goal in creating the FLEAA was to establish and provide a uniform training curriculum in the area of criminal intelligence and law enforcement analysis. During this six-week academy, analysts are challenged with hands-on training, assignments and weekly quizzes. They develop the skills necessary to complete individual and group research projects. Following the completion of all course work, analysts take a comprehensive examination. Successful graduates receive a state certification as a law enforcement analyst. The FLEAA is traditionally offered twice a year. To better prepare analysts for the academy, FDLE also developed two pre-requisite courses. The first is a 40-hour Florida Basic Analyst Training (FBAT) course. This course is designed to train newly and recently hired analysts in the field of law enforcement analysis. The course offers instruction blocks that lay the groundwork for their career in criminal or intelligence analysis. There is a very high demand for this course and it is traditionally offered two to four times a year.

During 2005, FDLE developed a new course titled "Computer Applications and Analytical Techniques" which is also a 40-hour course designed to train analysts in using computer applications to conduct investigative analysis. Once again there is a very high demand for this course as well and it is traditionally offered two to four times a year. The basic and computer courses serve as training "stepping stones" and are required to be completed prior to attendance in the FLEAA. Currently, other acceptable prerequisites are being considered. The FDLE has been planning the launch of an advanced course since fall 2005. This course will fill an existing void between the basic course and the FLEAA. The intent is for this training to concentrate on the applications and techniques taught in the basic course and allow for more

hands-on advanced investigative analysis. The advanced course is delivered to analyst academy graduates and will focus on emerging topics of concern in criminal intelligence analysis – such as fusion centers, suspicious activity reporting and intelligence-led policing.

Currently, the FDLE training program is funded through Law Enforcement Terrorism Prevention Program funds issued from the Department of Homeland Security. Students attending these courses must be assigned to an analyst position with a local or state law enforcement agency in the state of Florida. This funding allows FDLE to offers the FLEAA training courses free of charge to all state, county and municipal law enforcement and investigative agencies.

Analyst Performance Evaluation and Analyst Promotion

To reinforce and maintain consistent quality among intelligence analysts, FDLE has employed the use of both qualitative and quantitative methods for analyst performance evaluations. To begin with, the entry-level analyst at FDLE is a "Crime Intelligence Analyst I" (CIA I). The position of CIA I can be attained following the successful completion of all the applicable application/selection processes which includes approved exercises and interviews, as well as meeting the minimum qualifications for the position. Prior to the expiration of the CIA I probationary period, the analyst must successfully complete the 40 hour FBAT and the 40 hour "Computer Applications and Analytical Techniques" course. The next analyst level at FDLE is a "Crime Intelligence Analyst II" (CIA II). A CIA I may be upgraded to a CIA II upon attaining one year of analytical experience and successfully completing the aforementioned training requirements. Any promotion from the position of CIA I to CIA II is be contingent upon the satisfactory completion of all probationary requirements, a minimum rating overall of

"Achieves"[26] on the analyst's work plan and the recommendation of the analyst's supervisor and approval via the analyst's chain of command to the Special Agent in Charge or equivalent.

The next progression for analysts at FDLE is to become a "Certified Crime Intelligence Analyst" (GA I). A CIA II may be promoted to a GA I upon attaining two years of analytical experience as a CIA II with the FDLE and successfully completing the FLEAA. The final progression for analysts at FDLE is to become a "Senior Crime Intelligence Analyst" (GA II). A GA I may be promoted to a GA II upon attaining five years of analytical experience as a GA I as well as becoming a certified analyst instructor; successfully complete an additional 40 hours of advanced analyst training; maintaining membership and active participation in a professional organization, which is pertinent to the analyst's job assignment and approved by the member's supervisor, and lastly maintaining a minimum rating of "Achieves" on the analyst assignments. Upon becoming a GA II, the analyst will have additional responsibilities that include, but are not limited to: assisting in the development and approval of curriculum for all course work in the FLEAA; assisting in the development and monitoring testing processes within the FLEAA; and administering proficiency exams for CIA candidates and FLEAA candidates.

In addition to the minimum requirements of evaluation for career progression, FDLE goes beyond evaluating their analysts at pre-determined intervals. Analyst products are not only reviewed when they are tested for the progression of their skills, but also on a day-to-day basis as senior personnel examine daily intelligence products and investigative support work. If an analyst's quality of work is thought to be less than sufficient, the inadequate product is returned to the analyst with comments and a follow-up discussion from senior personnel on the areas for improvement. The FDLE emphasizes the importance of quality over quantity (FFC, 2010a).

[26] Analysts receive one of three evaluations of their intelligence products as related to FDLE's benchmark for quality analysis; "Excels", "Achieves", and "Below"

Protecting Citizens' Civil Rights

As many fusion centers across the country have come under public scrutiny for information sharing practices, whether legitimate or not, the FFC emphasizes transparency with respect to their operations. The FFC has a vigorous privacy policy which is open for public review and posted to the FDLE public website[27]. As explained in the FFC privacy policy document, the intent of the FFC is to:

> "The Florida Fusion Center (FFC) is committed to the responsible and legal compilation and utilization of criminal investigative and criminal intelligence information and other information important to protecting the safety and security of the people, facilities, and resources of the State of Florida and the United States. All compilation, utilization, and dissemination of information by FFC participants and source agencies will conform to requirements of applicable state and federal laws, regulations and rules, and to the greatest extent practicable be consistent with Fair Information Practices. The intent of this policy is to abide by all privacy, civil rights and civil liberties guidance issued as part of the Intelligence Reform and Terrorism Prevention Act of 2004, National Fusion Center Guidelines, State and Major Urban Area Fusion Center Baseline Capabilities and the National SAR Initiative. All local, state, tribal and federal agencies providing suspicious activity reports (SAR) with a nexus to Florida or participating with the Florida Fusion Center (FFC) by virtue of submitting, receiving or disseminating SAR information, criminal intelligence or criminal investigative information via the FFC are required to adhere to the requirements of the Florida Fusion Center Privacy Policy" (FFC, 2010b:3).

All members of the FFC are required to review, acknowledge and adhere to the FFC Privacy Policy. All participants and source agencies, which include all individual users of the InSite system, are required to review and adhere to the FFC privacy policy. The FFC provides a printed copy of their policy upon request to all entities participating in the FFC and InSite and requires a written acknowledgement to comply with this policy and the provisions it contains. All FFC personnel, participating agency members, personnel providing information technology services to the agency, private contractors, InSite users and any other information sharing partner

[27] http://www.fdle.state.fl.us/Content/Florida-Fusion-Center/Menu/Privacy-Policy.aspx

is required to comply with applicable laws protecting privacy, civil rights, and civil liberties. The FFC has adopted internal operating policies and procedures that are in compliance with applicable laws and regulations protecting privacy, civil rights, and civil liberties including but not limited to, the U.S. Constitution and state, local, and federal privacy, civil rights, civil liberties, and legal requirements applicable to the FFC. Florida State Statutes 119[28] – Public Records - is one applicable law pertaining to the criminal intelligence and criminal investigative efforts of the FFC and participating agencies. In order to maintain consistency and adherence of the privacy policy by all actors involved, the FFC has created an internal Standing Privacy Review Board that actively reviews information sharing policies.

A very unique aspect of the FFC in response to a heightened suspicion of fusion center activities with respect to civil rights issues is that the Director of the FFC receives guidance from a Constitutional Protections and Privacy Advisory Board (CPPAB) that collaborates with community privacy advocacy groups to ensure that privacy and civil rights are appropriately protected by the FFC's information acquisition, dissemination and retention practices as defined by the FFC's written policy. The CPPAB is comprised of three members not actively associated or employed by an FFC participating agency. The members are individuals with well established credentials in the fields of criminal justice and/or the law. Currently the CPPAB members are comprised of an ACLU Director from the state of Florida, a retired Special Agent in Charge with the Federal Bureau of Investigation, and the Director of the Center for Advancement of Human Rights at Florida State University. The members are appointed by the FFC Executive Advisory Board to serve for at least two years. The CPPAB will periodically review and recommend to the FFC Executive Advisory Board updates or changes to the FFC's policy and procedures for

[28] For more information visit http://www.leg.state.fl.us/Statutes/index.cfm?App_mode=Display_Statute&URL=Ch0119/ch0119.htm

protecting civil rights and civil liberties in response to changes in applicable laws, or as otherwise necessary. The CPPAB may be consulted to participate in any independent inquiry into complaints alleging violation of the privacy rights policy and will advise the FFC Executive Advisory Board of their findings and any recommended corrective action.

Conclusions

This overview of the administration and operation of the Florida Fusion Center has provided the necessary context for issues discussed earlier as well as provide some indication of best practices regarding building an intelligence capacity. While fusion centers differ from most other state, local, and tribal agencies, their role in the intelligence/information sharing process gives light to the facilitators and inhibitors of information sharing at the local level.

Perhaps the best illustration of information sharing and intelligence-led policing that can be extracted from this case study is the process and communication channels established throughout the structure of Florida's intelligence system. In the context of an individual agency at the local level, establishing communication channels for information sharing would essentially involve that agency to develop a process to manage collection requirements, develop partnerships with the private sector, and partnerships with the community. These steps represent the information collection infrastructure of police agencies that allow an agency to maintain the "pulse" of their community while also allowing for two-way communication of raw information. While this form of infrastructure aids the single agency is applying ILP to their specific needs, this also allows the single agency to engage in information sharing across jurisdictions and report on the types of trends and threats they feel are relevant. Such a process also allows for information to be pushed on to state fusion centers. This model is consistent with that of

Florida's state fusion center and its seven regional fusion centers. Simply put, each regional fusion center acts independent and is responsible for their regional issues – just as independent local agencies would be responsible for their jurisdiction and report to the state fusion center or to other agencies seeking information they might feel is useful.

The FFC adheres to an "all threats, all hazards" philosophy intended to prevent threats from reaching fruition. "Threats" is an all-encompassing term which refers to street crime, complex criminality, terrorism, and natural disasters. In short, the goal of this philosophy is to not only remain cognizant of traditional threats, but threats that have been outside the traditional law enforcement purview. Such a philosophy requires a variety of information sources and communication channels. The FFC has established sources consistent with this information collection environment that include public-private partnerships with Disney and "BusinessSafe". Moreover, the "BusinessSafe" portal allows for the submission of suspicious activity reports (SARs) – a threat-based source of behavioral information endorsed by practitioners. In addition, the importance of trans-jurisdictional information gathering and sharing was reinforced as a necessary function of intelligence-led policing. Once again, the philosophy of information being collected and for purposes of focusing on threats across jurisdictions – not just the jurisdiction in which an agency is located.

From an organizational structure perspective, all intelligence (and crime) analysts were civilian (non-sworn) personnel. An obvious caveat to the civilianization of the FFC as compared to local agencies is that it can logically be assumed that civilian employees within an intelligence-specific agency will be responsible for intelligence-specific tasks whereas civilian employees within a general local agencies may be tasked with responsibilities other than intelligence – thus clouding the effect of civilianization on ILP within local agencies. The FFC

relies on many formal policies and procedures to guide their intelligence practices – thus being high in formalization. Perhaps the best example of formalization is the memorandum of understanding (MOU) that is required by agencies/organizations that formally partner with the FFC. This MOU guides requirements for information sharing, collection, retention, and dedication of personnel and resources.

The influence of organizational context presented itself when the gap analysis indicated a significant lack of administrative commitment to the ILP philosophy as well as a requirement for comprehensive training on intelligence-related issues. It was noted by FFC personnel that the lack of support and buy-in at all levels of the organization is a key obstacle to effective information sharing. It is also worth noting that insufficient commitment is not in the form of unwillingness to share information, but insufficient resources needed to meet the standards for information sharing outlined by the FFC – most likely a result of no executive buy-in. Training is greatly valued and required within the Florida intelligence system. While all intelligence-related personnel are required to receive training on intelligence issues, analysts receive the most comprehensive training. This aspect of the FFC is also related to the importance of quality performance evaluation. Executives of the FFC acknowledge the importance of quality intelligence products to guide decision making. In order for quality products to be made available, analysts that create the products must be trained consistent with professional standards and expectations. Moreover, beyond the exhaustive training requirements, analysts are evaluated on the quality of their products – not the number of products. The quality of products is determined by senior intelligence analysts in the form of a blind-review. If an apparent decrease in quality is observed, the analyst can be required to attend further training programs.

The Florida Fusion Center identified a significant lack of understanding as to the concept of intelligence-led policing among local law enforcement agencies across the state of Florida. The ambiguity of ILP is one of the largest hurdles of adoption and research. This lack of understanding further demonstrates the need for additional research on law enforcement intelligence practices.

Chapter 7: Case Study #3: Southern Nevada Counter-Terrorism Center

This chapter provides a case study from the Southern Nevada Counter-Terrorism Center (SNCTC) as a means to build on the concepts discussed and to provide additional context for the conceptualizations and empirical findings of the present study. The SNCTC has a somewhat different structure for carrying out its mission. Furthermore, the SNCTC is designed to facilitate information sharing across a much different geographic and demographic area as compared to the FFC and MIOC. For example, the SNCTC is largely focused on activities within Clark County – specifically the city of Las Vegas, NV and the tourism/hospitality industry whereas the FFC is designed to manage multiple large cities, a large, spread-out geographic area, as well as a large tourism base. These different structures provide another unique insight into an intelligence-specific organization.

The Southern Nevada Counter-Terrorism Center

Housed in a 24,000 square-foot, non-descript airport office park, the SNCTC became operational on October 1, 2007. On March 18, 2009, Las Vegas Metro Police Sheriff Doug Gillespie testified before the U.S. House of Representatives Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment during a session titled "Homeland Security Intelligence: Its Relevance and Limitations" (HCHS, 2009). During his testimony, Sheriff Gillespie stated that the Las Vegas Metro Police Department and the SNCTC were committed to the key components of an effective fusion center – intelligence-led policing and an "all-threat, all-hazards" mission. Sheriff Gillespie explained that the Las Vegas Metropolitan Police Department employs the intelligence-led policing philosophy and that analysis of crime data,

coupled with the execution of innovative policing tactics, is the cornerstone of their efforts to successfully prevent risks to society.

All-Threats, All-Crimes Approach to Fusion Centers

Despite the name of the SNCTC as a “counter-terrorism center”, Sheriff Gillespie explained that the SNCTC could be more effective by taking a more broad "all-crimes, all-hazards" focus since law enforcement does not want to miss out on the criminal element that eventually turns out to be a terrorist. The SNCTC‘s core mission is to provide tactical and strategic analytic support to regional stakeholders. The tactical analysis section provides timely and actionable information to command staff and field personnel. The strategic analysis section complements tactical operations by developing long-term analytical products. Specific units exist to target gangs, counter terrorism, and narcotics as well a criminal analysts section to produce a variety of issue-specific products on issues facing the Clark County region. The SNCTC has established strong relationships with local industry, the public health community, and emergency management agencies to further enhance this approach.

Awareness training is provided to private sector businesses on how to identify and report suspicious behavior. Co-located with the analysts, the SNCTC houses a 24/7 watch station capability, investigators that handle tips, leads and suspicious activity reports, critical infrastructure protection group, and the All Hazards Regional Multi Agency Operations and Response (ARMOR) unit. This ARMOR team consists of local, county, state and federal experts in chemical, biological, radiological, nuclear, and explosive (CBRNE) response, detection, and identification. The SNCTC has developed a privacy policy that is founded on 28 CFR Part 23.

Mission

The mission of the SNCTC is to improve communication and coordination among international, federal, state, local, tribal, and private agencies. This mission is achieved through the combining of relevant information from disparate databases concerning terrorism, critical infrastructure, and raw information pushed from the community. The SNCTC is the regional hub for receiving information, providing analysis and dissemination of actionable intelligence to the participating agencies, Joint Terrorism Task Force (JTTF), All Regional Multi-Agency Operations and Response (ARMOR), and other appropriate law enforcement, public safety and intelligence entities. The SNCTC produces written reports concerning criminal trends and threat assessments in the Southern Nevada region and provides analytical case support and tailored analytical products.

Management and Structure

The SNCTC defines a "member agency" as an agency that contributes at least one full-time employee or one full-time contractor that is co-located at the SNCTC site dedicated to fulfilling the SNCTC's mission. A "contributing agency" is defined as an agency that contributes personnel on a part-time or surge (as needed) basis. Any local, state, or federal agency with statutory law enforcement, public safety, or public health jurisdiction may join the SNCTC upon approval by the board of governors. In general, all agencies that have invested in the SNCTC are referred to as "participating agencies". Each of these participating agencies must agree upon and enter into a memorandum of understanding (MOU) with the SNCTC that outlines responsibilities and commitments to the center. On the average work day, the SNCTC houses 60 employees from various agencies and organizations.

Board of Governors

The SNCTC is overseen by a board of governors comprised of agency executives, who all have equal voting rights, from each of the participating agencies. The chairperson of the board of governors is the executive of the agency that is designated as the fiscal agent for the SNCTC –which is currently the Las Vegas Metro Police Department. The board of governors, which convenes as a whole twice a year, provides mission guidance and policy direction. Additionally, they resolve conflicts or disputes that might arise related to policies or the mission. The board of governors appoints the executive director for the SNCTC who has day-to-day command authority over members assigned to the center. As staffing patterns change and full-time employees are added, contributing agencies may change their status to become member agencies. Each agency executive - who sits on the board - must possess, or be eligible and apply for a minimum security clearance at the level of "secret."

Collections Section

The deputy director of collection leads the collections section, which is responsible for the collection of hazard, threat, and suspicious activity information from a wide variety of sources and the distribution of the finished analytic products to the appropriate customers. There are two groups that comprise the collections section: the collection management group and the operations group - each supervised by a first line supervisor. The primary function of the collection management group (CMG) is to ensure that the SNCTC has a constant, robust situational awareness of all threats, hazards and crimes occurring in Clark County and the state of Nevada. The CMG also coordinates all matters associated with the terrorism liaison officer

program (TLO), and is responsible for the content and implementation of the SNCTC website and SAR programs. The operations group (OG) is responsible for the development of information sources, and the lawful collection of this source information. The OG is also responsible for the investigation and follow-up of suspicious activity reports, and other tips and leads. On occasion the OG is called upon to provide dignitary protection liaison for U.S Secret Service protection details, and other high-level dignitaries.

Analysis Section

The deputy director of analysis leads the analysis section and is responsible for the collation, synthesis, analysis, and production to meet the intelligence needs identified by the requirements committee (to be discussed subsequently), or any ad hoc intelligence need established by the SNCTC. The analysis section consists of two distinct, but inter-related groups: crime analysis group and counter-terrorism analysis group. Personnel assigned to the crime analysis group are responsible for strategic, operational and, tactical crime analysis, fulfilling the crime analysis requirements established by the requirements committee. The counter-terrorism analysis group is responsible for the analysis of terrorism threat information, and the production of situational awareness, threat assessment, strategic, and tactical analytical products, also meeting the requirements established by the requirements committee.

Intelligence Requirements Committee

As stated by a SNCTC executive, intelligence-led policing is fueled by intelligence requirements (SNCTC, 2010). The most significant approach taken to identifying intelligence requirements for the SNCTC is the creation of a requirements committee. The purpose of this

committee is to establish the information, intelligence and production requirements of the SNCTC and to establish the priority in which these requirements are addressed by personnel assigned to the SNCTC. Moreover this committee is responsible for ensuring that agencies receive the intelligence products that meet their needs – whether these products are related to organized crime, motorcycle gangs, or terrorism. Requirements for information collection fall into three categories;

1) Ad hoc requirements (highest priority, information related to a wide-range of possible emerging threats).
2) Priority requirements (information related to an identified, time-sensitive threat).
3) Standing requirements (information related to an identified, on-going threat).

This intelligence requirements committee is comprised of command-level managers, who are responsible for designing, approving and/or implementing initiatives, and who possess decision-making authority for their employing agency. Personnel who are assigned to the SNCTC are not permitted to be members of the committee in order to reduce potential conflicts of interest. In general, the positive outcomes of this committee are wide-ranging. Though more specifically, the result of the inclusion of the requirements committee into the business process of the SNCTC is better coordination of the human and technological resources available to the participating agencies of the SNCTC. Arguably the most important outcome of this committee is the assurance that the intelligence needs of each of the participating agencies are met. Also, with improved communication on the daily activities of the SNCTC, the partner agencies will realize a greater return on their personnel investment.

The requirements committee is responsible for providing four necessary outputs. The first, standing intelligence needs, are semi-permanent and enduring information and intelligence

needs that will change very little over time. Examples of this need are the weekly LVMPD action reports and analysis of every terrorist attack on a hotel or tourist destination. Second are the priority information needs that are requests for information or intelligence that are assessed and determined by the requirements committee to have a high priority. Third are the top priority information needs which occur during times of crisis or emergency and require immediate attention, and the suspension of work focused on standing and/or priority information needs. Lastly, a matrix of priorities, comprised by the committee, reflecting the priorities assigned to each standing or priority information need. SNCTC executives use this matrix as a guide in prioritizing and allocating work to SNCTC personnel.

From a procedural perspective, the requirements committee meets on the second and fourth Wednesdays of every month at the SNCTC. The executive director of the SNCTC is responsible for facilitating the meeting, and provides the committee with updates relative to the progress made towards completing each of the existing requirements. Each member of the committee is responsible for preparing to briefly summarize any initiative or action that resulted from a completed requirement. This type of feedback ensures that the intelligence and information needs of the participating agencies are being met by the SNCTC as well as ensuring that the requests for intelligence align with intended actions.

Quality Assurance Section

The deputy director of quality assurance leads the quality assurance section that is comprised of three groups. The first is the security group that is responsible for the operational and physical security of the SNCTC and all classified environments, the maintenance of all access and alarm systems, and the proofs of compliance for all security matters. This group is

also the single point of contact for all applications for security clearances, and maintains a roster of security clearances including dates for renewal investigations. Second is the privacy protection group that is responsible for ensuring that the SNCTC adheres to all pertinent laws, rules, and regulations relating to the protection of personal privacy and civil liberties. This group is also responsible for implementing the program and systems necessary - through training personnel - to provide regular and periodic audits to ensure compliance and provide proofs of compliance for all SNCTC investigations and intelligence products. Last is the performance measurement group tasked to develop and collect the data to measure the ability of the SNCTC to perform its established mission. Furthermore, this group seeks to determine if the work accomplished by the SNCTC aligns with the intelligence requirements set forth by the requirements committee.

Direction of SNCTC and Resource Control

Oversight and specific control over an agency's SNCTC resources and the continued dedication of resources to the SNCTC is retained by the participating agency - which are kept fully informed of all analytical developments by its respective subordinates, as appropriate security clearances permit. Salaries of the SNCTC personnel are paid by their respective agencies. LVMPD, as the fiscal agent, provides office space, equipment, and supplies to carry out the administrative operation of the SNCTC. Once the original seed money from federal and/or state grant funding is no longer available, sustainment for the SNCTC will be the responsibility of all participating agencies. This includes any additional equipment required by a participating agency and will be the responsibility of that agency to supply. Any and all expenditures by each participating agency are subject to the home agency's budgetary processes

and to the availability of funds and resources pursuant to applicable laws, regulations, and policies. When entering into a memorandum of understanding with the SNCTC, agencies expressly acknowledge that the language in the agreement no way implies that Congress or the Federal government will appropriate funds for such expenditures.

Supervision of SNCTC

Day-to-day supervision of matters assigned to the SNCTC is the responsibility of the LVMPD. Analysts are assigned based upon subject matter expertise and serve the entire southern Nevada region. As additional analytical resources become available, supervisory personnel from other member agencies are added. Each participating agency is subject to the personnel rules, regulations, laws and policies applicable to their respective agencies and abides by appropriate security agreements concerning the handling of classified and sensitive material. If a complaint made against any SNCTC member, while acting within the scope of their SNCTC assignment, they are reported to the SNCTC director. The executive director reports the complaint to the board of governors and the respective agency's direct supervisor of the SNCTC member under complaint. The executive (from the board of governors) of the complaint member's agency is responsible to conduct an investigation with assistance of the SNCTC executive director.

The SNCTC initially consisted of a combined body of the LVMPD supervisory and management staff, analysts, and support personnel, together with agents, analysts and support personnel assigned from the participating agencies. The MOU utilized by the SNCTC establishes and outlines the intent of the participating agencies to centralize and co-locate. This fusion is intended to provide resources, expertise, and information to maximize their ability to

detect, prevent, investigate, and respond to all crimes and all hazards in the greater Clark County, southern Nevada region. The benefits of collaboration and communication between the contributing agencies are readily apparent and widely recognized as absolutely essential. Further, the MOU established a framework for the organization of the SNCTC and to address issues that are common to the participating agencies. The MOU is to set out a common understanding of the policies and procedures that the SNCTC follows, in providing intelligence and coordination of service to the citizens encompassed by the populated areas of southern Nevada.

Analyst Environment

Analyst personnel at the SNCTC are comprised of a senior analyst to oversee all analytic functions, a private sector-specific analyst (to be discussed forthcoming), and four full-time analysts - both crime and intelligence analysts. Crime analysts are responsible for providing tactical and/or operational assessments to decision makers whereas intelligence analysts are responsible for providing case and/or strategic products. The analyst room is physically structured in the form of a "news room" with cubicle walls that stand only a few feet tall. This physical layout is to enhance awareness of each analyst's work in that each analyst will be in an environment where they will over-hear other analysts talking about cases or queries that they may also have information on and a connection can be made. This approach is consistent with the idea of eliminating barriers (such as bureaucracy) for more direct communication and thus, more effective information sharing.

Law Enforcement and Public-Sector Partnerships

The SNCTC has participating agencies from the public sector that go beyond the traditional law enforcement arena. Maintaining the "all-threats, all hazards" approach to intelligence, the SNCTC has engaged in partnerships with emergency response/preparedness agencies, local public schools, and federal law enforcement agencies. At the time of the case study, the SNCTC has received formal partnerships from the following public sector agencies and organizations:

- Las Vegas Metropolitan Police Department (LVMPD)
- Federal Bureau of Investigation (FBI)
- Henderson Police Department (HPD)
- North Las Vegas Police Department (NLVPD)
- Clark County School District Police Department (CCSDPD)
- Clark County Fire Department (CCFD)
- Las Vegas Fire & Rescue Department (LVFR)
- Nevada Department of Public Safety (NDPS)
- United States Federal Air Marshals Service (FAMS)
- United States Transportation Security Administration (TSA)
- Las Vegas Convention and Visitors Authority (LVCVA)
- City of Las Vegas Department of Law Enforcement and Detention (LVDLED)
- Southern Nevada Health District (SNHD)
- North Las Vegas Fire Department (NLVFD)
- Nevada High Intensity Drug Trafficking Area (NV HIDTA)
- Clark County District Attorney (CCDA)

Partnerships with the Private Sector – Suspicious Activity Reporting

One of the SNCTC's greatest strength is the ability to collect SARs from the community and private sector. Even though there is a constant need to improve SAR education and awareness for identification and reporting – being achieved by the SNCTC through the "See something, Say something" campaign – the SNCTC has one of the most sophisticated, user-friendly, and effective methods of both identifying and collecting SARs. The means by which SARs reach the SNCTC are the product of a formal partnership with the Las Vegas Convention and Visitor Authority (LVCVA), a successful partnership with the hospitality industry in Las

Vegas as a whole, and a user-friendly website interface that will be discussed in the following section.

The LVMPD entered into a formal agreement[29] with the LVCVA to enhance the private-sector SAR initiative. This agreement outlines the responsibility for both agencies to provide certain services to the public in accordance with their respective statutory authority. More specifically, the LVMPD is responsible for the day-to-day supervision of matters assigned to the SNCTC, which was established to improve communication and coordination among public safety agencies to maximize their ability to detect, prevent, investigate and respond to all crimes and all hazards in the greater Clark County and southern Nevada region. The LVCVA determined that being a formal and active participant of the SNCTC was in the best interest and a direct benefit to the hospitality industry in Clark County. As such, the LVCVA is now a member of the board of governors of the SNCTC and is required to contribute personnel or provide the financial support to hire personnel in order to fulfill the mission of SNCTC.

In order for this formal partnership to work effectively, the participatory role of the LVCVA in the SNCTC was adapted to allow participation without violating any statutes or laws regarding confidentiality and privileged information that only law enforcement agencies have access and right to access to in terms of certain classified and/or criminal information. To best serve this purpose, the LVMPD hired a private-sector specific intelligence analyst, dedicated to the interests of the hospitality industry, whose position is financially supported by the LVCVA. This intelligence analyst is an employee of LVMPD and is assigned to the SNCTC for the purpose of responding to the needs and security of the hospitality industry. Moreover, this intelligence analyst is not considered an employee of LVCVA for any purpose and only serves as a liaison between the LVCVA and SNCTC to represent the interests of the hospitality industry.

[29] Interlocal Agreement pursuant to the provisions of 277.180

The LVCVA does not have any right to control the work of the intelligence analyst, their assignments, work schedules, conditions of employment or any other aspect of the relationship with LVMPD.

Even though the private sector is primarily concerned with criminality related to gaming in Nevada, they are committed to an all-threats approach with the SNCTC. A highly successful example of this partnership is the SAR awareness program the SNCTC has with the hospitality industry in Las Vegas. In partnership with The University of Nevada Las Vegas Institute for Security Studies, state and local public safety, and homeland security agencies, the SNCTC developed a terrorism SAR awareness video titled "Nevada's Seven Signs of Terrorism[30]". The video - available in both English and Spanish languages - provides an informative walk through key behaviors and activities that are the hallmark of terrorist planning and preparations. While the video uses local examples in order for viewers to personally relate to the information, the key to the success of the terrorism SAR video is the fact that hotels in Las Vegas now require all employees to view the video – a promising indication of commitment to the partnership between the SNCTC and the private sector hospitality industry.

Information Sharing and Records Management

Collection

The SNCTC recognizes intelligence information as defined by the Fusion Center Guidelines (GIWG, 2005) and National Criminal Intelligence Sharing Plan (GIWG, 2003) as the product of systematic gathering and evaluation of raw information on persons or activities suspected of being criminal in nature. Criminal intelligence information submitted and stored within the SNCTC system/network is required to minimally meet the following three criteria:

[30] This video is available at: http://www.snctc.org/View-DVD.asp

1) Reasonable suspicion

2) Be obtained legally

3) Have relevance to a subject's suspected terrorist or criminal activity

Reasonable suspicion – or criminal predicate - means there is enough information to establish sufficient facts or basis to believe a subject or group is involved in definable illegal activity. This includes, but is not limited to, an enterprise that represents a significant/recognized threat to the population; is undertaken for the purpose of seeking illegal power or profits or poses a threat to the life and property of citizens; involves a significant permanent criminal organization or is not limited to one jurisdiction. Legally obtained refers to the information gathered and maintained through lawful means with authorized access that is relevant to the identification of a subject and the individuals' or groups' known or suspected involvement in terrorist or criminal activities. The SNCTC does not retain information related to political, religious, social views, associations (businesses, partnerships, etc.) or activities that are not related to criminal conduct or activity.

The SNCTC also utilizes different sources of information to enhance the intelligence fusion process. Many of the resources commonly accessed for information do not meet the criteria established for criminal intelligence and are not subject to 28 CFR Part 23[31]. Non-intelligence information may include data from law enforcement resources, public information outlets, and open sources such as the internet, newspapers, and other publications. Sources of information typically accessed by the SNCTC include:

- Criminal history records
- Warrants
- Case or investigative information from other systems

[31] Codified as 28 CFR Part 23 "Criminal Intelligence Systems Operating Policies", this regulation governs inter-jurisdictional and multi-jurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies and that are funded by or receive federal funds.

- Tips and leads
- Field Contacts
- De-confliction systems
- Driver's license, telephone subscriber, etc.
- Identification systems (AFIS, finger prints, mug shots, etc.)

In an effort to reduce the duplication of records and diminish the probability of maintaining dated, inaccurate information, to the extent possible, the SNCTC uses links and pointing tools to connect identifying data to a subject and the individuals' or groups' known or suspected involvement in terrorist or criminal activities. The SNCTC utilizes the collection and storage of non-criminal identifying information as applicable by 28 CFR Part 23 - which allows for the collection and storage of non-criminal identifying information in criminal intelligence systems under the following conditions[32]:

- Information must be clearly labeled as non-criminal.
- The field in which it is entered must be searchable.
- Information must be relevant to subject=s identification or criminal activity.
- Data cannot be used as the independent basis for meeting reasonable suspicion threshold.
- Political, religious, social views, associations (businesses, partnerships, etc.) or activities that are not related to suspicious conduct or activity are not permitted to be maintained.

Storage

The submission of information to the SNCTC system/network is critical to the overall success of its mission. As previously mentioned, criminal intelligence and non-intelligence data must be maintained separately in accordance with federal regulations. The SNCTC determined all data shall be kept in electronic format to ensure the security of information, minimize vulnerability, control audit activities, and expedite search and analysis activities. The originating agency is responsible for identifying information, attaching the correct labels, and saving or storing information in the designated criminal intelligence and non-intelligence areas of the

[32] Complete 28 CFR Part 23 information is available at: http://www.iir.com/28cfr/Laymensguide.pdf

SNCTC system/network. Paper documents are only available when electronic format is not an option, and stored under appropriate measures.

All criminal intelligence files contain a minimum of core information fields. In addition, the originating agency may include relevant and pertinent information as consistent with 28 CFR Part 23. The SNCTC intelligence files include:

- Name of subject (e.g. individual, organization, business, or group)
- Subject identifiers
- Suspected criminal activity
- Officer(s) involved
- Agencies/Bureaus involved
- Source
- Date of original submission
- Date of revision(s)
- Description of Activity
- Analysis
- Recommended Action

Information contained in working files can only be non-intelligence data. It is important for the SNCTC to minimize duplication of information. Information received by the SNCTC that is relevant to a file already on record is recorded by documenting the link to its location. In the event that data or information received is in paper form, it is scanned to an electronic format, labeled, and stored appropriately. The original paper hard copy is destroyed or returned to the originating agency depending on their policies or agreement with SNCTC. The SNCTC employs multiple classifications types for analytic products as well as certain pieces of raw information. An explanation of these classification types can be found in Appendix E.

In addition to the core file fields, the SNCTC requires the submitting agency to appropriately label all information intended for storage in the SNCTC systems/network. Both criminal intelligence and non-intelligence information is required to be labeled to denote the level of sensitivity or classification (restricted, limited, controlled, for official use, open source),

level of confidence (reliable, usually reliable, unreliable, unknown), and validity (confirmed, probable, doubtful, unknown).

Moreover, every named subject included in any submission must be reasonably suspected of direct involvement in criminal activity and must be properly labeled to identify the association – such as subject, associate, relative, or employee. For organizations or groups to be identified, a significant portion of the subject's activity must be criminal.

Dissemination

Information on the SNCTC system/network is disseminated using an established automated notification system to key personnel and participating agencies. This process maintains an electronic audit trail of notifications for security and auditing purposes. Participating agencies that receive electronic notifications are responsible for maintaining the appropriate security of all information as outlined by their agreements with the SNCTC. The SNCTC staff documents the release of all information - excluding the automated notifications mentioned above - using the appropriate form. Release of information requires verification of the inquirer's identity, right-to-know[33], need-to-know[34], and may be required to necessitate approval from the original source and/or an SNCTC executive. Recipients of intelligence/information/data from the SNCTC must agree to comply with 28 CFR Part 23 regulations. Each release form is maintained electronically and linked to the associated intelligence file being requested. In the event of an emergency or critical incident, the SNCTC

[33] The "right to know" dissemination standard is determined valid in a circumstance where the individual requesting the sensitive information is determined to have the official capacity and/or statutory authority to receive the information being sought.

[34] The "need to know" dissemination standard is determined valid in a circumstance where if the information to be disseminated is pertinent and necessary to the recipient in order to prevent or mitigate a threat or assist and support a criminal investigation.

director may approve the dissemination of information classified as restricted, limited, or controlled to law enforcement agencies, public safety, and emergency personnel who are coordinating information with responders on the scene. The release of information to private individuals for non-law enforcement purposes is restricted by Nevada Revised Statute (NRS) 239C[35] and requires the SNCTC director's approval.

Under NRS Chapter 239C Homeland Security (subsection 210), the Governor of Nevada declared certain documents prepared and maintained for the purpose of preventing or responding to an act of terrorism to be confidential. Further, documents (including records or other items of information) are not available for inspection by the public if such a disclosure creates a substantial likelihood of compromising, jeopardizing or otherwise threatening the public health, safety or welfare. Protected information under this statute includes, but is not limited to, the following:

- Critical infrastructure (maps, drawings, plans, etc)
- Emergency response plans
- Emergency radio transmission information
- Training, handbooks, manuals related to emergency response plans
- Other documents as determined by Executive Order

Original Documentation - Third Party Prohibition

The SNCTC does not allow original documentation obtained from an outside agency to be released to a third party by SNCTC staff without prior approval from the originating agency. However, some MOUs between the SNCTC and member/participating agencies contain this on-going approval. This includes both criminal intelligence information and data considered to be non-intelligence. It is the discretion of the SNCTC staff to choose to refer the requestor to the originating agency for further assistance. If the SNCTC believes original documentation

[35] Full reference for NRS 239C is available at: http://www.leg.state.nv.us/nrs/NRS-239C.html#NRS239CSec010

received from an outside agency should be released, a SNCTC executive coordinates with the originating agency to request permission to disseminate - or request a modified or redacted version that can be reclassified for release purposes. Only the originating agency can redact, modify information, and/or authorize release of their information. If the SNCTC is the original source of the information marked restricted, limited, controlled, or for official use only, and a request is received or determination is made to provide the information to agencies outside of law enforcement, SNCTC executive may approve modification and redaction for the purposes of reclassifying the information for distribution to other non-law enforcement entities as appropriate.

Approved Methods for Information Dissemination

The SNCTC disseminates information using the most secure methods available based on the sensitivity level of the information, available mechanisms for sharing information with the inquirer, and timeliness. Based on the criteria discussed previously, the SNCTC has approved the following mechanisms for the dissemination of information:

- Verbal communication; via telephone or in person.
- Hand delivered; appropriate labeling.
- Interoffice mail; appropriate labeling required.
- Approved secure electronic mail, using appropriate encryption applications.

Access to the SNCTC system/network maybe directly available to participating agencies not located within the SNCTC. Appropriate security controls to prevent unauthorized access or damage to information stored in the system have been adopted by the SNCTC.

Public Request for Information

All public requests for information made to the SNCTC must be directed to the records compliance administrator. Only a SNCTC executive, under the guidance of the SNCTC board of governors, SNCTC policies, and in accordance with all established agreements, has the authority to approve the release of information to the public. Only the subject of the information on record, or a legal representative, may obtain access to the requested information. A legal representative's authorization must be written and notarized and the person authorized must have picture identification to receive the information. The SNCTC follows a strict dissemination policy. The requestor will be advised if he or she is not entitled to the information. Juvenile information and certain victim and witness information are protected from disclosure by law. The SNCTC reserves the right to redact and delete information it deems prudent to protect from public disclosure in accordance with all laws, regulations, and policies.

An individual making a public request for information must fill out a form at the SNCTC and provide the following:

- Name
- Copy of driver's license or other government issued photographic identification (e.g. military id, passport, alien card)
- Name of employer
- Citizenship
- A statement of the purpose for the request to inspect the information. (Note: Nothing in the supporting statutes prohibits an SNCTC employee or public officer from contacting law enforcement to report suspicious or unusual requests to inspect information).

The SNCTC observes persons during inspection of information they have requested in a location and in a manner that ensures the information is not copied, duplicated, or reproduced in any way. Restricted documents may be copied, duplicated or reproduced only under the following circumstances and in compliance with all other laws, rules, and policies governing information requested:

- Lawful order of a court of competent jurisdiction.

- As reasonably necessary in the case of an act of terrorism or other related emergency.
- To protect the rights and obligations of a governmental entity or the public.
- Upon request of a reporter or editorial employee, affiliated with a news association, or commercially operated and federally licensed radio or television station for use in the course of this employment or affiliation.
- Upon request of a registered architect, licensed contractor (or designated employee of) for use in their professional capacity.

Information Review and Purge

In an effort to preserve citizens' civil rights related to the retention of information, the SNCTC has in place an ongoing review of criminal intelligence and non-criminal intelligence (SARs) files for relevancy, importance, and sensitivity required to delete inaccurate or outdated information and remain in compliance with federal regulations. Automated system audit trails, purges, and reports are periodically reviewed. Additionally, manual review and destruction processes are followed to ensure both electronic files and hard files remain in compliance with the SNCTC's privacy/records policies. As mandated by 28 CFR Part 23, there is a five-year maximum retention of criminal intelligence information. The SNCTC determines the start date by the initial date information (subject record or file) is stored in the SNCTC system/network. Any significant change or update to the information resets the purge date to be five years from the point of change - the changing of an address, phone number, or noncriminal associations are not considered significant changes. As such, if a criminal intelligence file remains without significant changes during the five-year period it is removed from the SNCTC system/network. This system automatically generates a report at six months prior to purging for files meeting this criterion. The originating agency reviews the file scheduled for destruction for currency and accuracy, and then an approval decision for removal of the document, along with an explanation as to why the information shall remain, is made.

Non-intelligence information is consistent with the same review period and purge criteria as intelligence data. Information scheduled for purge is returned to the originating agency or disposed of in accordance with the originating sources' requirements. These purging requirements from the originating agency must be in writing with the SNCTC. Information/intelligence/data that is approved for purging is documented as such and removed from the system by the originator of the information. Any paper documents containing criminal intelligence information approved for destruction are disposed of using approved destruction methods. Electronic files are purged (deleted) from the SNCTC system/network by the originating agency, supervisory authority, or information technology authority at their request. Paper documents are destroyed by shredding to prevent the reconstruction of any of the documents. Approved shredders are located in the SNCTC facility and all files and record destruction take place on site at the SNCTC.

Information Security Inside the SNCTC

The electronic storage of information on the SNCTC system/network is the most secure and therefore the recommended method for retaining all information. As stated previously, paper copies are kept to a minimum at the SNCTC and any paper documents classified at the restricted, limited, and controlled level are kept in a locked cabinet in a designated secure area of the SNCTC. Less classified documents – such as For Official Use Only - are kept secure within a locked area (e.g. file drawer) or office. The SNCTC has gone to great efforts to secure the facility and its equipment from unauthorized access. However, additional responsibility for protecting information lies with those individuals working within the SNCTC. The following safeguards are required to be adhered to by SNCTC staff:

- Do not leave documents in clear sight when in work areas.
- Always remove and store documents in a manner appropriate to their classification when leaving the work area.
- When using photocopiers, facsimiles, etc. do not leave originals behind.
- Be aware of others in the immediate area when documents are open for viewing on computer screens. Use the minimize function to limit exposure.
- Follow computer protection policies when setting passwords. Change passwords immediately if suspicion of compromise arises.
- Do not provide your password to anyone.
- Always turn your computer off when leaving the area for an extended period of time; and at the end your work day.
- Immediately notify the appropriate authority if you suspect information is missing, has been altered, or has been accessed without authorization.

Information Access

Each participating agency retains sole ownership, exclusive control over, and sole responsibility for the proprietary information it contributes to the SNCTC. All work that is the product of and originates from an employee of a participating agency clearly identifies the contributing agency and also clearly states that the information is and remains the sole property of the contributing agency under that agency's exclusive control. All joint reports or products of collaboration between participating agencies and the SNCTC are considered property of the SNCTC. However, the dissemination of joint products is dependent upon approval from any of the contributing participating agencies. Each participating agency has the sole responsibility to ensure the accuracy of information it has contributed to the SNCTC. If the participating agency becomes aware of any inaccuracy in information it has contributed, it has the responsibility to correct that information and communicate this correction to the SNCTC. Each participating agency is responsible for ensuring that all shared information is collected for legitimate law enforcement purposes to investigate, prevent or mitigate suspected criminal activity and/or threats.

All participating agencies' information and records system designs must ensure that audit trails, system security, and information dissemination correspond to the mission of the SNCTC. The following are key aspects that must be incorporated into each participating agency's information and records system design:

- Collection Limitation
- Data Quality
- Use Limitation
- Security Safeguards
- Openness
- Individual Participation
- Accountability

Any report prepared by a participating agency must be classified at the level of the highest classification of any material it contains and cannot be disseminated to any party who does not possess that clearance level as well as the right-to-know and/or need-to-know.

The SNCTC handles both "classified" and "sensitive but unclassified" law enforcement/public safety information. Participating Agencies are only granted access to classified or sensitive information if they have the appropriate security clearances. Any SNCTC members seeking access to classified information who do not possess secret/top secret clearances, depending on the level of access to classified information sought, are subject to a full background investigation with access to the sensitive information contingent upon receipt of an appropriate security clearance. In these circumstances where a background investigation is required, the participating agency is responsible for all costs associated with obtaining the necessary security clearance for their member.

All participating agencies, their employees, and their contractors must agree not to disclose classified or sensitive information to anyone not authorized to receive information at the specified classification level, and who does not also have a need- and right-to-know, without the

express written permission of the originating agency. Moreover, all intelligence products and intelligence sharing must comply with 28 CFR Part 23 standards.

Reports and Products

The SNCTC has an established system of report production and dissemination for other public safety agencies and non-government consumers. To begin with, the SNCTC utilizes a web portal called "All-Data Virtual Information Sharing Environment" (ADVISE) to disseminate products and other communications. The ADVISE system allows the SNCTC to disseminate and/or post a wide-range of general information products. Information typically available through program reports are; tips and leads, case files, intelligence files, SNCTC products, and a reference / research library. For agencies or organizations soliciting information from the SNCTC, their initial point of contact is the watch station. This point of contact is a phone line staffed by trained personnel to provide constant situational awareness and identify emergent patterns in crime, hazards and risks.

The type of products provided by the SNCTC follow an intelligence/information production plan. A standardized format is required for all products. This format includes a single banner that is agency-neutral across the top of the documents. Agencies that provide joint cooperation for compiling products are identified in the product narrative. Furthermore, the production plan identifies three categories of products:

- Situational Awareness Reports
- Periodic Reports
- Ad hoc Reports

Situational awareness reports are the most general and straightforward product from the SNCTC. These reports include a synthesis of open-source information and typically include the

latest and most pertinent information related to breaking news, significant crime events, and bulletins from the National Operations Center (NOC)[36]. In short, these reports are intended to provide the SNCTC community with a rich situational awareness of their areas of responsibility. Periodic reports are centered on counter-terrorism analysis. These reports are broken down into five sub-categories of types of terrorism. Even more specifically, these five sub-categories have their own methodology for crime analysis that incorporates 42 categories of analysis. Periodic reports are disseminated to SNCTC consumers on daily, weekly and monthly intervals. The final type of reports is ad hoc. Somewhat similar to the situational awareness reports, ad hoc reports provide more detailed crime advisories, tactical intelligence support, Homeland Security alerts (urgent), Homeland Security advisories (important), threat assessments (less important), and requests for analysis from other agencies.

Information Sharing Functional Exercise

From November 2-12, 2009, the SNCTC spearheaded a functional information sharing exercise with three Nevada Fusion Centers, the U.S. Department of Homeland Security / FEMA, and the State of Nevada / Clark County / City of Las Vegas Emergency Management – this exercise was referred to as "Operation Silver Rogue". The objectives of the exercise were to 1) detect, recognize and act upon indicators and warnings of potential criminal/threat activity, and 2) properly share and conduct investigations and operations related to potential terrorism. The exercise indicated strengths and weaknesses.

[36] The National Operations Center provides real-time situational awareness and monitoring of the homeland, coordinates incidents and response activities, and, in conjunction with the DHS Office of Intelligence and Analysis, issues advisories and bulletins concerning threats to homeland security, as well as specific protective measures. The NOC – which operates 24 hours a day, seven days a week, 365 days a year – coordinates information sharing to help deter, detect, and prevent terrorist acts and to manage domestic incidents. Information on domestic incident management is shared with Emergency Operations Centers at all levels through the Homeland Security Information Network (HSIN).

The most significant strength exhibited during the exercise was that intelligence sharing and coordination between the three Nevada fusion centers was effective. The Terrorism Liaison Officer program with the private sector provided effective information sharing. Participants of the exercise found the analyst and executive briefings to be effective. The SNCTC staff made effective use of predictive and geo-spatial analysis and discussed various modes and locations of attack. Weaknesses identified during the exercise included a critique of the ADVISE system given its limited search capacity. Moreover, there was a lack of a formalized reporting, vetting and storage process for SARs. The SNCTC lacked a formal Request for Information (RFI) tracking system. Lastly, there was disconnect in the information flow between the analytical staff and the investigative staff.

Access to the SNCTC via Internet

To enhance communication for information sharing between the SNCTC and its public/private partners, they have created a comprehensive and extremely user-friendly website by utilizing federal funds. The SNCTC's website - www.SNCTC.org - is multi-tiered. Tier access is as follows:

- Tier 1: Public Access
- Tier 2: Private Access
- Tier 3: Public Safety Access

The first tier, designed for the public to access, is the information displayed without having to login to the website. This is where the public can learn more about what the SNCTC is and its mission. Anyone who visits the website also has the ability to submit a SAR form to report anything they may have witnessed. The second tier, designed for the private sector to access, requires login information to move beyond the public realm. Access and login credentials are

granted by the SNCTC upon review when requested by persons who are not already affiliated with the SNCTC.

Second tier information that can be viewed after signing into the website is typically information that is pertinent to the private sector/hospitality industry. While specific information cannot be disclosed here, this information is typically "need-to-know" or "be on the lookout" to increase the level of preparedness/prevention among private sector organizations. Tier three is the most restricted access tier and is accessible only by public safety and law enforcement personnel. Once again login access must be granted by the SNCTC after a more comprehensive vetting process. This information typically includes access to SAR reports, intelligence products/reports, and additional sensitive information posted by the SNCTC for other law enforcement. This portion of the website is also referred to as the *SNCTC Trusted Information Exchange (STIX).*

Homeland Security Hotline – SNCTC Watch Station

The SNCTC manages a toll-free Homeland Security Hotline that is staffed twenty-four hours a day, seven days a week by watch station personnel. The purpose of the hotline is to facilitate the collection of suspicious activity reporting (SAR). It is the policy of the SNCTC that every suspicious activity report is investigated by the collection branch or the operations group. The Federal Bureau of Investigation (FBI) retains the statutory authority to investigate terrorism cases, and all SARs are immediately transmitted to the FBI personnel assigned to the SNCTC.

The watch station is staffed by personnel from the analysis section, regardless job classification and/or employing agency. The primary responsibility of the watch station is to maintain constant situational awareness of the southern Nevada metropolitan area as well as the

State of Nevada. This situational awareness is made possible by integrating the computer-aided dispatch displays of each of the participating agencies. It is the responsibility of the watch station personnel to report to the appropriate jurisdiction any emergent public safety or public health issues as soon as they become evident.

The watch station position is one of the most critical operational positions within the SNCTC. It is responsible for recognizing significant public safety events locally, nationally, and globally. It is one of the centerpieces to help achieve the SNCTC's mission to prevent, reduce, and disrupt crime and terrorism through the early warning of all-crimes, all-hazards, and all-threats. The watch station also assists in the support of critical incidents, emergency responses, and investigations. The watch station is where real time analysis begins, and it is therefore critical that personnel assigned are actively engaged monitoring events. Therefore, the person manning the position has the responsibility and authority to direct the completion of time sensitive requests to and from other members of the analysis section, all SNCTC partners, and to coordinate the dissemination of such information to decision makers.

Privacy and Civil Liberties Protection

The SNCTC has developed a privacy policy that utilizes 28 CFR Part 23 as a foundation, and with the guidance provided by the U.S. Department of Justice Privacy Policy Development Guide, Law Enforcement Intelligence Unit Intelligence File Guidelines, and the Global Justice Information Sharing Initiative. The SNCTC is transparent with their privacy policies, and welcomes review and input from local civil liberties communities. The SNCTC expects participating agencies to share their informational databases with other participating agencies to the extent allowable and authorized by the individual agencies guidelines, Nevada law, and

Federal law. Personnel from participating agencies utilize their own forms, recordkeeping, and reporting methods. Reports prepared by the SNCTC are shared with all SNCTC analysts and sworn personnel, with the proper security clearance and the need to know. Moreover, the SNCTC's privacy policy draws upon the eight privacy design principles developed by the *Organization of Economic Cooperation and Development's Fair Information Practices*[37.] These principles are:

- Purpose Specification - Define agency purposes for information to help ensure agency uses of information are appropriate.
- Collection Limitation - Limit the collection of personal information to that required for the purposes intended.
- Data Quality - Ensure data accuracy.
- Use Limitation - Ensure appropriate limits on agency use of personal information.
- Security Safeguards - Maintain effective security over personal information.
- Openness - Promote a general policy of openness about agency practices and policies regarding personal information.
- Individual Participation - Allow individual's reasonable access and opportunity to correct errors in their personal information held by the agency.
- Accountability - Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies.

The SNCTC has established mechanisms (interagency connectivity, public records subscription services, etc.) to create access to existing data sources from participating and member agencies to share data with the goal of identifying, developing, and analyzing information and intelligence related to terrorist activity and other crimes for investigative leads. This capability facilitates the integration and exchange of information between the participating and member agencies.

Collection Limitations

[37] For more information visit: http://www.oecd.org

Given the mission of the SNCTC is to develop information and intelligence products by cooperating with other agencies and organizations. The decision of these agencies to participate with the SNCTC, and the information they provide, is voluntary and is governed by the laws and rules governing the individual agencies as well as by applicable federal laws. Because the laws, rules, or policies governing information and intelligence that can be collected and released on private individuals will vary from agency to agency, limitations on the collection of identifying information is the responsibility of the collecting agency and the original source information. Each agency that contributes information is to abide by the collection limitations applicable to it by law, rule, or policy. Information contributed to the SNCTC must be done in conformance with those limitations. The SNCTC does not store information that has been collected in violation of these laws, rules or regulations.

Data Quality

The agencies participating or coordinating with the SNCTC are responsible for collecting the information, remain the owners of the information contributed, and are responsible for its quality and accuracy. Since inaccurate and/or identifying information can have a damaging impact on the individual concerned and on the integrity and functionality of the SNCTC, any information obtained through the SNCTC must be independently verified with the original source from which the information was extrapolated before any official action (e.g., warrants or arrests) is taken.

Limitation of Information Use

Information obtained from or through the SNCTC is only used for legitimate law enforcement investigative purposes. A legitimate law enforcement investigative purpose means the request for information can be directly linked to a law enforcement agency's criminal investigation or is a response to a confirmed lead that requires follow-up to prevent a criminal or terrorist threat. The board of governors takes the necessary measures to make certain that access to the SNCTC's information and intelligence resources is secure and have the authority to prevent any unauthorized access or use. The board reserves the right to restrict the qualifications and number of personnel who can access the SNCTC and suspend or withhold service to any individual violating the SNCTC's privacy policy. The board also reserves the right to conduct inspections concerning the proper use and security of the information received from the SNCTC to further ensure the integrity of their information sharing practices.

All personnel who receive, handle, or have access to information from the SNCTC receive training on information/intelligence requirements. Every authorized personnel with access to the SNCTC understand that this access can be denied or rescinded for failure to comply with the applicable restrictions and use limitations. All such personnel must agree to the following rules:

- Data will be used only to perform official law enforcement investigative-related duties in a manner authorized by the SNCTC.
- Individual passwords will not be disclosed to any other person except as authorized by SNCTC management.
- Individual passwords will be changed if authorized personnel of the SNCTC or members of the Center suspect the password has been improperly disclosed or otherwise compromised.
- Background checks will be completed on personnel who will have direct access to the Center by the participating agency for which the individual is employed.
- Use of data in an unauthorized or illegal manner will subject the user to penalties established by the board of governors, discipline by the user's employing agency, and/or criminal prosecution.

Transparency

The SNCTC is intent on promoting transparent information sharing practices. As such, the SNCTC, and its participating agencies, are open with the public concerning data collection practices - when such openness does not jeopardize ongoing criminal investigations. The SNCTC and participating agencies refer citizens to the original collector of the data as the appropriate entity to address any concern about data accuracy and quality – once again when this can be done without compromising an active inquiry or investigation.

Accountability

When a request for information is made to any of the SNCTC information applications, the original request is automatically logged by the system identifying the user initiating the request. When information is disseminated outside of the agency from which the original request is made, a secondary dissemination log is maintained in order to track information for audit purposes and provide notification in the event errors are identified or corrections are necessary. Secondary dissemination of information is only allowed by a law enforcement agency for a law enforcement investigative purpose or to other agencies as provided by law and in accordance with SNCTC policies. The originating agency from which the information is requested maintains a record of any secondary dissemination of information. This record reflects (at a minimum):

- Date of release.
- Name of releasing individual.
- Name, verification of inquirer (need-to-know and right-to-know will also be documented).
- Information released.

Recipients of SNCTC information are advised on, and agree to protect, its confidentiality and restrict its access based on right and need to know. SNCTC information cannot be disseminated outside the recipient's organization without the written permission of a SNCTC executive. Given the nature of law enforcement intelligence, the need for such protective use is necessary as any unauthorized disclosure of SNCTC information could damage or compromise ongoing or future investigations and operations. Furthermore, SNCTC information that is disseminated remains the property of the SNCTC and recipients must agree to comply with requests to immediately seal or destroy information obtained upon notification by a SNCTC executive. The SNCTC may request a recipient to sign a non-disclosure agreement prior to the release of any information. Refusal to sign such an agreement can limit or prohibit disclosure of requested information to that particular recipient. The SNCTC director, deputy director of quality assurance, and/or privacy protection officer is responsible for conducting or coordinating audits and investigating misuse of the SNCTC's information under the oversight of the board of governors.

Intelligence-Led Policing: Requirements Driven

In order for the SNCTC and their respective partners to have an effective intelligence-led policing (ILP) philosophy, a formal requirements process is necessary to guide information collection – this process is controlled by the requirements committee. Intelligence requirements are designed to fill intelligence gaps – typically with respect to case-specific information (case requirements) or on-going threats (standing requirements) – by focusing collection efforts. It has become increasingly evident that many agencies working with the SNCTC are uncertain as to what requirements actually are and how they can benefit their efforts. In order to address this

uncertainty, the SNCTC has urged other agencies to formulate their intelligence requirements as questions. This is a straightforward approach to identifying what information is necessary to analyze and thus input into the intelligence-led policing cycle. An example of an intelligence requirement question may be "Is there radicalization in Nevada prisons?" Agencies working with the SNCTC are urged to compose their requirement questions and forward them to the SNCTC with the intent of identifying emerging threats and issues.

Self-Proclaimed Strengths and Weaknesses

While an estimate on quantity or sources was not provided, one of the SNCTC's greatest strengths is its ability to gather raw information from the community in the form of suspicious activity reports. This improvement of increasing intelligence and information "receptors" is the result of the growth of awareness within the community and other public safety agencies above and beyond the SAR initiatives. For example, it is important for the SNCTC – and fusion centers in general – to market their resources and products to all law enforcement and the public. Given that fusion centers are a fairly new concept in the law enforcement arena, a great deal of misunderstanding and/or misconception exists as to the utility of fusion centers. Most local agencies are unaware of the resources and products provided by fusion centers and the applicability these products have for their everyday public safety missions – not just terrorism.

An additional strength of the SNCTC is that it contains multiple capabilities under a single roof. As it has been discussed, a variety of agencies and organizations are represented within the SNCTC – from law enforcement and the public/private sectors. Arguably the three most unique capabilities are the All Regional Multi-Agency Operations and Response (ARMOR) that focus on CBRN threats, the private-sector specific analyst funded by the LVCVA, and a

representative from the Clark County Public Schools. The ARMOR unit consists of a multitude of advance technological and strategic equipment for not only responding to CBRN threats, but also equipment that aids everyday law enforcement in a variety of situations and special events. The school representative is funded by the Clark County school dispatch to increase the level of school preparedness as well as aiding law enforcement's awareness of issues and threats arising from and taking place in Clark County schools. Another strength indicated by the SNCTC is their ability to leverage funding from federal sources and through the commitments of the LVMPD and other agencies/organizations.

Lessons learned have also attributed to improving some SNCTC weaknesses into strengths. The previously discussed watch station was created to serve as a primary point of contact for those reaching out to the SNCTC. Rather than speaking to "anyone who picks up the phone", this watch station personnel has a working knowledge of the different on-going initiatives and current issues within the SNCTC and can direct the inquiry to the correct person. Moreover, the watch station personnel maintain the most heightened sense of awareness as to emerging threats in the southern Nevada region. Additionally, an experienced senior analyst was hired by the SNCTC to supervise all analysts and their functions to improve efficiency and effectiveness of the intelligence products.

Conclusion

As compared to the Florida Fusion Center, the Southern Nevada Counter-Terrorism Center is quite different, but has similar baseline consistencies. With respect to the current study, the SNCTC is perhaps a further disconnect from how most local agencies would engage in

law enforcement intelligence practices; however relevant constructs are once again observed within this environment.

To begin with, the SNCTC subscribes to an "all threats, all crimes, all hazards" perspective. Moreover, this approach emphasizes the importance of collection requirements that incorporate suspicious activity reports (SARs). Such an approach requires the development of partnerships with the community and private sector in order to educate them on SARs as well as establish channels for two-way communication of this information. Similar to the FFC, this perspective is exemplified through formal partnerships with non-public safety participating agencies – such as the Southern Nevada Health District, Clark County School District, and Las Vegas Convention and Visitors Authority.

The importance of SARs was further demonstrated after the functional field exercise "Operation Silver Rogue" when one of the concluding recommendations was to further educate the community and private sector on SARs. Furthermore, sharing information across jurisdictional boundaries was deemed imperative. An "all-threats/hazards" philosophy combined with SARs, community policing, and trans-jurisdictional communication are characteristics consistent with the C&C model of intelligence-led policing.

Structurally, the SNCTC is reliant upon a high degree of formalization. A variety of formal personnel positions, committees, advisory boards, and policies/procedures guide the center. As it was mentioned previously, this is anticipated to be the nature of many comprehensive intelligence capacities across the country – whether they are fusion centers, state agencies, or large local agencies. Simply put, the more bureaucratic an agency is, the more likely they are to be formal. Interestingly, it was noted by a SNCTC executive that formalization might play a role as an inhibitor of successful intelligence-led policing. An identified weakness

– or obstacle – the SNCTC faces are the institutional inhibitors of getting policies put in place in a timely and effective manner. As with all large law enforcement bureaucracies, a certain amount of red tape can be expected. However, the landscape of intelligence and information sharing relies upon expedient decision making and the operational hierarchy of large agencies, at times, can inhibit the sharing of information in a manner consistent with the "need to know". This view is shared by organization theorists who argue formalization stifles innovation (Mastrofski, 1998).

Formalization is perhaps explained to an extent by functional differentiation – or the presence of different units. The SNCTC relies upon a variety of specialized units to vary out specific tasks. These units include the Collections Section (comprised of the Collection Management Group and Operations Group), Analysis Section, Intelligence Requirements Committee, and the Quality Assurance Section. Furthermore, the development of the multi-tier web portal that allows for two-way communications further enhances this capability. Interviews with the SNCTC personnel indicated these units greatly enhanced the ability of the SNCTC to carry out their intelligence-led mission as a result of having specialized persons responsible for specialized tasks – thus increasing effectiveness and efficiency.

The SNCTC requires analysts to maintain responsibility for a variety of analytic products as well as services. Products include those that have been discussed previously – such as risk assessments, trend patterns, and executive reports. However the services aspect is somewhat unique and is primarily concentrated on what the SNCTC calls the "watch station". A lesson learned from "poor practice" was rather than having an operator be responsible for incoming calls directly to the SNCTC, these calls are now answered by analysts or intelligence-specific persons with knowledge of the operations and different units. The phone calls received by the

watch station are typically SARs, requests for information, or a tip from another law enforcement agency. When an operator was answering these calls they were not knowledgeable about the actual operations of the SNCTC and this created a barrier in the communication channels – as well as increasing issues due to quality of interpretation on behalf of the operator. With analysts or intelligence-specific personnel answering the calls, the information coming in was immediately entered into system and could also be acted on immediately if a tactical response was required. Commitment is rather straightforward and was demonstrated by the lead law enforcement executive Sheriff Doug Gillespie.

The importance of commitment to note in this observation is in reference to two aspects 1) the commitment towards intelligence practices as the forefront of law enforcement, and 2) the devotion of resources from Las Vegas Metro Police Department to be the primary fiscal agency of the SNCTC – dedicating finances, personnel, and equipment. Lastly, the importance of quality intelligence products is demonstrated by the Data Assurance Section and importance of data quality. This section of the SNCTC (which is made up of three groups) is tasked with the responsibility of securing the physical security of the SNCTC as well as making sure the SNCTC is compliant with legal information collection, dissemination and retention. Of more relevance is the performance measurement group that is tasked to develop and collect the data to measure the ability of the SNCTC to perform its established mission and determine if the SNCTC outcomes align with the intelligence requirements set forth by the requirements committee. These performance measures are at the organizational-level and not the analyst level. However it can be logically assumed that as analysts are responsible for the creation of intelligence-products on which the SNCTC bases its decisions for strategic and operational planning that the SNCTC

recognizes the importance of quality analyst performance evaluation – even though this was not directly observed or documented.

Once again, the SNCTC has provided a unique example of an intelligence-environment that is different from most local agencies. Despite the differences, relevant ideas remain consistent as the underlying philosophy of law enforcement intelligence practices should remain consistent regardless of size of responsibility. Just as it is expected that different local agencies will have different intelligence-led policing philosophies, fusion centers will as well. These differences will play a critical role in future research as the most influential factors attributing to successful adoption and practice are identified across different environments.

Chapter 8: Summary of Key Findings, Policy Implications and Research Needs

Although the federal government has provided support to build an intelligence infrastructure to more effectively respond to terrorism, there has been virtually no empirical work that describes the major issues and obstacles faced by SLT law enforcement agencies and fusion centers on intelligence-related issues. Law enforcement leaders seek informed solutions for effectively managing the intelligence function and guidance that will allow them to gauge how well they are doing in terms of accomplishing intelligence goals. This study is a critical first step in documenting the status of the progress made accomplishing key intelligence goals, and we believe this study contributes to the knowledge of and literature pertaining to intelligence practices in the United States. In this final chapter, the research team attempts to accomplish three goals. First, provide an overview of the key findings from the study. Second, discuss policy implications. Third, highlight limitations with this research and suggest future research needs.

Summary of Findings

The research team surveyed state, local, and tribal law enforcement officers and fusion center personnel and conducted three case studies to better understand intelligence practices, information sharing, performance metrics, and communication networks. This section highlights some of the key findings.

1. It appears that significant progress has been made post 9/11 installing fundamental policy and procedures related to building the intelligence capacity of law enforcement and fusion center agencies. Both respondents from state, local, tribal law enforcement agencies and fusion centers indicated that they were familiar with intelligence guidelines

and standards, had a good working knowledge of threats in their community, and have some working knowledge of intelligence-led policing. Personnel also indicated that they have attempted to take advantage of the wide range of training opportunities available for intelligence analysts.

2. Despite the progress that has been made, there is significant room for improvement and development. For example, although respondents indicated that they were familiar with national standards and guidelines, they also expressed the belief that the policies and procedures within their agency have yet to reconcile with these requirements. Similarly, the respondents noted they were aware of the threats, but identified a need to build a capacity to better identify these threats and noted shortages in resources and personnel in accomplishing these goals. Also, they were aware of key civil rights and privacy issues, but respondents reported there is considerable work that needs to be done in their agencies to ensure agencies are fully compliant.[38]

3. Fusion centers appear to be farther along addressing many different issues, including instituting an intelligence-led policing philosophy, establishing and being compliant with privacy issues, and fostering relationships with other agencies. Not all fusion centers were fully functional at the time of the survey, but had plans and goals to provide them direction along with guidance available from their peers as well as federally-supported training and technical assistance.

4. Critical to prevention and response is the sharing of information. In addition, it is clear that a wide range of law enforcement, community, government and private

[38] It should be noted that since this survey was administered there were two new training programs on civil rights and privacy delivered to law enforcement intelligence personnel (one from DHS and one from BJA/DOJ). In addition, during this time period fusion centers have developed and submitted privacy policies for review through joint DHS/DOJ technical assistance.

businesses may have information that is important to the intelligence fusion process thus it is important to build relationships with a diverse range of agencies and organizations. Both SLT and fusion center respondents indicated that that they have worked at building relationships with different agencies especially other law enforcement agencies, but fusion centers had closer relationships with a more diverse range of agencies and were more likely to be working with National Guard, transportation, public health, homeland security, emergency management, fire marshal, and critical infrastructure personnel.

5. Although many information linkages have been established, the respondents also indicated that they were not completely satisfied with these relationships. That is, it appears that the personnel were working with other agencies and making connections, but they think the relationships need further development to ensure consistent, substantive and timely information sharing.

6. There is an overwhelming amount of information going into and out of these agencies, and it is likely, without having enough analysts within the organization or analysts not effectively trained to process this information, that there are missed opportunities for strategic and tactical understanding of homeland security and criminal threats.

7. Both SLT and FC respondents agreed that the quality of intelligence products produced should be critical to the assessment of performance by analysts. There was some variation when comparing the two samples of respondents Information sharing and the quality of products was somewhat more important to fusion center respondents while having intelligence that led specifically to arrests, investigations, and convictions was more important to the SLT agency respondents. This difference may be indicative of a misunderstanding among SLT officers regarding the value and purpose of intelligence

analysts as well as the responsibility of operational units to act on the intelligence products in order to interrupt threats and pursue investigations

8. An analysis of the types of products produced and analytical procedures used on a daily basis also highlighted some of the differences in the intelligence mission of state, local, tribal law enforcement agencies and fusion centers. Specifically, fusion centers were more likely to be fostering information sharing connections, conducting a greater range of different types of analysis, and working with public health and other hazards related data on a daily basis. This should be expected given the roles and national standards for fusion centers.

9. It is important to consider the formal communication patterns that support and impede the intelligence process. These systems are critical because they provide an additional way for homeland security and intelligence officials to promote a necessary understanding of the procedures that need to be followed for better information sharing. The findings that were presented indicated that both SLT and FC respondents think that they have access to key communication systems and other sources of information that might be used to enhance intelligence products. Fusion center respondents were however somewhat more critical when asked whether RISS.net, LEO, HSIN, ATIX, and FBINET meets their intelligence and information sharing needs. Not surprisingly, the results also indicated that a higher percentage of fusion center respondents noted that they had access to various critical sources of intelligence information, including HSIN, RISS.net, FBINET, LEIU, and Health Related data.

10. The case studies of fusion centers are valuable in that they provide in-depth coverage of structural, policy, and strategic approaches that have been successful. The

organizations studied were guided by a litany of formal policies and comprised of multiple task-specific units. These formalities allow for a strategic division of labor for specialized persons to perform specialized tasks – thus improving effectiveness and efficiency.

11. Each of the case studies also revealed that the fusion centers were "works in progress" and that the agencies had to update and embrace changes motivated by shifts in their external environment. For example, the Florida Fusion Center conducted an assessment of information sharing gaps between law enforcement agencies within the state of Florida. One of the findings from this gap analysis was that local law enforcement was not engaging in information sharing as a result of poor, or nonexistent, commitment to the intelligence-led approach. At the Southern Nevada Counter-Terrorism Center, a strong administrative commitment to an intelligence-led approach was established when Sheriff Doug Gillespie announced (multiple times) that the Las Vegas Metro Police Department (the primary agency of the SNCTC) was going to fully embrace this new philosophy.

Policy Implications

The status of law enforcement intelligence in SLT agencies appears to be similar to the early development of community- and problem-solving policing during the early 1990s. Law enforcement officers and executives recognize the importance of intelligence yet the implementation of law enforcement intelligence remains uneven a decade after 9/11. Several factors may contribute to this. First, the philosophical underpinnings of law enforcement intelligence was significantly changed and broadened, hence a resocialization process among

intelligence personnel had to occur. Second, while the 9/11 attacks remain as the benchmark for change, in reality new standards – such as the National Criminal Intelligence Sharing Plan and training programs did not emerge until 2003. Moreover, new standards and directions continue to evolve even at the time of this writing. Third, it simply takes time to develop new organizations such as fusion centers and get them at an operational level. Similarly, training and developing new policies in America's 16,000 law enforcement agencies is a massive task, particularly when new processes – such a participating in a fusion center – must be marketed and sold to the agencies as wise investment in resources.

Uneven development and evolution is even more the case when considering the intelligence-led policing philosophy and practice. Although respondents were familiar with the term ILP, the results suggest that most agencies are at an early stage of implementation. Indeed, there are different conceptual understandings of ILP and different visions of the role ILP should hold in law enforcement organizations. Like the community policing movement, these results reveal clear needs for training and commitment of resources and for addressing the tension between specialization and generalization. Additionally, the goal of increasing intelligence capacity and adopting ILP comes at a time that SLT agencies operate under significant budgetary constraints. Finally, the results suggest the potential for fusion centers to serve a critical role in continued development of the law enforcement intelligence capacity in local agencies.

Although the results of this study point to clear progress in the development of law enforcement intelligence capacity, they also reveal challenges. Clearly, there is a need for the commitment of resources in the form of personnel and training. Given the federated and decentralized structure of law enforcement in the U.S., it is critical that mid- to large agencies have analysts who can conduct local level analysis as well as push information and intelligence

to Fusion centers.. Small agencies need to have intelligence liaison officers who can serve as "nodes" in the intelligence network. This requires commitment of resources at a time that many agencies are not hiring or even cutting personnel. Law enforcement executives as well as policymakers at local, state, and federal levels will need to consider the implications of these budgetary issues. While many executives acknowledge that the use of analysts make the agency "work smarter" thereby having a great effect on crime and community order, it remains a difficult concept to sell to the public and politicians.

It is also clear that there is a need for continued and expanded training. This includes specific training for analysts, fusion center personnel, and intelligence managers. It also, however, means more general training for all SLT personnel on ILP and the role of SLT officers in the intelligence process to include what types of information can be shared, the process for sharing information, and the application of guidelines to protect privacy, civil rights and civil liberties.

Law enforcement executives also need to seriously consider and resolve several issues related to specialization and generalization. At one level is the issue of whether the intelligence capacity is viewed as specifically focused on homeland security and the threat of terrorism or whether it is viewed as building "all-crimes, all-hazards" capacity. On the one hand, the need to develop capacity and expertise focused on terrorism can justify a more specialized focus. As the commander of a local police department intelligence unit told us, "what keeps me awake is missing a tip or lead suggesting an Al Qaeda-type attack." On the other hand, the results of this study, combined with prior studies, suggests the potential power of the "all-crimes, all-hazards" focus. Prior research demonstrates the high level of involvement of terrorist groups in a variety of criminal activity that brings these individuals in contact with SLT agencies (Damphouse and

Smith, 2004; Smith et al. 2002; Hamm, 2005). The present study indicates a high proportion of Suspicious Activity Reports involving all-crimes. These results suggest that the continued development of the network of SLT agencies, linked to fusion centers and federal law enforcement and ultimately linked to the Intelligence Community (with appropriate firewalls and privacy safeguards) will be best served through the all-crimes, all-hazards information flow. Additionally, it strikes us that the costs of the investment in intelligence capacity will yield the greatest benefits for SLT agencies when the capacity equips such agencies to address not only terrorism but a range of criminal threats (e.g., organized crime, gangs, violent crime, drugs).

A parallel question of specialization/generalization relates to training and responsibilities within SLT agencies. On the basis of these findings, it appears that most agencies to date have developed intelligence capacity through training of officers and analysts dedicated or at least focused on intelligence assignments. Thus, the respondents to our surveys indicate a fairly high level of knowledge and expertise themselves but report much lower levels of familiarity throughout the organization. Again, this is similar to early stages of community- and problem-oriented policing when specialist officers were tasked with implementation but the majority of officers and supervisors focused on so-called "real policing." The danger is that the intelligence function becomes a specialized function divorced from the larger organization, what Toch and Grant (1991) once referred to as an "innovation ghetto." The risk is that information flow from street-level officers and investigators to analysts does not occur. Similarly, analysts do not fully understand the needs of officers and investigators. This, too, suggests the need for broad training on the intelligence function, the role of analysts, and ILP.

The development of a national network of 72 fusion centers (as of this writing) represents a monumental undertaking and achievement. Yet, there has been criticism of the fusion centers

in two broad areas: Fusion center operations[39] and the protection of civil liberties[40]. The results of the current study suggest that the fusion centers are playing a critical role in the nation's domestic intelligence capacity and could play an even more important role in the future. The co-location of personnel from SLT, federal law enforcement and, in some cases, the private sector appears to mitigate some of the historic, cultural, and organizational barriers to information sharing. Consequently, the fusion center's occupy an organizational or network "space" that is "closer" to both federal law enforcement and the SLTs. They appear to be a critical network "node" for the movement of information and intelligence "up-from" and "back-to" the local level. Further, the survey results and case studies reflect the specialized expertise in terms of both human capital (analysts) and technology that many SLT agencies will never attain (with the exception of large metropolitan departments). The fusion centers are already displaying an impressive range of information sources and high frequency actionable intelligence products. Based on these findings, the loss of these fusion centers would result in both a loss of analytic capability and a disconnect between SLT and federal law enforcement and ultimately the intelligence community. Consequently, these results appear to call for continued investment and development of the network of fusion centers.

Perhaps the most critical point for successful intelligence is the quality of the analysis. The need for continual training of analysts, particularly in the area of critical thinking, and the recognition that analysts are practicing professionals – not simply "civilians in the intelligence unit" – are among the factors which need to be recognized and address by law enforcement

[39] Masse, Todd, Siobhan O'Neil, and John Rollins. (2007). *Fusion Centers: Issues and Options for Congress*. Washington, DC: Congressional Research Service.

[40] German, Michael. (undated). What's *Wrong With fusion Centers?*.Washington, DC: American Civuil Liberties Union.

leaders. Greater attention by management needs to be provided for the professional development of intelligence analysts in order to increase the quality and utility of analytic outputs.

Future Research

As noted previously, there have been significant developments in law enforcement intelligence since this survey was administered: New standards and guidelines from the Global Intelligence Working Group and the Program Manager's Office for the Information Sharing Environment; training and technical assistance on civil rights and privacy; new initiatives for training and development of the Nationwide Suspicious Activity Reporting Initiative; self-assessments by fusion centers on the Baseline Capabilities including technical assistance for all fusion centers on this assessment; and the creation of the Fusion Centers Directors Association. Other more localized initiatives have also occurred. As a result, this same survey administered today would likely produce somewhat different results. Nonetheless, this first collection of baseline data is important for future comparisons and identifying critical issues.

Given the nature and sudden emergence of law enforcement intelligence practices, it is reasonable to assume that a significant portion of the persons that did not respond to the survey were likely re-assigned and no longer responsible for the intelligence function or were newly appointed and had little to any knowledge of such practices. These transitions certainly pose significant challenges for a building intelligence capacity as there is a steep learning curve for understanding policy issues, civil rights concerns, and information sharing opportunities that have to be understood. However given such circumstances, the responses that comprise the present study are thought to be the most valid from the available population of key personnel.

The low response rate presented a challenge for the current study. Although multiple efforts were made to contact respondents and encourage participation, it was still difficult to increase the response rate. The length of the survey was certainly an issue as not only was there over 100 questions asked, but many of the questions had 20-25 response options. In addition, because of the turnover as well as that multiple personnel were selected from a single agency, often a single respondent completed the survey on behalf of the agency. The length of the survey, however, provided us with rich context on a wide variety of critical intelligence issues and the results, although exploratory, provide a good introduction to intelligence practices in the United States.

The case studies provided environments where developed intelligence practices could be observed to provide valid contexts for the issues discussed in the current study. While these environments were greatly beneficial for the current study, examining an environment specifically at the local level where intelligence-practices are still being developed would have also benefited the current study. By not including a more representative environment of intelligence practices, the current study lacks specific insight as to how certain relationships are evolving. In addition, it would have been beneficial to have been able to spend more time at the fusion centers studied in order to develop some of the ideas even further. For example, the regional centers in Florida are critical to the intelligence successes there, but we were unable to examine variations in the connections across these regional centers, how they have had to adapt because of regional differences, and how the nature of crime, terrorism and hazard concerns faced in a region might impact the nature of their relationship.

Although this study provides some keen insights into the status of intelligence practices in the United States, it is an exploratory study and there is still a significant need for additional

research to better understand the transition to integrating intelligence work into strategic and tactical decisions. There should be a significant commitment to more completely examine the work of state and major urban area fusion centers. This study looked closely at three—chosen because the survey respondents and subject matter experts identified them saw as fair opportunities to explore the concerns highlighted in this study more closely. There are, however, 72 fusion centers across the country, and thus a need to better understand whether the work identified here is representative of what is occurring elsewhere in the country, but importantly, how variations in critical variables—such as resources that are available, philosophical differences, structural and historical issues, and geography impact the nature of relationships and outputs of fusion centers.

Law enforcement has changed dramatically over the last thirty years, impacted by the philosophical shifts to community and problem-oriented policing. Intelligence-led policing is a logical and important extension of these changes. We saw clear evidence of the fusion centers using a "problem solving" approach in designing new policies and practices, conducting survey work and analysis to identify strategic needs and then crafting policies based on their findings and evaluating whether or not the changes had any impact. We suspect that fusion centers are implementing a variety of strategies to meet the demands of their external environment, overcome perceived weaknesses in service delivery, or in response to a specific need or identified service gap. In addition, we would suspect that fusion centers would embrace the opportunity to implement new strategies if funding was made available to address specific issues. An evaluation component of these strategies would be critical to better understanding what works and what is promising in terms of pushing intelligence practices forward.

Just as there is a need to examine ILP at the fusion center level, there is a similar need to examine ILP at the SLT level. Beyond a recognition of the term ILP, the current findings suggest there is confusion on what ILP means and what it would look like if an agency fully adopted this model. Yet, the results also reveal agencies like Las Vegas Metro that have fully adopted this philosophy. Research is needed to understand this variation across agencies as well as in-depth understanding of the nature, structure, costs, and benefits of ILP at the agency level.

This research also concluded that a large amount of information is being shared across institutions, and importantly, the respondents indicated that a significant number of analytic products are being produced and shared every month. It is difficult for agencies to make full use of these products simply because there is such an overwhelming amount of information. It would be of considerable value to first attempt to better understand the type of intelligence that is being shared within these analytic products, perhaps content analyzing a good sample of products, particularly to determine if they are operationally "actionable". Moreover, it would be important to ask SLT respondents what products are the most useful to them and why, and also to identify any strategies that exist to make the processing of this information more efficient and useful. This is particularly important because the majority of law enforcement agencies do not have adequate resources or personnel to evaluate this information.

Finally, although we are able to provide some insights into the formal communication networks, there would also be value to in examining informal communication systems and the feedback mechanisms in these systems that promote or hinder information sharing. What network ties exist and are absent across organizations, how is intelligence and procedures related to intelligence distributed across these ties, and what factors (e.g., size of agency, geographic proximity, agency reputation) influence the functioning of these network ties? The examination

of these informal networks would be significant because they provide an additional way for homeland security and intelligence officials to promote a necessary understanding of the procedures that need to be followed for better information sharing. For example, Lessons Learned Information Sharing (llis.gov) completed a study in December 2005 that examined information and intelligence sharing requirements (LLIS, 2005). LLIS convened four focus groups with subject matter experts on this topic, and solicited feedback from other key members through its website. There were several important findings regarding information sharing and training needs, but the finding that both informal and formal networks have been established to address limitations in guidelines and process is particularly important. This finding supports other NIJ-sponsored law enforcement research that demonstrates sophisticated informal networks for information sharing (Chamard, 2003; Roberts and Roberts, 2006; Weiss, 1998). We believe that would be great value in documenting these networks.

References

Bayley, David H. 1985. Patterns of policing: A comparative international analysis. New Jersey: Rutgers University Press.

Bayley, David H. 1976. Forces of order: Police behavior in Japan and the United States. Berkeley, CA: University of California Press.

Bennett, Richard. 2004. "Comparative criminology and criminal justice research: The state of our knowledge." Justice Quarterly, 21 (1): 1-21.

Brick, J.M. and G. Kaffen. 1996. "Handling missing data in survey research." Statistical Methods in Medical Research, 5 (3): 215-238.

Bruneau, Thomas C., and Steven C. Boraz. 2006. Reforming intelligence: Obstacles to Democratic control and effectiveness. Austin, Texas: University of Texas Press.

Carter, David. 2004. Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies. Washington D.C.: U.S. Department of Justice.

Chalk, Peter and William Rosenau. 2004. Confronting the "Enemy Within:" Security intelligence, the police, and counterterrorism in four democracies. Santa Monica, California: RAND Corporation.

Chamard, Sharon E. 2003. Innovation-Diffusion Networks and the Adoption and Discontinuance of Computerized Crime Mapping by Municipal Police Departments in New Jersey. PhD dissertation, Rutgers University.

Chermak, Steven and Alexander Weiss. (2000). Identifying Strategies to Market the Police in the News. (Final Report). US Department of Justice: National Institute of Justice.

Cilluffo, F.J., J.R. Clark, and M.P. Downing. (2011). Counterterrorism Intelligence: Law Enforcement Perspectives. Research Brief. Washington, DC: Homeland Security Policy Institute.

Closs, D.J. and E.F. McGarrell. 2004. *Enhancing Security Throughout the Supply Chain.* Washington, DC: IBM Center for The Business of Government.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. 2005. Report of The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Available on the WWW at http://www.wmd.gov/report/.

Cooney, Mikaela, Jeff Rojek, Robert J. Kaminski. 2011. "An Assessment of the Utility of a State Fusion Center by Law Enforcement Executives and Personnel." IALEIA Journal, 20 (1): 1-18.

Damphousse, Kelly R. and Brent L. Smith. 2004. "Terrorism and empirical testing: Using indictment data to assess changes in terrorist conduct." Sociology of Crime, Law and Deviance, 5: 75-90.

Davies, Philip H.J. 2004. "Intelligence culture and intelligence failure in Britain and the United States." Cambridge Review of International Affairs, 17 (3):

Davis, Lois M., K. Jack Riley, Greg Ridgeway, Jennifer Pace, Sarah K. Cotton, Paul S. Steinberg, Kelly Damphousse, and Brent L. Smith. 2004. When terrorism hits home: How prepared are state and local law enforcement? Santa Monica, California: RAND Corporation.

Department of Homeland Security. 2008. Baseline Capabilities for State and Major Urban Area Fusion Centers. Washington D.C.: U.S. Department of Justice.

Florida Fusion Center [FFC]. (2010a). Interview with Florida Fusion Center Personnel. Conducted on February 4. Tallahassee, FL.

Florida Fusion Center [FFC]. (2010b). Interview with Florida Fusion Center Personnel. Conducted on February 4. Tallahassee, FL.

General Accounting Office. 2007. Numerous Federal Networks used to Support Homeland Security Need to be Better Coordinated with Key State and Local Information Sharing Initiatives. Washington, DC: General Accounting Office.

General Accounting Office. 2006. Homeland Security guidance and standards are needed for measuring the effective of agencies' facility protection efforts. Washington, DC: General Accounting Office.

General Accounting Office. 2005. Risk management: Further refinements needed to assess risks and prioritize protective measures at ports and other critical infrastructure. Washington DC: General Accounting Office.

General Accounting Office. 2003. Efforts to improve information sharing need to be strengthened. Washington, DC: General Accounting Office.

Godson, Roy. 1988. Comparing foreign intelligence: The US, the USSR, the UK, and the Third World. Washington DC: Pergamon-Brassey.

Global Intelligence Working Group. 2005. National criminal intelligence sharing plan. Washington D.C.: U.S. Department of Justice.

Global Intelligence Working Group. 2003. Executive steering committee meeting summary. Washington D.C.: U.S. Department of Justice.

Hamm, M. (2005). Crimes committed by terrorist groups: Theory, research and

prevention. Washington, DC: National Institute of Justice.

Hastedt, Glenn P. 1991. "Toward the Comparative Study of Intelligence." Conflict Quarterly, Summer: 55-73.

Herman, Michael. 2001. Intelligence services in the information age: Theory and practice. London: Frank Cass.

House Committee on Homeland Security. 2009. Homeland security intelligence: its relevance and limitations. Washington D.C.: U.S. House of Representatives.

Hu, Paul Jen-Hwa, Chienting Lin, and Hsinchun Chen. 2005. "User acceptance of intelligence and security informatics technology: A study of COPLINK." Journal of the American Society for Information Science and Technology, 56 (3): 235-244.

International Association of Chiefs of Police. 2002. Recommendations from the IACP Summit, Criminal intelligence sharing: a national plan for intelligence-led policing at the local, state and federal levels. Available from http://www.theiacp.org/LinkClick.aspx?fileticket=fkdp7AX%2FFac%3D&tabid=298.

Johnston, Rob. 2005. Analytic culture in the US intelligence community: An ethnographic study. Washington, DC: Central Intelligence Agency.

Lessons Learned Information Sharing. 2005. *LLIS* Intelligence and Information Sharing Initiative: Homeland Security Intelligence Requirements Process. Washington DC: Department of Homeland Security.

Masse, Todd, Siobhan O'Neil, and John Rollins. 2007. Fusion Centers: Issues and Options for Congress. Washington, DC: Congressional Research Service.

Mastrofski, S. 1998. Police agency accreditation: a skeptical view. *Policing: an international journal of police strategies & management, 21, 202-205.*

Mawby, Rob. 1999. Policing across the world: Issues for the twenty first century. London: UCL Press.

McDaniel, M. C., Shenouda, E., and Bustria, M. J. (2008). The functional desks as collaborative mechanisms in the michigan intelligence operations center. *Homeland Security Affairs*, Supplement No. 2., 1-18.

McGarrell, Edmund, Steve Chermak, and Joshua Freilich. (2007). "Intelligence Led Policing as a Framework for Responding to Terrorism," Journal of Contemporary Criminal Justice, 23 (2): 142-158.

McNamara, Thomas F. 2006. Information Sharing Environment Implementation Plan. Washington DC: Office of the Director of National Intelligence.

National Commission on Terrorist Attacks Upon the United States, 2004. The 9/11 Commission Report. Available from the WWW at: http://www.9-11commission.gov/

O'Connell, Kevin. 2004. "Thinking About Intelligence Comparatively," *Brown Journal of World Affairs*, 11 (1): 189–199.

Osborne, D. and T. Gaebler. 1992. *Reinventing Government.* Reading, MA: Addison Wesley.

President's National Strategy on Information Sharing (2007). Available from the WWW at: http://www.whitehouse.gov/nsc/infosharing/index.html

Riley, K. Jack and Bruce Hoffman. 1995. Domestic terrorism: A National assessment of State and Local law enforcement preparedness. Santa Monica, California: RAND Corporation.

Riley, K. Jack, Gregory F. Treverton, Jeremy M. Wilson, and Lois M. Davis. 2005. State and local intelligence in the war on terrorism. Santa Monica, California: RAND Corporation.

Roberts, Aki and John M. Roberts. 2006. Police innovations and the structure of informal communication between police agencies: Network and LEMAS Data. Washington, DC: National Institute of Justice.

Saari, Shane, C. 2010. Fusion Centers: Securing America's heartland from threats. (Master's Thesis, Naval Postgraduate School). Retrieved from http://www.hsdl.org/?view&did=11009.

Smith, Brent L. 1994. Terrorism in America: Pipe bombs and pipe dreams. New York: State University of New York Press.

Smith, Brent L. and Kelly R. Damphousse. 1996. "Punishing political offenders: The effect of political motive on Federal sentencing decisions." Criminology, 34 (3): 289-321.

Smith, Brent L. and Kelly R. Damphousse. 1998. "Terrorism, politics and punishment: A test of structural-contextual theory and the 'liberation hypothesis.'" Criminology, 36(1): 67-92.

Smith, Brent L., Kelly R. Damphousse, Freedom Jackson, and Amy Sellers. 2002. "The prosecution and punishment of international terrorists in federal courts: 1980-1998." Criminology & Public Policy, 1(3): 311- 338.

Smith, Brent, Kelly Damphousse, and Paxton Roberts. 2006. Final Technical Report: Pre-Incident Indicators of Terrorist Incident: The Identification of Behavioral, Geographic, and Temporal Patterns of Preparatory Conduct (pp. 1-100). National Institute of Justice. Washington, DC: Office of Justice Programs.

Smith, Brent L. and Gregory Orvis. 1993. "America's response to terrorism: An empirical analysis of Federal intervention strategies during the 1980s." Justice Quarterly, 10: 661-681.

Smith, Brent L. and Kathryn D. Morgan. 1994. "Terrorists right and left: Empirical issues in profiling American terrorists." Studies in Conflict and Terrorism, 17: 39-57.

Toch, H. and Grant, J.D. *Police as Problem Solvers* (Revised edition). American Psychological Association (APA Books), 2005.

Treverton, Gregory F. 2005. The next steps in reshaping intelligence. Santa Monica, California: RAND Corporation.

Treverton, Gregory F., Seth G. Jones, Steven Boraz, and Phillip Lipscy. 2006. Toward a theory of intelligence: Workshop report. Santa Monica, California: RAND Corporation.

Weiss, Alexander. 1994. "Identifying Sources of Error in Informant Reports: A Confirmatory Measurement Model Approach." Evaluation Review, 18 (5): 592-612.

Weiss, Alexander. 1998. Informal information sharing among police agencies. Washington DC: National Institute of Justice.

Dissemination of Research Findings (to date)

Publications

Carter, Jeremy and Steven Chermak. [forthcoming, 2011]. "The Role of Fusion Centers as Sources of Information." In C. Lum and L.W. Kennedy (Eds). Evidence-Based Counterterrorism Policy. New York: Spring-Verlag

Presentations

Carter, Jeremy and Steven Chermak. 2011. The Role of Fusion Centers as Sources of Information. American Society of Criminology. Washington, DC. November

Dissertations

Jeremy Carter (Member). 2011. "Police Innovation: Exploring the Adoption of Intelligence-Led Policing. Michigan State University.

Publications and presentations resulting from this award should be listed, including the full journal citation, scientific conference and location, etc.