Law Enforcement Fusion Centers: Cultivating an Information Sharing Environment while Safeguarding Privacy

Jeremy G. Carter, Ph.D.[1]
Assistant Professor
School of Public and Environmental Affairs
Indiana University - Purdue University Indianapolis
801 W. Michigan Street, BS 4081
Indianapolis, IN 46202
Office: (317) 274-4170

David L. Carter, Ph.D.
Steve Chermak, Ph.D.
Edmund McGarrell, Ph.D.
School of Criminal Justice, Michigan State University

Abstract
The national network of fusion centers, of which there are currently 78 nationwide, was created in response to the terrorist attacks of September 11, 2001 and continue to play an integral role in contemporary law enforcement. Their mission, put simply, is to facilitate information sharing across disparate agencies and organizations. Despite a significant presence within the law enforcement landscape, fusion centers have received relatively minimal scholarly attention. This limited literature alludes to operational challenges and public concerns that inhibit fusion center effectiveness. More specifically, little information is known about how fusion centers develop relationships with external partners as well as institute mechanisms to safeguard against violations of individual privacy. The present research employs a combination of national survey data and three in-depth case studies of fusion centers in Florida, Nevada, and Michigan to provide initial answers to these questions. Implications for improved policy and practice are discussed.

Keywords
Fusion center, Law enforcement intelligence, Information sharing

Citation:
Carter, J. G., Carter, D. L., Chermak, S., & McGarrell, E. (2016). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police and Criminal Psychology*. DOI: 10.1007/s11896-016-9199-4.

Link:
http://link.springer.com/article/10.1007/s11896-016-9199-4

[1] Corresponding Author

Law Enforcement Fusion Centers:
Cultivating an Information Sharing Environment while Safeguarding Privacy

1. INTRODUCTION

In the wake of the terrorist attacks of September 11, 2001, the need for greater information sharing and increased intelligence capabilities across various law enforcement levels and locales became widely apparent (National Commission on Terrorist Attacks, 2004). State and major urban area fusion centers, of which there are currently 78 nationwide, have been one of the main vehicles for enhancing information sharing by acting as hubs for information and intelligence on terrorist, criminal, and other public safety threats within a particular geographic area (Carter & Carter, 2009a). Though the literature on fusion centers is beginning to take shape, there remains two critically understudied questions that rest at the core of fusion center research and practice. First, how do fusion centers develop relationships with both law enforcement and non-law enforcement organizations? Second, what mechanisms do fusion centers utilize to safeguard against violations of individual privacy? The present research employs a mixed-methods approach to provide initial answers to these questions. More specifically, national survey data is reported to describe these issues and three in-depth case studies of fusion centers in Florida, Nevada, and Michigan are leveraged to identify specific organizational practices.

2. REVIEW OF LITERATURE

2.1 Fusion Centers and the Sharing of Information

Fusion centers are brick-and-mortar entities comprised of representatives primarily from federal, state, and local law enforcement agencies as well as members of the private sector and public organizations. In theory, this diverse composition of organizations is best positioned to

identify and understand threats facing a particular jurisdiction or region. The premise of fusion centers is that information analyzed from diverse sources gleans more accurate intelligence (Clark, 2007) through a "fusion" process resulting from analyzed raw intelligence provided by the disparate organizations (Carter & Chermak, 2012). Dissemination of intelligence products to relevant stakeholders brings the intelligence fusion process full circle and helps to ensure that fusion centers do not operate as silos of information (Ratcliffe, 2008). While the idea of state and regional collaborative centers is not new to law enforcement (Carter & Carter, 2009a), the rise of contemporary fusion centers occurred simultaneous to the emergence of intelligence-led policing (ILP) within the United States (Carter & Carter, 2009b; Chermak *et al*., 2013). In the highly fragmented U.S. law enforcement environment, fusion centers are positioned to enhance ILP practice (Carter, 2015). With currently 53 state and 25 major urban area fusion centers spread throughout the country and U.S. territories, each center is designed to cover a specific geographic area, connecting local, state, and federal law enforcement, emergency services, transportation services, and a wide variety of private businesses within their state or geographic area. Further, these centers serve as a force multiplier that enhances the analytic capabilities within their areas of operation (Saari, 2010). Each jurisdiction has distinctive and diverse needs. As a Congressional Research Service report stated, "There appears to be no 'one-size-fits-all' structural or operational model for fusion centers" (Rollins, 2008, pp.18). In fact, a large number of centers have undergone changes in structure and focus since their inception in order to meet the needs of their constituents.

Few scholars have gained access to fusion centers and begun to examine the intelligence process within these organizations. Graphia-Joyal (2010) employed a qualitative study that included 49 interviews at four fusion centers in the northeast region of the U.S. Her study concluded that centers had yet to develop a robust analytical capability. Rather, they had been

providing investigative case support that lacked analysis to inform operational, tactical, or strategic action (the goal of intelligence analysis). This lack of analysis with regard to intelligence production has been echoed by other scholars examining intelligence-led and analytic-driven policing. In their ethnographic study of four intelligence units from the United Kingdom, Innes, Fielding, and Cope (2005) concluded that analytic functions within these units were, in reality, a repackaging of traditional policing data and information. The intelligence units examined attempted to lend a degree of objectivity to the products created as a result of an analytic process that lacked any true scientific application. This may be the result of what Cope (2004) contends to be a cultural disconnect between analysts and police personnel as well as a general lack of understanding as to how analysis can influence police practice. Similarly, through 86 interviews with varying police intelligence personnel from six agencies in Canada, Sanders, Weston, and Schott (2015) observed that intelligence production and information sharing were steeped in rhetoric and contingent upon an agency's culture to embrace innovative analyses. Though each agency appeared to institutionalize intelligence-led policing, actual intelligence analysis and analytic-driven decision making was an exception rather than the rule.

Cooney, Rojek, and Kaminski (2011) provide a more optimistic outlook with respect to information sharing. Using a quantitative survey of local law enforcement personnel in South Carolina, they illustrated the utility of the state fusion center and noted that 75 percent of the police executives found the center to be moderately useful or very useful. A general sense of the applicability of fusion center products to client operations may be challenging given the diversity of end-user needs. This is both a strength and weakness of the fusion center model as these centers are designed to promote information and intelligence sharing across disparate organizations, but this organizational variation creates hurdles for centers to tailor analytic products (Carter, 2015).

A diverse group of end-users is ideal for information collection and dissemination as personnel from different law enforcement environments (i.e., federal, state, local, rural, urban) and sectors (i.e., financial, private business, public health, transportation, emergency management) are able to provide unique information to be integrated into the analytic process. However, many fusion centers currently lack the resources and analytic capacity to create analytic products that are tailored to the unique needs of these diverse groups. As Lewandowski and Carter (2014) observed in their survey of fusion center end-users, this lack of specificity within analytic products can create dissatisfaction and hinder relationships between fusion centers and their end-users as the value fusion centers can provide via their analytic capacity is minimized.

Ratcliffe and Walden (2010) employed a mixed-methodology to examine the volume and frequency of information that flowed from local law enforcement to the state fusion center. Their statistics reported that 48 percent of New Jersey troopers had not communicated with the fusion center and that many of the troopers voluntarily sent information only because they believed it would help their investigation – not because it could have implications for terrorism or other criminality. Within the qualitative portion of their research, Ratcliffe and Walden (2010, pp. 9) found that fusion center services were largely unknown or misunderstood by troopers, with one trooper noting: “I don’t know when to use them, so I don’t use them. I don’t know what they can do for me.” Despite this disconnect, the researchers found some positive outcomes as troopers who did engage the fusion center almost always received the information or intelligence they were seeking.

Ratcliffe and Walden (2010) also indicated that troopers in their study interpreted their role as one that consumes and further distributes intelligence products received from the center, but they had no responsibility for pushing information to the fusion center. In their recommendations

for this gap in information sharing, the authors concluded fusion centers must develop an outreach component to ensure that fusion center partners are not only aware of their services, but also direct them on how to effectively collect and contribute information to the fusion center. Relatedly, scholars have recognized that law enforcement may not understand the utility of fusion centers because the centers need to be more proactive in marketing themselves. Studies have noted that the centers do a poor job of communicating their analytic services (Chermak *et al*., 2010; Graphia-Joyal, 2010) and data availability (Carter & Chermak, 2012). In a similar vein, Cooney *et al*. (2011) found that personnel who had received training about a fusion center's capabilities were more likely to rate the center as useful.

2.2 Private and Public Health Sectors as Fusion Center Partners

To best protect against acts of terrorism and develop comprehensive threat awareness capabilities, fusion centers have been directed to engage the private and public health sectors to establish a process for sharing information (Lessons Learned Information Sharing, 2005). The Program Manager for the Information Sharing Environment (PM-ISE) (2006) observed that the private sector can be a rich resource of information. Many large corporations have sophisticated security operations that monitor global threats to their facilities, products, and personnel. This information is more diverse than that traditionally captured by law enforcement and can provide for more robust analytic products. Similarly, the private sector is a "need to know" consumer of law enforcement intelligence as 85 percent of the critical infrastructure in the United States is operated within the private sector (Homeland Security Advisory Council, 2005). Moreover, the private sector has a large personnel force that could be leveraged to significantly increase the capacity for fusion centers to receive reports of suspicious activity.

In 2011 the *Health Security: Public Health and Medical Integration for Fusion Centers* document was published by the U.S. Department of Justice to provide a roadmap for integrating public health information into the fusion process. This initiative urged fusion centers to work with public health partners to conduct ongoing risk assessments and mutually access relevant and timely information in support of threat awareness. The integration of public health partners positions health information to be readily available in an environment where analytic techniques are commonplace for strategic planning and identifying threats (Carter & Rip, 2013). This collaborative effort is believed to enhance the preparedness level of public health practitioners across the country, while supporting the fusion center all-hazards approach to prevention, protection, and response (Riegle, 2009).

A report from the Centers for Disease Prevention and Control (2011, pp.55) notes the benefit of public health participation in fusion centers:

> "[Fusion center participation enhances…] the ability to conduct multijurisdictional, multidisciplinary exchange of health-related information and situational awareness data among federal, state, local, territorial, and tribal levels of government, and the private sector. This capability includes the routine sharing of information as well as issuing of public health alerts…in preparation for, and in response to, events or incidents of public health significance."

Moreover, contemporary policing has recognized the importance of integrating public health information into policing strategies to further reduce crime, disorder, and calls for service while improving the quality of communities (Wood *et al*., 2015). Such strategies are rooted in the movement of harm-focused policing that seeks to facilitate public safety through a more expansive view of the role of police while "An emphasis on harm would provide a welcomed focus for intelligence-led policing" (Ratcliffe, 2015, pp.179). The inclusion of health-related information in fusion centers is just one aspect that raises concerns of the legality and privacy issues surrounding law enforcement information sharing. Related concerns have been voiced by critics of fusion

centers and are thus an emphasis of the present study to provide insight into how fusion centers attempt to safeguard against these concerns.

2.3 Privacy Concerns in the Information Sharing Environment

Law enforcement generally, and fusion centers more specifically, have access to vast amounts of diverse data from law enforcement and open sources (Pearsall, 2010). This effort to collect large amounts of information and data, combined with efforts to develop mechanisms for secure access and sharing, have led civil rights advocates to worry that this increase in data and federal security clearances serves as proof of far-reaching law enforcement initiatives to collect and secretly share personal information (Taylor & Russell, 2012). Such concerns are fostered by the assumption that fusion centers operate as a pre-emptive law enforcement action wherein information is collected without the presence of a reasonable suspicion (Masse & Rollins, 2007) and that such data is readily available to an array of law enforcement and non-law enforcement personnel who could use this data for purposes of unlawful discrimination[2] (Monahan & Palmer, 2009).

Critics of fusion centers contend that fusion centers have developed ad-hoc secure sharing portals (i.e., web-based databases or internal databases with credential login) to serve as mechanisms for sharing information with varied end-users. As these sharing systems are largely developed and operated by fusion centers themselves with no overseeing authority, concerns may exist surrounding background checks for access to sensitive information, expectations for information and data usage, and processes to review, renew, or revoke continued access. Such an approach is largely necessitated by a confound of security and legal requirements that apply to

[2] Racial profiling, violations of privacy and the abridgement of First Amendment protections of expressive activity are the most commonly expressed concerns.

some users (such as law enforcement personnel) but not others (such as private sector personnel) (Monahan & Palmer, 2009). Moreover, critics perceive an overall lack of transparency with respect to how fusion centers actually share information, who has access to information, and how information is used by different partners that may include, for example, partners from the financial banking sector, critical infrastructure (transportation and energy), public schools, and public health (hospitals and state health organizations).

The involvement of non-law enforcement partners in fusion centers has been a source of contention as such participation is thought to be questionable as to whether or not the government has the right to view, analyze, and disseminate the personal data collected by these organizations (Electronic Privacy Information Center, 2008). Moreover, it has been alleged that the involvement of private organizations in the fusion center process allows for fusion centers to circumvent the law by operating through a private entity (Monahan & Palmer, 2009) and that such partnerships may provide opportunities for corruption and the misuse of information (Newkirk, 2010). In response, fusion centers claim they have rigid privacy policies which have been independently reviewed by designated U.S. Department of Homeland Security (DHS) personnel as well as having required non-disclosure agreements with all fusion center personnel and partners.

The creation of DHS' *Nationwide SAR Initiative* to report suspicious activities that may be precursor behaviors for acts of terrorism has further fueled fusion center privacy and civil rights concerns (Harper, 2009). Privacy advocates contend that this initiative opens the door for racial profiling (German & Stanley, 2008) and the unlawful surveillance of citizens (Monahan, 2011, Monahan & Regan, 2012). Others have gone as far to allege the collection of suspicious activity reports may equate to the identification of dangerous classes of people (Taylor & Russell, 2012) resulting in tensions between these classes of individuals and the police (Deflem, 2004). Kurlander

(2005) notes that legal mechanisms have slowed such initiatives. However, German and Stanley (2008) contend that the federal government allows states to exempt fusion centers from these legal constraints. To remedy these issues, it has been suggested that fusion centers employ an independent authority to ensure centers are operating within constitutional and legal bounds and that there exists a system of accountability (Rollins & Connors, 2007; Taylor & Russell, 2012). Despite these concerns and calls for systems of checks and balances, research has yet to quantify the extent to which fusion centers safeguard against privacy concerns and develop effective practices for protecting civil rights. The present research provides actionable findings to inform this shortcoming.

3. Methods

To date, much of the fusion center research has employed survey methodologies (Carter, 2015; Chermak *et al*., 2013; Lewandowski & Carter, 2014; Cooney *et al*., 2011). While these studies have provided much-needed scholarly guidance, they lack contextual detail necessary to explain nuances of these complex organizations (Carter, 2015). Chermak, *et al*. (2013) note that while their study allows them to identify patterns of information sharing that hold across various fusion centers, it does not allow them to dig deeper into the reasons for their findings. Carter (2015) urged for such in-depth studies to better identify the determinants of information sharing. Few studies have explored fusion center functioning through in depth interviews; those that do have shed valuable insights. As Graphia-Joyal (2010) noted, interviewing personnel allowed for exploration of "poorly understood contexts and constructs" (pp. 362), providing a richer set of data that help inform future policy and research. Law enforcement fusion centers are designed to facilitate information sharing across, and analyze information from, disparate organizations. This

mission involves a range of complex and nuanced practices that have received minimal scholarly attention to date. The present study seeks to illustrate these practices and provide unique context as to how fusion centers engage in information sharing with diverse organizations and make efforts to safeguard against privacy concerns. To this end, the present study employs a mixed-methods approach consisting of a national survey of fusion centers and three in-depth case studies conducted at fusion centers in Florida, Nevada, and Michigan within the same time period.

3.1 Survey of Fusion Centers

Survey data were gleaned from a larger project[3] and include responses from 96 fusion center personnel.[4] The survey sample of fusion center respondents comprised of persons who attended the National Fusion Center Conference (NFCC). Attendees of the NFCC include fusion center directors, administrators, and upper-level operational personnel. This sampling strategy, which includes nationally representative fusion center personnel, was chosen for three reasons. First, in attending this conference, these persons were identified by their respective fusion center as a key representative of their organization. Second, as a result of their selection on behalf of their center, this sample includes personnel who have a working knowledge of key issues tied to their fusion center and its intelligence capacity. Thus, these persons are best able to address the organizational capacity of their centers. Third, these persons' awareness of the contemporary intelligence structures, requirements, and formal communication networks involved in fusion

[3] Grant award number 2008-IJCX-0007 from the National Institute of Justice, US Department of Justice.

[4] The most responses from within a single fusion center was three, which occurred for two centers. Ten fusion centers had two respondents while the remaining 70 fusion centers in the study had a single survey respondent. The findings to follow present responses from all 96 survey respondents as this approach was deemed most appropriate by the research team to reflect perceptions of fusion center practices. For diagnostic purposes, a complex survey design in STATA (ICv14) was employed to adjust for clustered responses from respondents within the same fusion center. Not surprisingly, given minimal multiple responses from the same center and the present research's focus on descriptives, the findings were consistent.

centers increases the likelihood that they will have direct knowledge about the strengths and weaknesses of these issues. This sampling approach to target key knowledgeable personnel in law enforcement organizations has been utilized in police research focused on specialty personnel when examining similar contemporary issues, such as police assigned to cybercrime (Bossler & Holt, 2012; Holt & Bossler, 2012).

Table 1 displays descriptive information of the fusion centers represented in the current study. Responses were reported predominantly by administrators (51%) and supervisors (20%). This is beneficial to the validity of the responses, as these persons are most likely to have an accurate perception of the activities that occur within the center as they oversee daily operations and strategic planning. The modal response category for tenure at the fusion center was one to three years. This is not outside the norm, given the nature of turnover within fusion centers as agencies rotate assigned personnel. In the case of newly assigned personnel, having been assigned to the fusion center for only one to three years may not be indicative of a lack of knowledge, since assigned personnel are typically chosen as a result of their experience in intelligence operations within their home agency.

[Insert **Table 1. Fusion Center Respondent Descriptives** approximately here]

3.2 Case Studies

Greene (2014) challenged scholars to balance quantitative prediction and qualitative context in policing research. He argued the evidence-based movement, while beneficial for a number of reasons, diluted the "cognitive lens" (pp. 193) through which meaning could be gleaned from research to inform practice and future inquiry. He further contended that such context must

be captured through qualitative methods. The present study embraces this approach through in-depth case studies of three fusion centers; Florida Fusion Center (FCC), Southern Nevada Counter-terrorism Center (SNCTC), and Michigan Intelligence Operations Center (MIOC). A case study approach is most appropriate for this research given little is known about the organizational practices of fusion centers and their highly complex structures (Fitzpatrick, Sanders, & Worthen 2003). Each of these centers became operational in 2007, are designated as "primary" centers by the U.S. Department of Homeland Security[5], and focus on counter-terrorism, all-threat, all-crimes, and all-hazards. The FFC is operated solely by the Florida Department of Law Enforcement (FDLE) while the MIOC is co-operated by the Michigan State Police (MSP) and National Guard. The SNCTC is operated by the Las Vegas Metro Police Department (LVMPD). These three centers display welcomed variation across their organizational structure and geographic location. While the FCC and SNCTC exhibited organizational consistency over time, the MIOC was undergoing an administrative transition at the time of study. This transition period provided an opportunity to observe operational challenges that are likely experienced by the broader national network of fusion centers (i.e., change in management and other personnel; developing new policies and procedures; staff learning new job responsibilities, developing new information sharing partnerships).

Though the FCC, SNCTC, and MIOC are only three of 53 officially recognized primary fusion centers, their organizational capacity mirrors those of the general fusion center population. A report by the U.S. Department of Homeland Security (2014) documented the organizational capabilities and practices of each fusion center nationwide and quantified operational scores for each center across a range of metrics. Based on these metrics, the three fusion centers examined

[5] http://www.dhs.gov/fusion-center-locations-and-contact-information

in the case studies each received an overall rating comparable to centers across the country. This rating lends credence to the generalizability of the findings to be presented in the current study as the operations and practices of the center of study are consistent with those nationwide. More specifically, the likeness of the fusion centers sampled in the present study to those of the greater population of fusion centers suggests promise for the findings to be applicable for improved practice for fusion centers across the United States. The decision to conduct case studies at these three centers was the result of the research team's contacts with key fusion center staff as well as independent recommendations from subject matter experts.

Following the completion of the national survey of fusion centers, the research team conducted on-site visits with each fusion center to interview administrative and analytic personnel. Interviews were conducted with the use of a semi-structured interview protocol that was developed to explore findings observed in the national survey as well as the aforementioned operational challenges identified in research and federal reports. At each of the three centers, the research team conducted interviews with the fusion center's Director (lead administrator), one supervisor of center operations, one records management person, and two intelligence analysts (one of which was a supervisory analysts at each center) for a total of five interviews per center. In total, the majority of interview time, an average of 90 minutes per interview, was conducted with fusion center directors, administrators, and supervisory analysts as the research team was focused on gathering data regarding key fusion center practices, policies, and initiatives. Upper-level management personnel were best positioned to inform the research team on these issues.

3.3 Analytic Strategy

Survey responses are presented in figure format for illustrative purposes. Valid percent is presented along the x-axis. Means and standard deviations are also reported in the tables below each figure. Reliability coefficients (alpha) are provided to demonstrate internal consistency across the items presented within groups. Though the items contained within groups, and presented as such, do not reflect any form of latent construct, the use of reliability coefficients assists to affirm that the items reported grouped appropriately for discussion. Qualitative data was captured through investigator field notes and audio recordings of interviews that were later transcribed, managed, and analyzed within theme-identification software (Nvivo v11). Drawing upon a grounded theory approach (Glaser & Strauss, 1999) that allows for repeat constructs, or elements, to emerge in qualitative data in combination with insights provided from previous research, key response traits, indicators, and themes were reviewed and agreed upon by the research team. To enhance the validity of interpretations from the interviews, the research team undertook additional phone and email communications with fusion center personnel occurred to solicit feedback, clarify, and reaffirm the information gathered (King, 1994). Though the research team identified additional information believed to be insightful, only the findings which gained saturation and consensus among those interviewed are reported. Saturation of qualitative findings is a subjective threshold (Fusch & Ness, 2015) with debate surrounding necessary sample size (O'Reilly & Parker, 2013).

The present study sought to establish saturation using three methods. First, case studies were conducted at three unique fusion centers. This allowed the research team to interview persons from diverse environments. Second, different personnel types were interviewed that included administrators, analytic supervisors, and analysts. This personnel diversity allows for the triangulation of individual perceptions of different personnel types to converge on consistent themes (Denzin, 2012) and therefore reinforce the reliability and validity of qualitative findings

(Stavros & Westberg, 2009). Though the bulk of interviews were conducted with upper-management, the perceptions and observations from all personnel were captured and analyzed. Relatedly, the research team employed a saturation grid to cross-tabulate qualitative data across respondents and positions. The use of such grids demonstrate levels of saturation when consistent findings are intersected across people and positions (Brod, Tesler, & Christiansen, 2009).

4. Discussion of Findings

Given the mixed-methodology and the focus of this research to inform fusion center practice and policy, findings are both reported and discussed in this section. The unique insights from the case studies provide contextual nuances for the survey findings reported and are thus discussed in parallel. This section presents findings that illustrate fusion center practices and operational gaps from a national sample and unique practices and lessons learned from three fusion center case studies to inform gaps and challenges identified in the survey findings and previous research. Conclusions, in addition to recommendations for policy, are provided in the subsequent section.

4.1 Cultivating Relationships for Information Sharing: Survey Results

Respondents were asked to indicate how close of a working relationship they experienced for purposes of information sharing with a range of jurisdictions and sectors. Respondents were also asked to indicate their level of satisfaction with these relationships. Figure 1 reports respondents' perceptions of these information sharing relationships as "very close" or "distant." Survey respondents indicated having the closest information sharing relationships with law enforcement organizations; specifically with state (60%) and local (58%) law enforcement

followed by other fusion centers (47%). Given the mission of fusion centers to serve as information hubs, it is reasonable to question why the reported percentages are not higher. Information from the site visit interviews suggest that fusion centers were focusing on getting their structure and processes in place – including the more mundane but time-consuming process of installing secure systems and gaining security clearances. Interviews at each site visit clearly indicated that personnel understood the need to have proactive outreach with agencies in their jurisdictions.

The extent to which these relationships were perceived as "distant" was minimal across each of these law enforcement categories. Interestingly, this is not the case with respect to the private and public health sectors. Respondents reported a "distant" relationship (22%) with the private sector more frequently than a "very close" relationship (15%). Although 31 percent of respondents indicated a "very close" relationship with public health, a relatively large proportion also indicated their relationship with public health as "distant" (18%). Interviews during the site visits found that establishing relationships with the private sector and public health posed information sharing challenges related to privacy for which there was little precedent. Hence, some relationships were started with operational agreements. Information sharing agreements would take longer and were largely dependent on legal advisors.

In terms of satisfaction, fusion centers sampled were generally not very satisfied with their information sharing relationships. Consistent with perceptions of working proximity, respondents rated their satisfaction levels higher among law enforcement partners. Private sector (9%) and public health (13%) were again the sector receiving the fewest positive satisfaction results. Given the overall lack of engagement displayed in Figure 1, these low responses might be linked to lack of interaction with these entities as opposed to specific concerns about these relationships. Moreover, despite few respondents reporting a "distant" relationship with law enforcement

organizations, the overall levels of "very close" relationships are perhaps lower than would be expected given the mission of fusion centers to facilitate information sharing across disparate law enforcement organizations. This holds true for reported satisfaction with other law enforcement organizations as well. These descriptives begin to illustrate the gap between fusion centers and the organizations which they seek to engage in information sharing.

Unique practices to close these gaps and improve relationships were found among the case study fusion centers. The most unique and promising practices gleaned from the case studies focused on fostering relationships with the private sector. These findings are interesting given the survey results reported minimal fusion center interaction and satisfaction with the private sector. It is important to note that the survey occurred as most fusion centers were becoming operational, and thus one would expect weak relationships with private sector. In addition, two of the centers chosen for the case studies (Florida and Nevada) had reached operational maturity. As a result, these two centers had been able to experience the value in such relationships and reached an operational period where such partnerships could be cultivated; as evidenced by the innovations below.

[Insert **Figure 1. Relationships for Information Sharing** approximately here]

4.2 Cultivating Relationships for Information Sharing: Case Studies Findings

Through discussion with the center personnel, the FFC was conscious of these relationship gaps and conducted a "gap analysis" to identify the root problems and develop solutions for improved information sharing. This gap analysis revealed that 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 resources the FFC actually provides. This knowledge shortcoming was coupled with a lack of commitment from local law enforcement executives. An FFC administrator noted this "…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 we [FFC] outline to ensure quality, legality and effectiveness." In addition, the gap analysis identified three barriers to private sector cooperation. FFC personnel explained that private businesses were 1) hesitant to share proprietary information, 2) desired intelligence products that related to their operational environment, and had 3) difficulty in gaining access to government information sharing systems as a result of their non-law enforcement status.

To remedy these shortcomings, the FFC implemented two initiatives. First, a formal intelligence-liaison officer (ILO) program was developed to gain participation and information integrity compliance with local law enforcement. Second, the FFC created the "BusinessSafe" program as an outreach component specifically for the private sector. The ILO program involved the assignment of specific persons to be a designated information sharing point of contact that sends, receives, and integrates information between their agency and the FFC. In addition to sharing information, the ILO is responsible for the legality and integrity of information, communicating FFC resources to their home agency, and communicating their agency needs to the FFC. Though an ILO may be physically assigned to the fusion center, the more common arrangement was for the ILO to perform his or her fusion center responsibilities simultaneously to those of their home agency from their home location. This ILO program also created a mechanism through which the FFC could "market" their resources and capabilities to local law enforcement with the hope of garnering additional support from the ILO's neighboring agencies. As one FFC

interviewee noted, “The ILO program provides a grass-roots approach to developing the much-needed local law enforcement participation in the broader information sharing environment.”

To engage the private sector, the FFC launched the BusinessSafe program that incorporates both website and in-person components. The website is a designated private sector-only secure portal that provides businesses with the necessary tools and resources to facilitate two-way communication with the fusion center. This website hosts a variety of private sector specific fact sheets for businesses to reference that are categorized within specific business areas – such as businesses operating out of ocean ports, theme parks, or sporting events. Private sector partners are able to retrieve these analytic products as well as gain access to threat and security information that the FFC determines is applicable and legal for sharing. This website allows for businesses to push information to the FFC and connect with other designated security personnel from the private sector in their region. To safeguard against individual privacy concerns, legalities of law enforcement information, and the proprietary nature of private sector information, both the FFC and private sector organization would sign memorandums of understanding (MOU) that specifically outlined how information would be shared, stored, and utilized. Participation in the BuisnessSafe program was contingent upon the agreement to this MOU. Private sector partners were also able to engage in in-person meetings with FFC personnel as well as ILO personnel in their specific region. FFC personnel explained that these face-to-face contacts helped to establish relationships and communicate the diverse needs of both parties. At the time of study, the FFC utilized BusinessSafe to disseminate notices regarding breaking news, possible threats, suspicious activity, and specific preparedness techniques pertinent to approximately 4,000 local business partners.

An innovative and comprehensive private sector engagement program was also found with the SNCTC. One of the self-proclaimed "greatest strengths" of the SNCTC was its ability to collect suspicious activity information from the community generally and private sector more specifically. Given Las Vegas' reliance on tourism, the hospitality-dominated business industry in the area, and the interconnectedness of high traffic tourism and the SNCTC's counterterrorism mission, the SNCTC recognized the need to develop a formal relationship with the hospitality industry to serve as a force multiplier. With this in mind, the SNCTC created a formal partnership with the Las Vegas Convention and Visitor Authority (LVCVA). Similarly, the LVMPD entered into a formal agreement with the LVCVA to enhance this private sector initiative. This agreement outlined the responsibility for both organizations to provide certain services in accordance with their respective statutory authority. The LVCVA determined that being a formal and active participant of the SNCTC was a direct benefit to the hospitality industry in Clark County. As part of this agreement, the LVCVA is a member of the board of governors (oversight committee) of the SNCTC and is required to dedicate 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 to which only law enforcement agencies have access. To facilitate this partnership, the LVMPD hired a private-sector specific intelligence analyst dedicated to the interests of the hospitality industry. This analyst is funded by the LVCVA but 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.

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 was a SAR initiative between the University of Nevada Las Vegas Institute for Security Studies, state and local public safety, homeland security agencies, and the SNCTC to develop a terrorism SAR awareness video titled “Nevada’s Seven Signs of Terrorism”. The video - available in both English and Spanish languages - provides an informative summary key behaviors and activities that are characteristic of terrorist planning and preparations. The video used local examples in order for viewers to personally relate to the information. The key to the success of the terrorism SAR video was the fact that hotels in Las Vegas required all employees to view the video; a promising indication of commitment to the partnership between the SNCTC and the private sector hospitality industry.

The MIOC has employed a different model to facilitate direct communication with their diverse stakeholders; a dedicated set of sector-specific telephone source lines. These lines would be direct communication channels for three key sectors: 1) critical infrastructure and key resources, 2) environmental risk, and 3) border security. At the time of study, the Critical Infrastructure and Key Resource Desk (CIKR) was the only operational source line. The environmental risk and border security lines were programs in progress, but would follow a similar model. The CIKR was a telephone source line, with multiple dialing numbers, created to specifically receive and distribute information with the private sector. This point of contact was staffed around the clock with personnel trained specifically with knowledge of the state’s key critical resources and partners (such as car manufacturers). Private partners were able to call the CIKR desk to provide information they believed the MIOC would deem beneficial or to receive information in response to an inquiry. An additional function of this desk was to conduct private sector outreach to promote capabilities of the MIOC. Although private sector liaisons were not formally integrated within the MIOC structure on a full-time basis at the time of study, this desk shared intelligence analytic

products with private sector members on both a proactive and need-to know basis. Personnel staffing the CIKR desk were responsible for reaching out to existing partners to solicit feedback regarding intelligence products and information needs while also making contact with new potential partners that may have been unaware of the MIOC.

In sum, the FFC, SNCTC, and MIOC each exhibited unique practices for cultivating relationships, especially with respect to non-law enforcement partners. These practices took the form of active and dedicated outreach efforts that aligned with fusion center, partner, and local needs. These practices range in scope and scalability and it appears to be incumbent upon individual fusion centers to assess what local partners should be formally involved with the center and what form their outreach efforts should take in attempting to leverage potential relationships. The practices identified here can likely be modified or amended to meet a range of fusion center needs.

4.3 Methods of Sharing Information: Survey Results

The types of information being shared with officers and partners are characterized in three basic ways: Controlled Unclassified Information (CUI), For Official Use Only (FOUO) and Law Enforcement Sensitive (LES). The fusion center that produced the intelligence product is stating the information is not for public distribution and asking that recipients only share the information with those persons who have the "right-to-know" and "need-to-know" the information. Despite these caveats, there is no sanction if the information is shared widely. While virtually all fusion centers have access to classified information, the distribution of these materials is closely monitored because there are both administrative and criminal sanctions if these guidelines are violated.

Just as relationships and initiatives to cultivate information sharing between fusion centers and external organizations are critical to success, so too are the methods through which information and intelligence are disseminated to, and collected from, external organizations are salient to sustained success. In two case studies of fusion center end-users, Lewandowski and Carter (2014) and Ratcliffe and Walden (2010) observed that recipients of fusion center products may become frustrated with formal, bureaucratic processes to receive information and intelligence from fusion centers. While these studies are insightful to understand end-user perceptions, little is known regarding the mechanisms through which fusion centers disseminate information and intelligence products and how such mechanisms are perceived by fusion center personnel. The following findings lend insights into this unknown.

Survey respondents were asked to indicate through which methods their fusion center disseminated information. The results are reported in Figure 2. Generally, respondents reported sharing information through less formal methods. Email (79%), personal contact (73%), and meetings (66%) were the most frequently reported methods. Though less frequent, respondents indicated sharing information via telephone (40%) and fax (20%) as well. Information sharing systems – such as RISS.net and Law Enforcement Online – were reported to be used by 61 percent of respondents. HSIN (operated by DHS), RISS.net (operated by the Bureau of Justice Assistance) and Law Enforcement Online (operated by the FBI) are all secure but unclassified information systems. The Fusion Center Guidelines urge fusion centers to "leverage the databases, systems, and networks available … to maximize information sharing (Global Justice Information Sharing Initiative, 2003, pp.6). These information sharing systems are designed to facilitate the sharing of, and access to, information between fusion centers and external partners. Given the importance of such systems to information sharing, survey respondents were asked to indicate if they had access

to an information sharing system and whether or not they perceived the system to meet their information sharing needs.

As illustrated in Figure 3, there exists a large discrepancy between respondent registered user access to these sharing systems and respondents' perceptions that the sharing systems met their information sharing needs. The Homeland Security Information Network (HSIN) (91%), Law Enforcement Online (LEO) (89%), and Regional Information Sharing System (79%) were the most frequently reported systems to which respondents were registered users. Across all of the systems reported, HSIN was the most positively viewed system with only 20 percent of respondents indicating it met their information sharing needs. Interviews suggest that intelligence personnel and analysts, while having access to all these systems and more, will typically default to the use of one system – often that is a local system rather than the national system. Ironically, a commonly expressed frustration was that HSIN, RISS.net and LEO all required complex configurations of passwords that had to be changed every six months. This stumbling block became sufficiently prominent that representatives from the three systems, met on several occasions with the Criminal Intelligence Coordinating Council to develop processes to have a Single Sign On (SS) for all three systems. Despite a consensus in the value of the SSO, the hurdle could not be cleared. Insights from the case studies help to understand the gap between user access and perceived utility illustrated in Figure 3.

[Insert **Figure 2. Methods of Sharing Information** approximately here]

[Insert **Figure 3. Information Sharing Systems** approximately here]

4.4 Methods of Sharing Information: Case Studies Findings

Contextualizing these descriptive findings are the specific information sharing practices of the three case study fusion centers. Each of the three case study centers had access to Law Enforcement Online and the Homeland Security Information Network. Despite being registered users of these networks, all three fusion centers have created their own secure information sharing portal. In each instance, the fusion center personnel explained that the creation of their own system allowed the fusion center to tailor the system functionality to meet their information sharing needs as well as the needs of their partnering external organizations. These unique, center-specific systems were used to communicate with local partners while national systems (such as LEO and HSIN) were used for communications with other fusion centers. Each center expressed varying levels of dissatisfaction with the national information sharing systems (i.e., HSIN, LEO, etc.). Personnel at each of the centers expressed similar sentiments that these systems were of "basic functionality" and that varying functional aspects could be enhanced to better serve their needs. An issue of common occurrence was that many local agencies – and especially community organizations and private businesses – lacked awareness and access to formal sharing systems as a result of bureaucratic approval processes.

Law enforcement agencies carefully control access to information systems for three basic reasons: (1) concerns about privacy, and consequently, civil liability (2) concerns that sensitive threat information and (3) historical information contained in police records systems simply should not be shared with non-law enforcement personnel. Moreover, each center expressed displeasure with an inability to have a more two-way system of information sharing where fusion centers could

push intelligence products to the community as well as receive raw information and products from outside organizations via the same system. As a result of this one-way nature of formal sharing systems, information pushed to fusion centers from local sources typically occurs via email, telephone, and personal contacts. Such insight confirm the survey findings reported in Figure 2 regarding methods of information sharing as well as the low approval of information sharing systems illustrated in Figure 3.

To remedy the functional shortcomings and bureaucratic processes accompanying national information sharing systems, the FFC and SNCTC created their own center-specific system to share information directly with local partners. The FFC created the Statewide Intelligence Site (InSite) while the SNCTC created the All-Data Virtual Information Sharing Environment (ADVISE). The InSite and ADVISE systems share similar functionality that, as personnel at both centers indicated, are "more user friendly for our clients." Both systems allow for active two-way information sharing between the fusion center and external organizations via secure online web access in addition to hosting access to a range of archived intelligence products, information bulletins, and criminal history data. From an access management perspective, each fusion center reviews applications for, and grants access to, the sharing system. While this process requires certain checks and balances, such as verifying user information and compliance with privacy regulations, the processes for external organizations to gain access to these unique systems – and thus engage in information sharing – are more streamlined and efficient when compared to national systems.

Moreover, personnel interviewed at both the FFC and SNCTC indicated the management of their own sharing systems allowed them to better identify and track the organizations in which they were engaged for information sharing. This allowed both centers to further develop

relationships and initiatives with these external partners as well as develop plans for information collection requirements based on both fusion center and client needs. Though the MIOC utilizes HSIN as their primary sharing system, it decided to integrate a system known as Memex that created compatibility and information compliance with the data systems of their existing law enforcement partners. MIOC personnel interviewed explained that this decision was driven by feedback from external partners who expressed frustration with the HSIN portal. As one supervisor at the MIOC noted, "Our users couldn't simply pull down information we made available or push us information they thought was relevant…Memex made the sharing of information a more functional reality."

4.5 Mechanisms to Affirm Appropriate Intelligence Practices: Survey Results

As noted in the review of literature, fusion centers have been the focal point of criticism regarding individual privacy with respect to the collection and retention of personal identifying information; especially terrorism-related information. Though a salient issue for society in general and fusion center research and practice more specifically, the protection of individual privacy in the fusion center environment has received sparse scholarly attention. To this end, Figure 4 displays the extent to which survey respondents indicated they had mechanisms in place to safeguard individual privacy. The two most frequent mechanisms were a specific policy to guide the sharing of information with external organizations (88%) and a record system that is compliant with 28 CFR Part 23 (88%); the leading regulatory requirement governing the retention of personal identifying information in law enforcement criminal intelligence records systems. Consistency with federal privacy standards (78%), auditing intelligence records (78%), and requiring privacy

policy training (71%) were also quite common among the centers sampled. Interestingly, only 32 percent of respondents indicated they provided privacy training to local law enforcement.

[Insert **Figure 4. Safeguarding Privacy** approximately here]

4.6 Mechanisms to Affirm Appropriate Intelligence Practices: Case Studies Findings

These descriptive findings generally illustrate the steps fusion centers are taking nationwide to safeguard against violations of privacy; however they provide little insight regarding specific practices as to how fusion centers operationalize such safeguards. The three case studies provide detail as to how this is achieved. To begin, each of the case study centers instituted policies and practices that are tailored to a system of check and balances. One of the most common approaches to establishing operational policies to guide the legal collection and handling of information was the establishment of memorandums of understanding (MOU) between the center and formal information sharing partners. The FFC, MIOC, and SNCTC each discussed their MOUs and noted that each included specific language directed to the legal compliance of information collection, storage, and dissemination. Any entity seeking to receive information from the fusion centers – including other law enforcement agencies – must sign the MOU prior to gaining access to information and intelligence products. Each fusion center provided the research team a copy of their MOU for review. Though each MOU varied with respect to references to specific state laws and guidelines, consistent characteristics of these MOUs included direct language guiding the definition of privacy, consent to records audits, maintaining security of information, responsibility for the accurate documentation and dissemination of information, liability for improper dissemination, and the responsibility of the partnering organization to

provide privacy training for each user seeking access to fusion center information. Furthermore, each center examined employs a vigorous privacy policy[6] that is accessible by law enforcement and the general public via the fusion center's website.

Unique practices to safeguard privacy emerged within each center. At the FFC, the Director 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 the FFC or participating agency. The members are individuals with well-established credentials in the fields of criminal justice and/or the law. At the time of study, the CPPAB members are comprised of an American Civil Liberties Union Director from the state of Florida, a retired Special Agent in Charge with the Federal Bureau of Investigation, and a member from the Center for Advancement of Human Rights at Florida State University. The CPPAB reviews and recommends updates or changes to the FFC privacy policy and procedures for protecting civil rights and civil liberties in response to changes in applicable laws, or as otherwise necessary. The CPPAB is consulted to participate in any independent inquiry into complaints of alleged privacy violations and advises the FFC of their findings and any recommended corrective action. The MIOC leverages a similar privacy advisory board comprised of community privacy advocates, privacy-trained law enforcement officers, and a delegate appointed by the Director. Unlike the FFC CPPAB, the MIOC's privacy board is less formal and typically convenes in instances where a privacy complaint has been filed. The FFC CPPAB is a

[6] The Privacy Policy is a national standard required of each fusion center in order to receive federal funding.

more innovative model that should be considered a “best practice” for other fusion centers across the country.

The SNCTC employs a dedicated group of personnel referred to as the “Quality Assurance Section” (QAS). This group of personnel is led by a deputy director of quality assurance (privacy officer) that oversees three sub-groups. The first is the security group that is responsible for the operational and physical security of the center’s 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, 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. Lastly, the performance measurement group tasked to develop and collect the data to measure the ability of the SNCTC to perform its established mission. As it relates to privacy, this group seeks to determine if all operational tasks engaged in by the SNCTC align with the information sharing privacy policy, federal privacy standards, and applicable state and federal laws. Moreover, the QAS is responsible for ensuring compliance of information sharing partners with all applicable policies and laws. Thus, the QAS has regulatory power over the SNCTC as well as external partners seeking to engage with the SNCTC.

5. Conclusions and Implications for Policy

The present study provides unique insights into the operational nuances and challenges faced by fusion centers nationwide as well as a number of insightful mechanisms through which centers can navigate these challenges. At the heart of effective threat prevention, mitigation and response is two-way information sharing among all agencies that have a responsibility for the safety, security and sustained functionality of America's communities. To this end, if processes are not developed to ensure full participation of all information sharing partners, the functional capability of the fusion centers will be reduced. Sampled fusion center personnel indicated efforts to develop relationships with different agencies; especially other law enforcement agencies and a more diverse range of public safety, private sector, and public health organizations. To achieve their goals, these partnerships need to be broadened and substantively sustained. While it is achievable, it is a difficult barrier to overcome.

Comprehensive threat assessments require raw information from diverse sources to maximize validity and reliability of analysis. As such, fusion centers must proactively reach out to both law enforcement and non-law enforcement partners to 1) communicate center resources and capabilities, 2) learn about local intelligence needs, 3) develop local collection requirements to make information sharing more efficient/effective, and 4) develop mechanisms that allow for more efficient two-way information sharing. For fusion centers to be effective, reciprocal information sharing relationships must be developed with law enforcement agencies within the jurisdiction of the fusion center. Findings indicate that the most effective way to accomplish this is through an ILO/FLO program that can build and sustain local law enforcement relationships.

Many aspects of a fusion center's work is different than the typical law enforcement experience. There are different processes, responsibilities and nomenclature. Findings indicate that the role of the fusion center is not intuitively apparent to law enforcement officers nor is the

importance of a trusted, two-way information sharing relationship. A remedy learned from the site visits is the benefit derived from the fusion centers providing training to local law enforcement personnel, intelligence analysts and in some cases relevant private sector employees. Beyond the substantive knowledge that is shared in training programs, important personal contacts are made and the fusion center can be marketed to local law enforcement. This outreach component builds relationships and helps ensure the quality and legal integrity of information provided to the fusion center.

While experience remains limited, findings indicate that there is value to clearly defined public-private partnerships. There remains challenges for information sharing between fusion centers and private entities due to privacy issues. Similarly, some private sector entities are reluctant to share information with fusion centers because of uncertainty related to intellectual property, client privacy, and the brand image. However, where there is clear value to the partnership and a mechanism can be established to address concerns -- such as with the SNCTC -- the value to both partners can be substantial.

The status of law enforcement intelligence in law enforcement agencies appears to be similar to the early development of community- and problem-solving policing during the early 1990s and the developing literature exploring the adoption of intelligence-led policing (Carter, 2016; Darroch & Mazerolle, 2013). Law enforcement officers and executives recognize the importance of intelligence yet the implementation of law enforcement intelligence remains uneven a decade after September 11, 2001 (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. For example, there is an increasing application of the intelligence process for violent crime suppression, such as found in Real time Crime Centers -- a notable different application than the counterterrorism role. Third, it simply takes time to develop new organizations such as fusion centers and develop them at an operational level. Similarly, training and developing new policies in America's approximately 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.

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. Findings from the present study suggest small agencies should have intelligence liaison officers who can serve as "nodes" in the intelligence network. This requires commitment of resources at a time when many agencies are operating under conditions of financial constraint. 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 acknowledged that the use of analysts made the agency "work smarter" thereby having a notable 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 to include specifying types of

information can be shared, the process for sharing information, and the application of guidelines to protect privacy, civil rights and civil liberties.

Collectively, the data identified a number of factors that help safeguard against privacy and civil rights concerns while concomitantly maximizing both threat detection and risk reduction. The policy implications will reinforce the protection of civil rights in the intelligence process while maximizing the organizational effectiveness of the fusion center. As a result of concerns by some community members about privacy and civil rights protections related to the intelligence process, fusion centers should ensure their privacy infrastructure is in place. This includes having a privacy policy, training personnel on privacy guidelines, and having a privacy review board such as the one discovered in the FFC. This review board should include diverse members from outside the fusion center to elevate legitimacy and best ensure accountability to ultimately ease privacy concerns of fusion center practices.

REFERENCES

Bossler, A. M., & Holt, T. J. (2012). Patrol officers' perceived role in responding to cybercrime. *Policing: An International Journal of Police Strategies & Management*, 35: 165–181.

Brod, M., Tesler, L. E., & Christiansen, T. L. (2009). Qualitative research and content validity: Developing best practices based on science and experience. *Quality of Life Research*, 18: 1263-1278.

Carter, D. L. & Carter, J. G. (2009a). The intelligence fusion process for state, local and tribal law enforcement. *Criminal Justice and Behavior*, 36: 1323-1339.

Carter, D. L. & Carter, J. G. (2009b). Intelligence-led policing: Conceptual considerations for public policy. *Criminal Justice Policy Review*, 20: 310-325.

Carter, J.G. (2015). Inter-organizational relationships and law enforcement information sharing post-September 11, 2001. *Journal of Crime and Justice*, 38: 522-542.

Carter, J. G. (2016). Institutional pressures and isomorphism: The impact on intelligence-led policing adoption. *Police Quarterly*. DOI: 10.1177/1098611116639536.

Carter, J. G., & Chermak, S. (2012). Evidence-based intelligence practices: Examining the role of fusion centers as a critical source of information. In C. Lum and L. Kennedy. (Eds). *Evidence-Based Counterterrorism Policy*, 65-88. Springer, New York.

Carter, J. G. & Rip, M. (2013). Homeland security and public health: A critical integration. *Criminal Justice Policy Review*, 24: 573-600.

Centers for Disease Control and Prevention. (2011e). *Public Health Preparedness Capabilities: National Standards for State and Local Planning*. U.S. Department of Health and Human Services, Washington, DC.

Chermak, S., Carter, J. G., Carter, D. L., McGarrell, E. F., & Drew, J. (2013). Law enforcement's information sharing infrastructure: A national assessment. *Police Quarterly*, 16: 211-244.

Clark, R. M. (2007). *Intelligence Analysis: A Target-Centric Approach* (2nd Ed.). CQ Press, Washington, DC.

Cooney, M., Rojek, J., & Kaminski, R. J. (2011). An assessment of the utility of a state fusion center by law enforcement executives and personnel. *IALEIA Journal*, 20: 1-18.

Cope, N. (2004). Intelligence led policing or policing led intelligence? *British Journal of Criminology*, 44(2): 188-203.

Darroch, S., & Mazerolle, L. (2013). Intelligence-led policing: A comparative analysis of organizational factors influencing innovation uptake. *Police Quarterly*, 16(1): 3-37.

Deflem, M. (2004). Social control and the policing of terrorism: Foundations for a sociology of counterterrorism. *The American Sociologist*, 35: 75-92.

Denzin, N. K. (2012). Triangulation 2.0. *Journal of Mixed Methods Research*, 6: 80-88.

Electronic Privacy Information Center. (2008). *Information Fusion Centers and Privacy*. Retrieved from http://epic.org/privacy/fusion.

Fitzpatrick, J. L., Sanders, J. R., & Worthen, B. R. (2003). *Program Evaluation: Alternative Approaches and Practical Guidelines*. (3rd Ed.). Pearson, Boston.

Fusch, P. I. & Ness, L. R. (2015). Are we there yet? Data saturation in qualitative research. *The Qualitative Report*, 20: 1408-1416.

Greene, J. R. (2014). New directions in policing: Balancing prediction and meaning in police research. *Justice Quarterly*, 31: 193-228.

German, M., & Stanley, J. (2008). *Fusion center Update*. New York, NY: American Civil Liberties Union. Retrieved from http://www.aclu.org/pdfs/privacy/fusion_update_20080729.pdf

Glaser, B. & Strauss, A. (1999). *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Pisctataway: Aldine Transaction.

Global Justice Information Sharing Initiative. (2003). *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*. Washington, DC: U.S. Department of Homeland Security. U.S. Department of Justice. Retrieved from http://it.ojp.gov/documents/d/fusion_center_guidelines.pdf

Graphia-Joyal, R. (2010). Are fusion centers achieving their intended purposes? Findings from a qualitative study on the internal efficacy of state fusion centers. *IALEIA Journal*, 19: 54-76.

Harper, J. L. (2009). *Fusion Center Privacy Policies: Does One Size Fit All?* Master's Thesis. Monterey, CA: Naval Post Graduate School, Monteray, CA.

Holt, T. J., & Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. *American Journal of Criminal Justice*, 37: 396-412.

Homeland Security Advisory Council. (2005). *Intelligence and Information Sharing Initiative: Homeland Security Intelligence an Information Fusion*. U.S. Department of Homeland Security, Washington, DC.

Innes, M., Fielding, N., & Cope, N. (2005). The application of science? The theory and practice of crime intelligence analysis. *British Journal of Criminology*, 45(1): 39-57.

King, N. (1994). The Qualitative Research Interview. In C. Cassell and G. Symon (Eds.), *Qualitative Methods in Organizational Research*, 14-36. Sage, London.

Kurlander, N. (2005, February). Fighting crime and terrorism through data integration. *The Police Chief*, 72(2). Retrieved from http://policechiefmagazine.org.

Lessons Learned Information Sharing. (2005). *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview*. U.S. Department of Homeland Security, Washington, DC.

Lewandowski, C., & Carter, J. G. (2014). End-user perceptions of intelligence dissemination from a state fusion center. *Security Journal*. Advanced online publication. DOI:10.1057/sj.2014.38.

Masse, T., & Rollins, J. (2007). *A Summary of Fusion Centers: Core Issues and Options for Congress*. Congressional Research Service. RL 34177. Washington, DC.

Monahan, T. 2011. The future of security? Surveillance operations at homeland security fusion centers. *Social Justice*, 37: 84-98.

Monahan, T., & Palmer, N. A. (2009). The emerging politics of DHS fusion centers. *Security Dialogue*, 40: 617-636.

Monahan, T. & Regan, P. M. (2012). Zones of opacity: Data fusion in post 9/11 security organizations. *Canadian Journal of Law and Society*, 27: 301-317.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11 Commission Report*. Government Printing Office, Washington, DC.

Newkirk, A. B. (2010). The rise of the fusion-intelligence complex: A critique of political surveillance after 9/11. *Surveillance & Society*, 8: 43-60.

O'Reilly, M., & Parker, N. (2013). 'Unsatisfactory Saturation': A critical exploration of the notion of saturated sample sizes in qualitative research. *Qualitative Research*, 13: 190-197.

Pearsall, B. (2010). Predictive policing: The future of law enforcement? *NIJ Journal*, 266, 16-19. NCJ 230414.

Program Manager for the Information Sharing Environment. (2006). *Information Sharing Environment Implementation Plan*. Office of the Director of National Intelligence. Washington, DC.

Ratcliffe, J. H. (2008). *Intelligence-Led Policing*. Willan Publishing, Cullompton.

Ratcliffe, J. H. (2015). Towards an index for harm-focused policing. *Policing: A Journal of Policy and Practice,* 9(2): 164-182.

Ratcliffe, J. H., & Walden, K. (2010) State police and the intelligence center: A study of intelligence flow to and from the street, *Journal of the International Association of Law Enforcement Intelligence Analysts*, 19: 1-19

Riegle, R. (2009). *The Future of Fusion Centers: Potential Promise and Dangers*. Testimony of Director Robert Riegle. Committee on Homeland Security. Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. U.S. Department of Homeland Security, Washington, DC.

Rollins, J. (2008). *Fusion Centers: Issues and Options for Congress*. Washington, DC. Congressional Research Service. Report No. RL34070.

Rollins, J., & Connors, T. (2007). *State Fusion Center Processes and Procedures: Best Practice and Recommendations*. Manhattan Institute for Policy Research. Retrieved from http://www.manhattan-institute.org/html/ptr_02.htm.

Taylor, R., & Russell, A. (2012). The failure of police 'fusion' centers and the concept of a national intelligence sharing plan. *Police Practice and Research,* 13: 184-200.

Saari, S. C. (2010). *Fusion Centers: Securing America's Heartland from Threats*. Master's thesis, Naval Postgraduate School, Monterey, CA

Sanders, C. D., Weston, C., & Schott, N. (2015). Police innovations, 'secret squirrels' and accountability: Empirically studying intelligence-led policing in Canada. *British Journal of Criminology,* 55(4): 711-729.

Stavros, C., & Westberg, K. (2009). Using triangulation and multiple case studies to advance relationship marketing theory. *Qualitative Market Research,* 12: 307-320.

Wood, J. D., Taylor, C. J., Groff, E. R., & Ratcliffe, J. H. (2015). Aligning policing and public health promotion: Insights from the world of foot patrol, *Police Practice and Research.* 16(3): 211-223.

U.S. Department of Homeland Security. (2014). *2013 Fusion Center Assessment*. Final Report. Washington, DC.

U.S. Department of Justice. (2011). *Health Security: Public Health and Medical Integration for Fusion Centers*. Global Intelligence Working Group. U.S. Department of Justice, Washington, DC.

U.S. Governmental Accountability Office. (2010). *Information Sharing: Federal Agencies Are Helping Fusion Centers Build and Sustain Capabilities and Protect Privacy, but Could*

Better Measure Results. Report to Congressional Requesters. Report GAO-10-972. Washington, DC.

US House of Representatives. (2013). *Majority Staff Report on the National Network of Fusion Centers*. Committee on Homeland Security, Washington, DC.

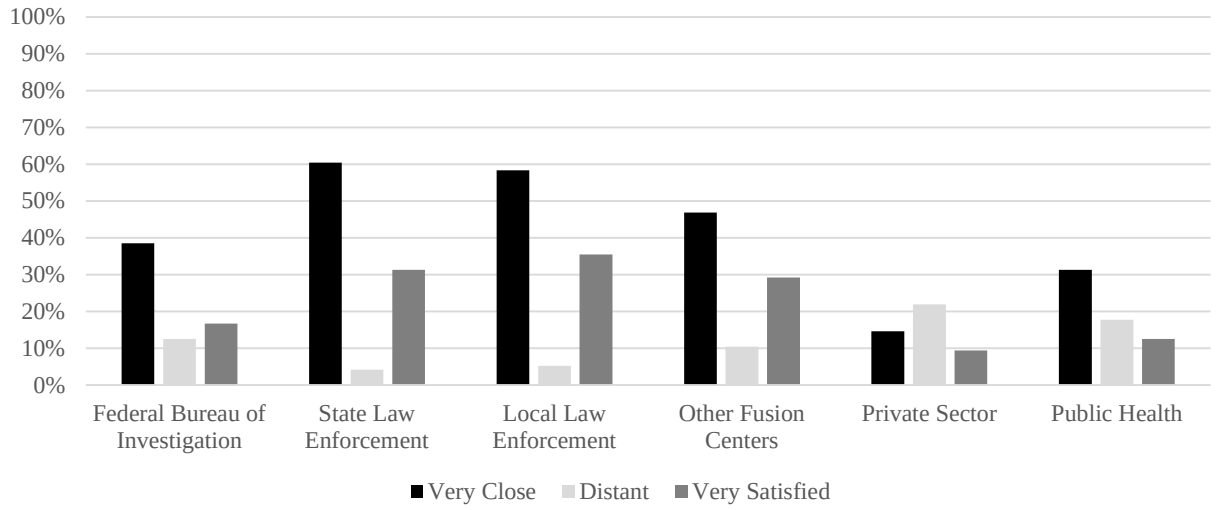
U.S. Senate. (2012). *Federal Support for and Involvement in State and Local Fusion Centers*. Permanent Subcommittee on Investigations. Committee on Homeland Security and Governmental Affairs, Washington, DC.

FIGURES AND TABLES

Table 1. Fusion Center Respondent Descriptives (*n* = 96)

	n (Percent)
Respondent's Position	
Administrator	49 (51%)
Supervisor	19 (20%)
Investigator	7 (8%)
Analyst	10 (10%)
Not Specified	11 (11%)
Respondent Years at Fusion Center	
Less than 1 Year	10 (10%)
1-3 Years	39 (41%)
4-9 Years	26 (27%)
More than 10 Years	5 (5%)
Not Specified	16 (17%)
Operational Focus of Fusion Center	
Terrorism Only	5 (5%)
"All-Crimes"	28 (29%)
"All-Crimes, All-threats, All-Hazards"	50 (52%)
Not Specified	13 (14%)

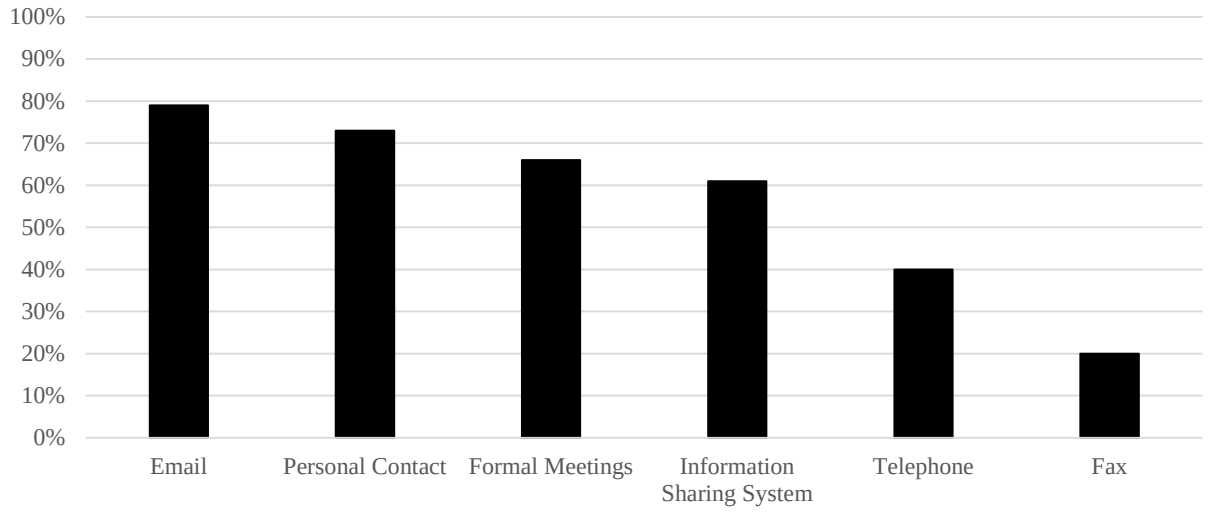
Figure 1. Relationships for Information Sharing



	FBI	State LE	Local LE	Other FC	Private Sector	Public Health
Very Close Mean	0.39	0.60	0.58	0.47	0.15	0.31
Very Close S.D.	0.49	0.49	0.50	0.50	0.35	0.47
Distant Mean	0.13	0.04	0.05	0.10	0.22	0.18
Distant S.D.	0.33	0.20	0.22	0.31	0.42	0.38
Very Satisfied Mean	0.17	0.31	0.35	0.29	0.09	0.13
Very Satisfied S.D.	0.37	0.47	0.48	0.46	0.29	0.33

Very Close: $n = 96$, $\alpha = .933$
Distant: $n = 96$, $\alpha = .763$
Very Satisfied: $n = 96$, $\alpha = .914$

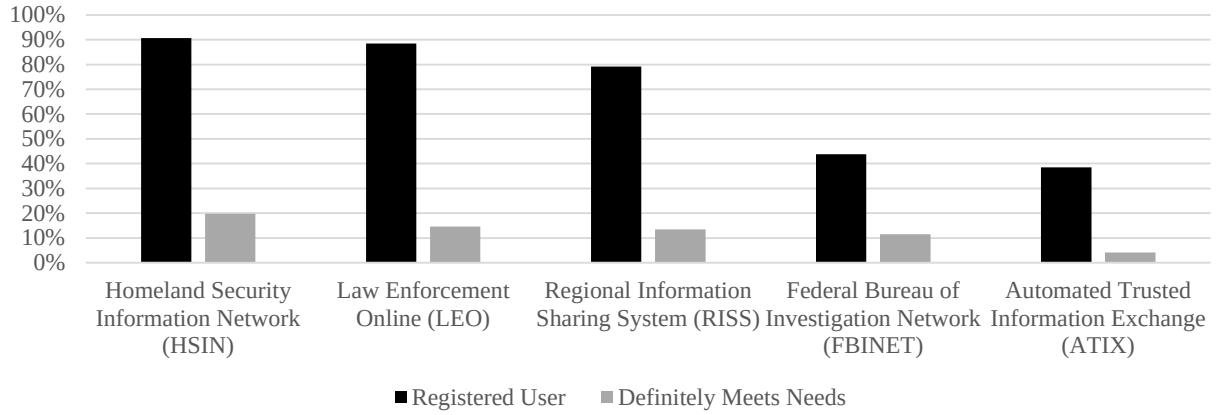
Figure 2. Methods of Sharing Information



	Email	Personal Contact	Formal Meetings	Information Sharing System	Telephone	Fax
Mean	0.79	0.73	0.66	0.61	0.40	0.20
S.D.	0.41	0.45	0.48	0.49	0.49	0.40

n = 96, α = .723

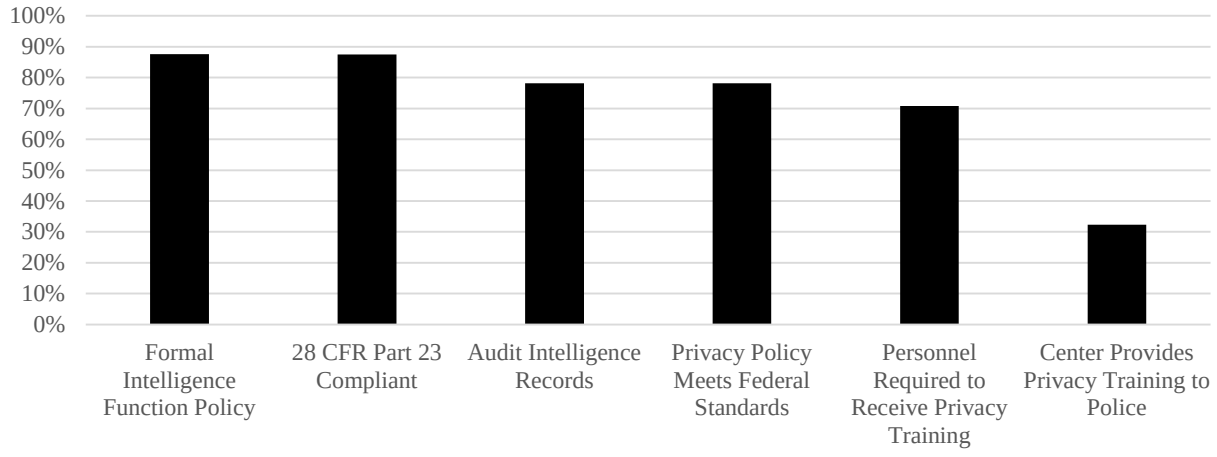
Figure 3. Information Sharing Systems



	HSIN	LEO	RISS	FBINET	ATIX
User Mean	0.91	0.89	0.79	0.44	0.39
User S. D.	0.18	0.21	0.36	0.50	0.50
DMN Mean	0.20	0.15	0.14	0.12	0.04
DMN S.D.	0.40	0.35	0.34	0.32	0.20

Registered User (User): n = 96, α = .564
Definitely Meets Needs (DMN): n = 96, α = .748

Figure 4. Safeguarding Privacy



	Intell Policy	28 CFR Part 23	Audit	Federal Standards	Personnel Privacy Training	Privacy Training to Police
Mean	0.88	0.88	0.78	0.78	0.71	0.32
S.D.	0.33	0.33	0.42	0.42	0.46	0.47

n = 96, α = .785

Appendix
Glossary for Acronyms

Acronym	Full Name	Description
28 CFR Part 23	28 Code of Federal Regulation Part 23	An operating policy for law enforcement agencies. It contains implementing standards for operating federally grant-funded multijurisdictional criminal intelligence systems. It specifically provides guidance in five primary areas: submission and entry of criminal intelligence information, security, inquiry, dissemination, and review-and-purge process.
9/11	Terrorist Attacks of September 11, 2001	The terrorist attacks of September 11, 2001 in New York, Washington, DC and Pennsylvania, United States.
ADVISE	All-Data Virtual Information Sharing Environment	Secure information sharing system developed and utilized by the Southern Nevada Counter-Terrorism Center to share information across sectors and partners.
CIKR	Critical Infrastructure and Key Resource Desk	An outreach program in the Michigan Intelligence Operations Center to facilitate information sharing partnerships across non-law enforcement organizations.
CPPAB	Constitutional Protections and Privacy Advisory Board	Advisory board within the Florida Fusion Center that collaborates with community privacy advocacy groups to ensure that privacy and civil rights are appropriately protected by the center's information acquisition, dissemination and retention practices as defined by written policy.
CUI	Controlled Unclassified Information	Information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act.
DHS	U.S. Department of Homeland Security	Cabinet organization in the United States government that oversees domestic security.
FDLE	Florida Department of Law Enforcement	State law enforcement entity of Florida.
FFC	Florida Fusion Center	State fusion center in Florida.
FLO	Fusion Center Liaison Program	Initiative to designate a single point of contact between a partner organization and a fusion center to facilitate information sharing.

FOUO	For Official Use Only	A document control designation, but not a classification. This designation is used by Department of Defense and a number of other federal agencies to identify information or material that, although unclassified, may not be appropriate for public release.
HSIN	Homeland Security Information Network	Information sharing network for homeland security mission operations to share sensitive but unclassified information.
InSite	Statewide Intelligence Site	Secure information sharing system developed and utilized by the Florida Fusion Center to share information across sectors and partners.
ILO	Intelligence Liaison Officer Program	National program in the United States to train individuals in public safety and the private sector to facilitate the flow of information from local to federal law enforcement operations.
ILP	Intelligence-Led Policing	An underlying philosophy of how intelligence fits into the operations of a law enforcement organization.
LEO	FBI Law Enforcement Online	Secure information sharing system for law enforcement that is provided by the Federal Bureau of Investigation.
LES	Law Enforcement Sensitive	A document control designation, but not a classification. This marking indicates recipients should be law enforcement personnel.
LVCVA	Las Vegas Convention and Visitor Authority	The official marketing organization of Las Vegas that promotes tourism, conventions, meetings and special events. It is a formal partner of the Southern Nevada Counter-Terrorism Center.
LVMPD	Las Vegas Metropolitan Police Department	Municipal police department of Las Vegas, Nevada and operating agency of the Southern Nevada Counter-Terrorism Center.
MIOC	Michigan Intelligence Operations Center	State fusion center in Michigan.
MOU	Memorandum of Understanding	Written policy agreement that guides action, inaction, expectations, and procedures for partnerships.
MSP	Michigan State Police	State law enforcement authority of Michigan.
QAS	Quality Assurance Section	Dedicated personnel within the Southern Nevada Counter-Terrorism Center that oversee legal, ethical, and policy compliances for information sharing.

RISS.net	Regional Information Sharing System Network	Secure information sharing system to facilitate capabilities, critical analytical and investigative support services, and event de-confliction across the United States.
SAR	Suspicious Activity Report	A report containing observed or reported behaviors that may be indicatives of terrorist planning or criminal activity.
SNCTC	Southern Nevada Counter-Terrorism Center	State fusion center of Nevada.
SSO	Single Sign On	Initiative to develop credentialing that allows for session/user authentication process that permits a user to enter one name and password in order to access multiple applications or secure systems.