THE INTELLIGENCE FUSION PROCESS FOR STATE, LOCAL AND TRIBAL LAW ENFORCEMENT

A White Paper

Prepared for the

Intelligence Program
Michigan State University

David L. Carter, Ph.D.
Program Director

Version 3.5

January 2007

Web: http://intellprogram.msu.edu ● E-mail: intell@msu.edu

Copyright © 2006 by David L. Carter. All Rights Reserved.

THE INTELLIGENCE FUSION PROCESS FOR STATE, LOCAL AND TRIBAL LAW ENFORCEMENT

The intelligence fusion process represents a new generation for the intelligence function and a new structure for most state, local and tribal law enforcement agencies to understand. Contrary to intuition, the fusion process (developing intelligence from diverse resources) and the creation of fusion centers (the physical plant) is more involved than merely changing organizational functions for an existing law enforcement intelligence unit. It typically involves either the re-engineering of the entire conceptual framework of the intelligence function in an agency or the creation of an entirely new entity. It requires engaging a wide array of people and organizations to be contributors and consumers of the intelligence function; it involves changing attitudes and processes of personnel; it requires establishing new functional and information sharing processes among state, county, municipal, tribal and federal law enforcement partners; it involves the development of new agreements and functional relationships; the development of new policies and processes; and the inculcation of the Intelligence Led Policing[1] philosophy.

As a result, the challenges are multifold, not the least of which is opening oneself and one's agency to organizational change. Most humans are dogmatic, resisting change. However, if incongruent past practices and erroneous assumptions are not eliminated from intelligence processes, the likelihood of success is diminished. The following discussion is intended to provide insight about the intelligence fusion process in the hope it will help facilitate the change needed to make intelligence fusion a functional reality.

Historical Perspective

Initially, intelligence Fusion Centers were referred to as Regional Intelligence Centers (RIC). They took different forms throughout the United States with no "single model" for what the intelligence center did or how it should be organized. They evolved largely based on local initiatives as a response to perceived threats related to crime, drug trafficking, and/or terrorism within a geographic region. The intent was to marshal the resources and expertise of multiple agencies within that region to deal with cross-jurisdictional crime problems. In some cases, a region was defined as a county (e.g., Rockland County, New York Intelligence Center); as the area surrounding a major city (e.g., Los Angeles Joint Regional Intelligence Center); a portion of a state (e.g., Upstate New York Regional Intelligence Center), or it may encompass an entire state (e.g., Minnesota Joint Analysis Center).

The earliest RICs began as the product of counterdrug initiatives starting in the 1980s. Indeed, the High Intensity Drug Trafficking Area (HIDTA)

[1]See http://www.theiacp.org/documents/pdfs/Publications/intelsharingreport.pdf and http://www.cops.usdoj.gov/mime/open.pdf?Item=1395

intelligence centers[2] served as models for successful structures and initiatives as well as identifying systemic issues that needed to be overcome.[3] In the late 1990s, the Bureau of Alcohol, Tobacco and Firearms (ATF) developed a number of programmatic activities to reduce gun violence. Emerging from these initiatives were ATF Regional Crime Gun Centers. The centers, in some cases co-located with the HIDTA RIC, had a number of intelligence-related roles including "…analyzing trace data to identify gun traffickers, disseminate investigative leads, and coordinate with the HIDTA RIC to identify drug traffickers and their sources of guns".[4] In virtually all cases, both the HIDTA and ATF intelligence centers had a great deal of interaction with state, local and tribal law enforcement agencies. The intent was to integrate – i.e., "fuse" – information from diverse sources to better understand and prevent multi-jurisdictional crime problems.

Hence the foundation was laid for intelligence centers. However, beyond idiosyncratic local crime issues, there was little incentive to expand the centers. Of course, this changed after September 11, 2001.

What is Intelligence Fusion?

The fusion process is an overarching methodology of managing the flow of information and intelligence across levels and sectors of government in order to integrate information for analysis.[5] That is, the process relies on active involvement of state, local, tribal and federal law enforcement agencies – and sometimes non-law enforcement agencies – to provide the input of raw information for intelligence analysis. As the array of diverse information sources increases, there will be more accurate and robust analysis that can be disseminated as intelligence. Information fusion utilizes the intelligence process[6] for information management and analysis. The Fusion Center is the physical location where the fusion process occurs.[7]

While the phrase "Fusion Center" has been used widely, often there are misconceptions about the function of the Center. Perhaps the most common misconception is that the Center is a large room full of work stations where the staff is constantly responding to inquiries from officers, investigators and agents. This vision is more accurately a "watch center" or "investigative support center" – *not* an intelligence Fusion Center. Another common misconception is that the

---

[2] http://www.whitehousedrugpolicy.gov/hidta/ny-nj-content.html

[3] The Counterdrug Intelligence Executive Secretariat (1331 F Street, NW, Suite 700, Washington, DC 20530; Telephone: (202) 353-1875/Fax (202) 353-1901) has an insightful unpublished report on *Metropolitan Area Consolidation/Collocation of Drug Intelligence Elements* that describes success and challenges for Regional Intelligence Centers.

[4] http://www.atf.gov/field/newyork/rcgc/

[5] *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview*. (2005) Lessons Learned Information System, U.S. Department of Homeland Security. http://www.LLIS.gov.

[6] The Intelligence Process – also known as the Intelligence Cycle – involves the systemic steps used to collect, assess, analyze and dissemination intelligence.

[7] *Executive Summary: Fusion Center Guidelines*. (2005) Global Intelligence Working Group. http://it.ojp.gov.

Fusion Center is minimally staffed until there is some type of crisis wherein representatives from different public safety agencies converge to staff work stations to manage the crisis. This is an "emergency operations center", *not* an intelligence Fusion Center.

The Fusion Center is not an operational center, but a support center. It is *analysis* driven. The fusion process proactively seeks to identify threats posed by terrorists or criminal enterprises and stop them before they occur – prevention is the essence of the intelligence process. The distinction, however, is that the Fusion Center is typically organized by amalgamating representatives – ideally, mostly intelligence analysts – from different federal, state, local and tribal law enforcement agencies into one physical location. Each representative is intended to be a conduit of raw information from his/her agency who can infuse that agency-specific information into the collective body of information for analysis. Conversely, when there are intelligence requirements[8] needed by the Fusion Center, the representative is the conduit back to the agency to communicate, monitor and process the new information needs. Similarly, the agency representative ensures that analytic products and threat information is directed back to the parent agency for proper dissemination.

According to the Global Intelligence Working Group's (GIWG) national Fusion Center Guidelines, a Fusion Center is:

> … defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The intelligence component of a Fusion Center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity.[9]

Obviously, not every law enforcement agency can contribute a person to work in the Fusion Center. Hence the Fusion Center must develop mechanisms for two-way information sharing that captures information from the "nontraditional collectors" and provides threat-based information back to those who have the

---

[8]"Intelligence requirements" are information that is needed to help make a comprehensive and accurate analysis of a threat. *See*: Global Intelligence Working Group, Intelligence Requirements Subcommittee Report. *Recommendations for Intelligence Requirements for State, Local and Tribal Law Enforcement Agencies*. (October 2005).

[9]Global Intelligence Working Group. (2005). *Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level*. Washington, DC: U.S. Department of Justice and U.S. Department of Homeland Security, p. 8.

"need to know". As a result, multiple strategies and technologies need to be developed for diverse two-way information sharing.

For example, electronic two-way information sharing via the various secure electronic information systems – RISS.NET, LEO, HSIN, JRIES, NLETS or ATIX – can be very effective. In the case of ATIX, individuals beyond the law enforcement community who have a demonstrated need – including some private sector persons – may also have access to the system and use it for secure two-way information sharing. Another example is the New York Police Department's "Operation Nexus":

> The New York City Police Department's Operation Nexus is a nationwide network of businesses and enterprises joined in an effort to prevent another terrorist attack against our citizens. Our detectives [visit] firms that have joined us in this mutual effort. Members of Operation Nexus are committed to reporting suspicious business encounters that they believe may have possible links to terrorism. The NYPD believes terrorists may portray themselves as legitimate customers in order to purchase or lease certain materials or equipment, or to undergo certain formalized training to acquire important skills or licenses. … Through Operation Nexus, the NYPD actively encourages business owners, operators and their employees to apply their particular business and industry knowledge and experience against each customer transaction or encounter to discern anything unusual or suspicious and to report such instances to authorities.[10]

Another model has emerged and is being increasingly adopted throughout the U.S. Developed in Los Angeles, the Terrorism Early Warning (TEW) group has multiple functions, including supporting the intelligence Fusion Center.

> The Los Angeles TEW includes analysts from local, state and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-, and post attack) specifically tailored to the user's operational role and requirements. The TEW bridges criminal and operational intelligence to support strategic and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and

[10] http://www.nyc.gov/html/nypd/html/nexus.html

refined processes to analyze and synthesize threat data to support its client agencies.[11]

Regardless of the method of information sharing, the key factors are: there must be diverse raw input, it must be analyzed; and intelligence output must be shared with appropriate consumers.

Why Fusion Centers?

The heart of good intelligence analysis is to have a diverse array of valid and reliable raw information for analysis. The more robust the raw information, the more accurate the analytic output (i.e., intelligence) will be. If one thinks of information input in terms of bandwidth, the typical law enforcement intelligence unit has a narrow bandwidth. That is, information is gathered from a fairly narrow array of sources, thereby limiting both the quality of the analysis and the ability to see the "big picture" of a criminal enterprise. Quite simply, the more limited the input of raw information, the more limited the quality of intelligence. However, if the number of sources is broadened to include a wide range of agencies representing much broader geographic and jurisdictional parameters, then the bandwidth is much wider. With wider bandwidth, there is a greater (and more diverse) information flow. Therefore, with greater information flow, the analysis becomes more accurate and utilitarian. As the quality of analysis increases, the ability to prevent or mitigate the operations of a terrorist or criminal organization increases exponentially.

Recent analyses of both law enforcement and national security intelligence operations found a problem that has been referred to as the "stovepipe" of information in agencies.[12] That is, each agency would develop a large body of information and analytic products that would be retained within the agency and rarely shared with other agencies. Analysis was generally limited to the information that came from internal sources and dissemination of information was also largely internal. As a result, while agencies were developing information it was simply being stacked, metaphorically like a stovepipe. Current thought recognizes that far more value can be derived from information that is widely shared for analysis – information from one agency may be a key in learning about a threat when integrated with information another agency. Hence, there was a need to "fuse" as much information as possible.

As noted in a report from the Heritage Foundation, the Fusion Center would not simply duplicate the activities of existing agencies, but would enhance and improve their efforts by providing a service that does not yet exist.[13]

---

[11]Sullivan, John P. (2005). *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence*. A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada, p. 1.
[12]As an illustration see, Kindsvater, Larry C. (2003). "The Need to Reorganize the Intelligence Community". *Studies in Intelligence.* Vol. 47, No. 1, http://www.cia.gov/csi/studies/vol47no1/article03.htm.
[13]Dillon, Dana R. (2002). "Breaking Down Intelligence Barriers for Homeland Security." *Backgrounder #1536*. Washington, DC: Heritage Foundation. http://www.heritage.org/Research/NationalSecurity/BG1536.cfm.

Is There a Role for the Private Sector?

Often overlooked, the private sector can be a rich resource of information that adds a broadened dimension to information collection. Many large corporations have sophisticated security operations that monitor global threats to their facilities, products and personnel posed by organized crime and criminal extremists as well as predatory criminals. This type of information is often different than that collected by law enforcement organizations and can add a unique, and more insightful, component to the body of information being analyzed by the Fusion Center.

Similarly, the private sector is often a legitimate consumer of law enforcement intelligence meeting the "right to know" and "need to know" information sharing standards. For example, 85% of the U.S. critical infrastructure is owned by the private sector. Moreover, the private sector has a large personnel force who, if given the proper information, can significantly increase the "eyes and ears" on the street to observe individuals and behaviors that pose threats. As noted in one the "Best Practices" papers produced by the Department of Homeland Security, "a jurisdiction's analysis and synthesis entity, [such as a Fusion Center], should also establish processes for sharing information with the local private sector".[14]

Of course, there are information sharing issues that need to be resolved. For example, certain types of personal information may be inappropriate for law enforcement to release to the private sector. Conversely, proprietary information related to corporate products may also be restricted. Despite these limitations, there is a legitimate role for the private sector in Fusion Centers. Just as in the case of law enforcement partners, Memoranda of Agreement need to be in place that includes provisions on information sharing processes and restrictions.

Outputs of the Fusion Center

The Fusion Center is not designed to answer on-going calls or inquiries about individuals or threats. While this will no doubt occasionally occur, if it happens too frequently the staff will be overwhelmed and unable to perform their responsibility of analysis. The most important output of the intelligence Fusion Center is *actionable* intelligence. This means that the intelligence produced by the center will drive operational responses and strategic awareness of threats.

An operational response would be when the analysis determines that there is a threat against a specific type of target. Operationally, the law enforcement agency may then take necessary actions to harden the target or intercept the threat. Strategic awareness is broader information that provides

[14] Lessons Learned Information Sharing Best Practices. (2006). *Local Anti-Terrorism Information and Intelligence Sharing: Dissemination*. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=13091.

information on threats and methodologies – or indicators – of terrorists and criminals. For example, it may be learned that terrorists plan to use Vehicle-Based Improvised Explosive Devices (VBIED) for attacks. The characteristics or indicators of people, vehicles and materials that may be used in a VBIED attack would be distributed to officers on the street, and perhaps some security personnel, so they may be constantly on alert for such an attack.

The specific kinds of output from a Fusion Center are not universal. Different regions of the country, the character of targets in a region and the unique character of threats must be taken into consideration when output is being designed. For example, in a given geographic region there may be a large presence of active right wing extremists. As a result, a significant amount of attention from the Fusion Center would be focused on their activities. Similarly, the U.S. Border with Mexico would have significant attention devoted to drug smuggling and human trafficking. Thus, while all Fusion Centers should have an "all crimes" approach, there should appropriately be priorities within those crime categories.

In light of this, the Fusion Center's substantive outputs should be based on three basic factors:

- Defined threats based on comprehensive – and ongoing – threat assessments within the jurisdiction of the Fusion Center.
- Information and intelligence needs defined by stakeholders.
- National priorities – including those of external funding – such as the National Preparedness Goal[15] or FBI intelligence requirements.

Beyond the substantive content, the format and frequency of outputs need to be identified, specifically in light of the types of analysis and products that are produced and the frequency of which they are produced. In some cases the format of the output may be dependent on unique characteristics of the Fusion Center's jurisdiction. For example, e-mail alerts may not be feasible in regions where there is limited electronic connectivity by law enforcement agencies. Similarly, intelligence alerts and bulletins that are designed to be briefed and handed out at roll calls would not be feasible for rural or decentralized law enforcement agencies. Types of output may include any or all of the following:

- *Summary briefs* – incidents and activities, globally or locally, that may have some correlation to threats, particularly if the incidents reflect a trend.
- *Threat assessment* – a detailed description of threats, targets, the likelihood of an attack against a defined target, and the potential methods of attack.

[15] https://www.llis.dhs.gov/member/secure/dynamicpage.cfm?pagetitle=Preparedness

- *Situational awareness reports* – the current status of known threats or changes in the status of known threats.
- *Information bulletins* – information on new or emerging threats, including threat indicators and methodologies.
- *Intelligence assessments* – comprehensive analysis, usually of a strategic nature, about a threat.
- *Raw intelligence* – information that is derived from a source deemed to be reliable but has not been corroborated or analyzed. Typically the threat is time critical and potentially severe, hence the dissemination of the information.

In addition to these intelligence products, the Fusion Center will also produce "case intelligence". This is intelligence related to specific threats, targets and suspects. Case intelligence is produced and disseminated on a timely basis as facts warrant. Dissemination is typically more narrow and only goes to those persons who have a demonstrable "right to know" and "need to know" the information.

The different intelligence outputs may employ a variety of analytic techniques: link analysis, financial analysis, association matrices, visual investigative analysis, threat profiling, and pattern analysis are illustrations. Typically a Fusion Center would also be involved in other processes that enhance the criminal inquiries of intelligence targets, such as deconfliction, case correlation (particularly between jurisdictions) and intelligence support of investigations related to criminal enterprises and terrorism.

DEVELOPING THE FUSION CENTER

Importantly, a Fusion Center's operations should be consistent with the recommendations of the *National Criminal Intelligence Sharing Plan* (NCISP)[16] and the *Fusion Center Guidelines*[17] of the Global Intelligence Working Group. The NCISP provides standards for all aspects of the intelligence function to ensure best practices, effective operations and adherence to civil rights. The Fusion Center Guidelines are designed to ensure:

> Information and intelligence sharing among states and jurisdictions will become seamless and efficient when each Fusion Center utilizes a common set of guidelines. The complete support of public safety leaders at all levels is critical to the successful implementation and operation of Fusion Centers.[18]

[16] *See* http://it.ojp.gov/topic.jsp?topic_id=93
[17] *See* http://it.ojp.gov/topic.jsp?topic_id=209
[18] Global Intelligence Working Group. (2005). Ibid., p. ii.

Adherence to established national standards will increase the quality of information sharing both within the Fusion Center's participants' jurisdictions and with intelligence entities outside of the region. Further, the standards will institutionalize a consistent approach to information collection, retention, analysis and dissemination that represent recognized and accepted processes as defined by the consensus of intelligence subject matter experts (SME's) who helped design the standards.

Beyond relying on national standards, consideration must be given to defining who the Center's stakeholders are and determining what it will take to get the stakeholders "buy-in" to the Center's operations. It is this simple: There is a direct correlation between stakeholders (or consumers) participation in the Fusion Center and the success of the Center.

Three broad phases, each with specific focal areas, are envisioned to accomplish the Fusion Center's development.

Phase 1. This is the foundation phase and includes these elements:

- **Re-education**. Stakeholders must understand the contemporary role of law enforcement intelligence and the capabilities of the Fusion Center. Just as importantly, stakeholders must understand their role in making the intelligence function a success at preventing acts of terrorism and the occurrence of organized crime. As recommended by the NCISP, personnel at all levels of the organization – from executives to line personnel – must receive awareness training as intelligence relates to their role.

- **Developing a mission, goals and objectives**. What is the new Fusion Center to do? How will it operate? What crimes will be addressed? What will it produce? What is its role and relationship to its consumers? What are the priorities of the Fusion Center? These are questions that must be resolved and articulated in the mission, goals, and objectives. This is a laborious process requiring input from executives and stakeholders. It cannot be effectively done, however, until after the training component because all personnel must understand the contemporary law enforcement intelligence function and ensure their vision of the Fusion Center is consistent with contemporary standards.

- **What the Fusion Center will *not* do**. Just as important, as what the Fusion Center will do, is some discussion of what the Fusion Center will *not* do. There will likely be changes in the historic intelligence activities of agencies that will not be continued in the Fusion Center. For example, many activities of state police intelligence units tended to be more like a "clearinghouse" or

"investigative support" rather than intelligence activities. In order for the Center to function most effectively, these factors must be clear. Similarly, stakeholders and consumers must understand what the Fusion Center will not do in order to avoid erroneous expectations.

Phase 2. Proactive developmental activities that must be overtly addressed in this phase include:

- **Developing relationships**. Two critical elements to the success of any intelligence activity is information collection and information dissemination. Both have detailed elements to ensure that everyone "does their job" with respect to intelligence activities. The Fusion Center must rely on management support from partnering agencies to support the Fusion Center. It must also rely on personnel to collect needed information, document it, and forward it to the Fusion Center. Similarly, for there to be success, there must be effective dissemination of information and products from the Fusion Center in a manner that is easily accessible by consumers, in a format that is easy to use, and contain information on a consistent basis that it useful. In order to accomplish these things, there must be overt initiatives to develop relationships among stakeholders within the Fusion Center and with its external constituency. Developing these relationships must involve developing commitments to participate in the Center's activities.

- **Outputs/products**. The Fusion Center must identify specific outputs and products that will be produced on a regular basis. Will both tactical and strategic reports be produced? Will bulletins and advisories be produced? Will summaries be produced? What is the schedule for outputs? How will responses to specific inquiries be produced? What is the process for determining "right to know" and "need to know" standards for products and outputs? These are among the questions that need to be addressed and articulated as the Fusion Center's development process moves forward.

Phase 3. This phase involves moving all of the Phase 1 and Phase 2 activities into operational form. It includes everything from facilities and staffing to developing Memoranda of Agreement, to the actual implementation of the Fusion Center's operations. This phase can consume a massive amount of time and logistics, particularly when the intelligence function is not being just revised, but is being re-engineered.

Among other activities in this phase are melding agencies and their data, protecting each agency's data, standardizing data for incorporation into a single

system, ensuring quality control of data and establishing processes for auditing and accountability.

Fusion Centers and Civil Rights Issues

There is a concern among many privacy advocates that the growth of Fusion Centers will increase the jeopardy to citizens' civil rights and privacy. As noted in a National Governor's Association "Best Practices" paper, "The risks to individuals' privacy begin when personal information of any kind is entered into criminal justice information systems."[19]

Complicating this issue is the fact that not understanding the concept of the fusion process, many privacy advocates fear that the centers are the next iteration of centralized surveillance of citizens. As noted by John Reinstein, Legal Director of the ACLU of Massachusetts

> The establishment of a single-source intelligence center raises important issues concerning the scope of its operations and need for safeguards to ensure that its operation does not violate civil liberties or intrude on personal privacy.[20]

Perhaps the greatest concern of a Fusion Center in this regard is participation of federal law enforcement agencies whose jurisdiction for information collection and retention is different than state, local and tribal law enforcement agencies. Certainly, when a state, local or tribal law enforcement agency is the custodian of an intelligence records' system, care must be taken to exclude information from the Fusion Center that does not meet the standards of 28 CFR Part 23, as per the recommendations in the Fusion Center Guidelines and the National Criminal Intelligence Sharing Plan.

Fundamentally, the privacy and civil rights issues of citizens related to Fusion Centers are the same as any other aspect of the intelligence process. Those relevant standards of the NCISP apply in the same manner and should be fully adhered to. Further, Guideline 8 of the Fusion Center Guidelines states that the management of the Fusion Center should, "Develop, publish, and adhere to a privacy and civil rights policy."[21] Commentary on this Guideline goes on to note that:

> …one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals' privacy and constitutional rights through the use

---

[19] MacLellan, Thomas. (2006). *Protecting Privacy in Integrated Justice Systems*. Washington, DC: National Governors' Association Center for Best Practices, p. 4.
[20] http://www.aclu.org/privacy/spying/15315prs20050511.html
[21] *Fusion Center Guidelines*, Ibid., p. 49.

> of intelligence sharing systems. In order to balance law enforcement's ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place.[22]

As a consequence, civil rights issues for Fusion Centers have components related to policy, training, supervision and public information that must be addressed in the development and implementation stages.

Conclusion

The intelligence fusion process holds a great deal of promise for effective intelligence operations. This is particularly true given the multi-jurisdictional character of terrorists' operations and criminal enterprises. The three greatest challenges are (1) to develop a cooperative and committed relationship between all stakeholders; (2) to establish policies and processes that support efficient, effective and lawful intelligence operations; and (3) for the Center to "stay on message" as an analytic center.

[22] Ibid.