Law Enforcement Intelligence Classifications, Products, and Dissemination

6

CHAPTER SIX

Law Enforcement Intelligence Classifications, Products, and Dissemination

A range of terms describe different types of law enforcement intelligence. A brief discussion of these as they relate to state, local, and tribal law enforcement (SLTLE) will provide some context for the reader when these terms are encountered.

Intelligence Based on the Nature of Analysis

Two terms are often used in this category: "raw intelligence" and "finished intelligence." Typically, raw intelligence is information that has been obtained from generally reliable sources; however, it is not necessarily corroborated. It is deemed valid not only because of the sources but also because it coincides with other known information. Moreover, raw intelligence usually is time sensitive and its value is perishable in a relatively short period. Because of its time sensitivity and critical relationship to the community or individual safety, an advisory is disseminated as a preventive mechanism.

Finished intelligence is when raw information is fully analyzed and corroborated. It should be produced in a consistent format to enhance utility and regularly disseminated to a defined audience. Different types of finished intelligence reports meet the needs of diverse consumers and are referred to as the "products" of an intelligence unit.

111 For example, follow-up instructions may direct a patrol officer to complete a field interview card, notify a special unit, conduct surveillance of the target, or take safety precautions.

Intelligence Products

To accomplish its goals, intelligence and critical information need to be placed in a report format that maximizes the consumption and use of the information. The report should do the following:

1. Identify the targeted consumer of the information (patrol officers, administrators, task force members, others).
2. Convey the critical information clearly.
3. Identify time parameters wherein the intelligence is actionable.
4. Provide recommendations for follow-up.[111]

Such products are a series of regularly produced intelligence reports that have a specific format and type of message to convey. They are most useful when each product has a specific purpose; is in a consistent, clear, and aesthetic format; and contains all critical information the consumer needs and no superfluous information. The types of products will vary by the character of the agency (e.g., state/local, urban/rural, large/small) as

well as the collection and analytic capacity of unit personnel. As a general rule, only about three products may be needed:

- Reports that aid in the investigation and apprehension of offenders.
- Reports that provide threat advisories in order to harden targets.
- Strategic analysis reports to aid in planning and resource allocation.

Without fixed, identifiable intelligence products, efforts will be wasted and information will be shared ineffectively.

"PRODUCTS" are a series of regularly produced intelligence reports that have a SPECIFIC FORMAT and type of message INTENDED TO CONVEY.

Operational ("non-product") Intelligence

SLTLE often find a need to maintain information, in either raw or finished form that can place them in a controversial position. For purposes of community safety, law enforcement needs to maintain information on some people and organizations for two reasons: (1) The have the potential to commit crimes and (2) They pose a bona fide threat, although the parameters of that threat are often difficult to specify. Their actions are monitored and affiliations recorded to help prevent future crimes and/or build a future criminal case. Inherently problematic is the idea of a future crime: what is the rationale for keeping information on a person who has not committed a crime, but might do so? Essentially, if there is a compelling interest for community safety, an effective argument can be made to maintain records on individuals who threaten that safety as long as reasonable justification can be presented to show a relationship to criminality.

In this type of intelligence there is no product, per se, but regularly prepared and disseminated operational records on people and groups who are associated with terrorists or criminal enterprises. The important, yet difficult, balance is to ensure that there is no violation of constitutional

rights during the course of the process, but at the same time maintaining a resource of credible information for legitimate law enforcement purposes. An example is anarchists who advocate the "Black Bloc" tactic of property destruction, confrontation with the police, and disruption of the public's right to movement. Typically, the simple advocacy of such forms of protest would be expressions of free speech and therefore inappropriate to maintain in an intelligence records system. However, a legacy of anarchists using the Black Bloc tactic that includes causing property damage – some of it significant – and public disruption is a circumstance where operational intelligence becomes important because of the potential for criminal law violations.

If anarchists who advocate the use of the Black Bloc held a public meeting, it would be proper for an undercover agent to attend, take notes, describe participants, and take literature for inclusion in the intelligence records system.

Beginning in the fall of 2001, the police faced new challenges for operational intelligence. In the wake of the terrorists attacks in New York, Washington, and Pennsylvania, the U.S. Department of Justice began identifying people who entered the United States under the grant of entry afforded by various types of visas. Some were detained for several weeks on civil immigration violations. Others were detained on grounds that they had conspired with the terrorist, had materially assisted the terrorists, or had knowledge of the terrorist's plans. In an effort to expand the investigation, for both resolution of the September 11 attacks and to prevent future attacks, the FBI began a systematic identification of specific people who had entered the U.S. on a visa with the intent of interviewing the visa holders.[114] Evidence of knowledge about any aspect of the terrorists' attacks was not a precursor for a person to be interviewed.

Because of the potential for civil litigation and ethical concerns about the propriety of these interviews, some police departments – beginning with Portland and Corvallis, Oregon – declined to comply with the FBI's request to assist in the interviews. It is probable that future conflicting interests will emerge in the war on terror and the prudent police manager must carefully consider the legal and ethical concerns of such practices and balance them with the need to protect the community.

114 The questions asked of people in the U.S. on non-immigrant visas: If they…….noticed anybody who reacted in a surprising way to the news of the September 11 attacks.
…know anyone who has helped plan or commit terrorism or anybody capable of or willing to commit terrorism.
…have sympathy for the September 11 hijackers or other terrorists and the causes they support.
…have heard of anybody recruiting people to carry out terrorism against the United States, or if anyone has tried to recruit them.
…know anyone who has received financing or training for terror activities.
…are willing to provide information in the future.
…know anyone capable or developing any biological or chemical weapon such as anthrax.

Intelligence Based on the Orientation of the Analysis

Traditionally, intelligence for SLTLE agencies has also been described according to whether the output of the analysis is either ***tactical or strategic***.

Tactical intelligence is used in the development of a criminal case that usually is a continuing criminal enterprise, a major multijurisdictional crime, or other form of complex criminal investigation, such as terrorism. Tactical intelligence seeks to gather and manage diverse information to facilitate a successful prosecution of the intelligence target. Tactical intelligence is also used for specific decision making or problem solving to deal with an immediate situation or crisis. For example, if there is a terrorist threat to a target, tactical intelligence should provide insight into the nature of both the threat and the target. As a result, decisions can be made on how to best secure the target and capture the offenders in a way that increases the probability of some form of action, such as prosecution or expulsion from the country if the person(s) involved is(are) not United States citizen(s).

Strategic intelligence examines crime patterns and crime trends for management use in decision making, resource development, resource allocation, and policy planning. While similar to crime analysis, strategic intelligence typically focuses on specific crime types, such as criminal enterprises, drug traffickers, terrorists, or other forms of complex criminality. Strategic intelligence also provides detailed information on a specified type of crime or criminality.[113] For example, terrorists cells[114] related to Al-Qaeda within the United States might be described to the extent possible on their characteristics, structure, philosophy, numbers of members, locations, and other distinguishing characteristics. Similarly, a strategic intelligence report may document attributes of "eco-extremists"[115] by describing typical targets and methods used in their attacks. This information helps police understand the motivations of the intelligence targets and can help in deploying investigative resources, developing training programs for police personnel to better understand the threat, and provide insights which may help in target hardening. Such ongoing

113 For examples of strategic intelligence reports related to drug trafficking, see the Drug Enforcement Administration's intelligence publications at http://www.dea.gov/pubs/intel.htm.

114 A terrorist cell refers to a loosely structured working group with a specific terrorism-related mission that has multiple targets depending on how leaders decide to operationalize the mission. Typically, there is a loose hierarchy within the cell based largely on the idea of having one person who is the "first among equals"–this is the individual who communicates with decision makers and is generally responsible for handling expenses and logistics of the cell members. The relationship is not actually a "supervisory" one. Cell members typically live in close geographic proximity and may share a habitat. The activities of the cell may change, but that is determined by hierarchical leaders external to the cell, not a cell member.

115 The eco-extremist movement represents environmental activism that is aimed at political and social reform with the explicit attempt to develop environmental-friendly policy, law, and behavior. As stated by one group, "The work of Green social transformation is only partially a matter of electoral and legislative victories. A far more important aspect of this work involves a fundamental retooling of the basic cultural values and assumptions that have led us to our current ecological and social problems."

strategic intelligence keeps officials alert to threats and potential crimes. Each type of intelligence has a different role to fulfill. When performed properly, the different forms of intelligence can guide investigations; provide insights for resource allocation; suggest when priorities should be expanded or changed; suggest when new training and procedures may be needed to address changing threats; and permit insight when there is a change in the threat level within a specific community or region.

… the different forms of intelligence can GUIDE INVESTIGATIONS; PROVIDE INSIGHTS for resource allocation; suggest when PRIORITIES should be expanded or changed; suggest when new training and procedures may be needed to address CHANGING THREATS; and permit insight when there is a change in the threat level…

On this last point, the federal government created the color-coded Homeland Security Advisory System (HSAS) to provide information to communities when indications and warnings (I&W) arise resulting from the analysis of collective intelligence. A formal and deliberate review process occurs within the interagency process of the federal government before a decision is made to elevate the threat level. The HSAS continues to be refined[116] and adjustments are made in line with security enhancements across the major critical infrastructure sectors. Additionally, as intelligence is assessed and specific areas are identified, the HSAS is sufficiently flexible to elevate the threat within the specific sector, city, or region of the nation. This was not something that could have been done in the infancy of the Department of Homeland Security or at the creation of the HSAS. As the intelligence capacity of the DHS continues to mature, along with the FBI's increased domestic intelligence capability supported by state and local law enforcement intelligence, threats can be targeted on geographic and temporal variables with greater specificity. As a result, the system becomes more useful to law enforcement and citizens alike.

115 (Cont.)

http://www.well.com/user/smendler/green/grnculture.htm As is the case with virtually any political or religious group, the eco-extremists also have members who commit acts of terrorism in the name of ecological conservation, such as the Environmental Liberation Front's (ELF) arsons of condominiums in the Rocky Mountains.

116 As an example, for the first time the HSAS was raised for a specific target (financial institutions) in specific areas (Washington, DC; northern New Jersey, and New York City) in the summer of 2004.

Assuming these developmental factors converge, there may well be greater interplay between the HSAS alert level and the emphasis given to the different forms of intelligence. For example, when the alert level increases, there will be a greater need for raw and operational intelligence to increase the probability of identifying and apprehending those involved in planning and executing a terrorist attack as well as to harden potential targets. As the alert level decreases, there will be a greater need to focus on strategic intelligence as a tool to assess trends, identify changes in targets and methods, or develop a pulse on the mood of the various terrorist groups to sense changes in their strategies. Tactical intelligence, involving criminal case development, should continue at a pace dictated by the evidence to identify and prosecute perpetrators. Law enforcement should seek all lawful tools available to secure the homeland through prevention, intervention, and apprehension of offenders.

DISSEMINATION[117]

The heart of information sharing is dissemination of the information. Policies need to be established for the types of information that will be disseminated and to whom. Critical to appropriate dissemination of information is understanding which persons have the "right to know" and the "need to know" the information, both within the agency and externally. In some cases, there may need to be multiple versions of one product. For example, an unclassified public version of a report may be created to advise citizens of possible threats. A second version may be "Law Enforcement Sensitive" and provide more detailed information about potential suspects that would be inappropriate to publicize.[118]

When considering disseminating sensitive material, a law enforcement organization should impose the "Third Agency Rule." This means that any recipient of intelligence is prohibited from sharing the information with another (i.e., third) agency. This affords some degree of control and accountability, yet may be waived by the originating agency when appropriate.

Clearly, the most efficient way to share information is by electronic networking. With the availability of secure connections, i.e., RISS.net, Law

117 On August 28, 2004, President Bush announced, "I have ordered the Director of Central Intelligence to ensure that we have common standards and clear accountability measures for intelligence sharing across the agencies of our government. I have established a new Information Systems Council to identify and break down any remaining barriers to the rapid sharing of threat information by America's intelligence agencies, law enforcement agencies, and state and local governments. To continue to protect the freedoms and privacy of our citizens, I've established a civil liberties board to monitor information-sharing practices." No additional details were available at this writing. http://www.whitehouse.gov/news/releases/2004/08/20040828.html

118 This is conceptually similar to what federal agencies use as a "tear line". In a classified report there may be a summary of critical information, without a description of sources and methods that is below a designated line on the report. This portion may be "torn off" of the report, making it Sensitive But Unclassified (SBU) and may be disseminated to law enforcement personnel who do not have a security clearance as "Law Enforcement Sensitive".

Enforcement Online (LEO), and the Joint Regional Information Exchange System (JRIES),[119] – as well as intranets in growing numbers of agencies, dissemination is faster and easier. The caveat is to make sure the information in the intelligence products is essential and reaching the right consumer. If law enforcement officers are deluged with intelligence reports, the information overload will have the same outcome as not sharing information at all. If officers are deleting intelligence products without reading them, then the effect is the same as if it had never been disseminated.

National Criminal Intelligence Sharing Plan

Formally announced at a national signing event in the Great Hall of the U.S. Department of Justice on May 14, 2004, the National Criminal Intelligence Sharing Plan (NCISP) (see Figure 6-1) signifies an element of intelligence dissemination that is important for all law enforcement officials. With endorsements from Attorney General John Ashcroft,[120] FBI Director Robert Mueller, Homeland Security Secretary Tom Ridge, and the Global Information Sharing Initiative,[121] the plan provides an important foundation on which SLTLE agencies may create their intelligence initiatives. The intent of the plan is to provide local police agencies (particularly those that do not have established intelligence functions) with the necessary tools and resources to develop, gather, access, receive, and share intelligence information.

119 The newly developed Homeland Security Information Network (HSIN) is intended to become the overarching information-sharing backbone.

120 http://www.usdoj.gov/opa/pr/2004/May/04_ag_328.htm

121 http://it.ojp.gov/topic.jsp?topic_id=8

Following a national summit on information-sharing problems funded by the Office of Community Oriented Policing Services of the Department of Justice, the International Association of Chiefs of Police (IACP) proposed the development of a plan to overcome five barriers that inhibit intelligence sharing:

1. Lack of communication among agencies.
2. Lack of equipment (technology) to develop a national data system.
3. Lack of standards and policies regarding intelligence issues.
4. Lack of intelligence analysis.
5. Poor working relationships/unwillingness to share information.

As a result, the Global Intelligence Working Group (GIWG) was formed to create the plan to address these issues:

- Blueprint for law enforcement administrators to follow
- Mechanism to promote Intelligence-Led Policing
- Outreach plan to promote intelligence sharing
- Plan that respects individual's civil rights.

The NCISP has 28 recommendations that address four broad areas. Among the key points are these:

1. The establishment of a Criminal Intelligence Coordinating Council
   - Consist of local, state, tribal, and federal agency representatives who will provide long-term oversight and assistance with implementing the plan (Recommendation #2)
   - Develop the means to aide and advance the production of “tear line” reports (Recommendation #17)
   - Develop working relationships with other professional law enforcement organizations to obtain assistance with the implementation of intelligence training standards in every state (Recommendation #19)
   - Identify an “architectural” approach to ensure interoperability among the different agencies' intelligence information systems (Recommendation #23)
   - Develop centralized site that allows agencies to access shared data (Recommendation #28)
2. Individual Agency Requirements
   - Adopt the minimum standards for Intelligence-Led Policing and develop an intelligence function (Recommendation #1)
   - Provide criminal intelligence training to all levels of personnel
3. Partnerships
   - Form partnerships with both public and private sectors to detect and prevent attacks on infrastructures (Recommendation #7)
   - Expand collaboration and sharing opportunities by allowing other types of organizations with intelligence information to work with law enforcement agencies (Recommendation #24)

Figure 6-1: Fact Sheet – National Criminal Intelligence Sharing Plan

"This plan represents law enforcement's commitment to take it upon itself to ensure that the dots are connected, be it in crime or terrorism. The plan is the outcome of an unprecedented effort by law enforcement agencies, with the strong support of the Department of Justice, to strengthen the nation's security through better intelligence analysis and sharing."

Attorney General John Ashcroft, May 14, 2004

The Department of Justice is effectively pursuing the goals of the National Criminal Intelligence Sharing Plan by ensuring that all of its components are effectively sharing information with each other and the rest of the nation's law enforcement community.

Activities by DOJ and Related Agencies:

- Through the Global Justice Information Sharing Initiative, the Attorney General captures the views of more than 30 groups representing 1.2 million justice professionals from all levels of government. Global members wrote the National Criminal Intelligence Sharing Plan and published guides, best practices, and standards for information sharing.
- The Department's Chief Information Officer, under the authority of the Deputy Attorney General, has formed a Law Enforcement Information Sharing Initiative to establish a strategy for the Department of Justice to routinely share information to all levels of the law enforcement community and to guide the investment of resources in information systems that will further this goal. The strategy identifies how the Department of Justice will support the implementation of the Plan.
- The newly established Criminal Intelligence Coordinating Council (CICC) under Global will serve to set national-level policies to implement the Plan and monitor its progress on the state and local level. The CICC will work with the Department's Law Enforcement Information Strategy Initiative and with the Justice Intelligence Coordinating Council, created by a directive of the Attorney General, to improve the flow of intelligence information among federal, state, and local law enforcement agencies.
- The Federal Bureau of Investigation (FBI) has built an enterprise-wide intelligence program to fulfill its responsibility to get vital information about those who would do us harm to those who can act to prevent that harm. To that end, the FBI has built robust intelligence production and sharing processes enabled by technologies developed and operated by the Criminal Justice Information Systems (CJIS) Division. The FBI has established an intelligence requirements process to both drive its investigative work against common threats and to satisfy the information needs of the larger U.S. national security community, including other partners in law enforcement. This process ensures that the FBI produces not only the information it can produce, but also the information it must produce to safeguard the nation.

Figure 6-1: Fact Sheet – National Criminal Intelligence Sharing Plan (Cont.)

In addition, the FBI has implemented a policy of "writing to release" to ensure the maximum amount of information is pushed to key customers and partners at the lowest possible classification level. The FBI Intelligence Webpage on Law Enforcement Online was created to make this information available at the unclassified level for FBI partners in state, local, and tribal law enforcement. Finally, the FBI has established Field Intelligence Groups (FIG) in each FBI field office to ensure the execution of the intelligence program in FBI field divisions. The FIGs are the bridge that joins national intelligence with regional and local intelligence information through entities like the Joint Terrorism Task Forces.

- The Drug Enforcement Administration (DEA), in partnership with the High Intensity Drug Trafficking Area Program and the Regional Information Sharing Systems (RISS), is developing the National Virtual Pointer System (NVPS) that will allow federal, state, local, and tribal law enforcement agencies access to pointer databases through a single point of entry. Through NVPS, participating agencies will be able to determine if any other law enforcement entity is focused on the same investigative target–regardless of the crime. They will be linked to the agent or law enforcement officer who has information on the related case. Information will be transmitted over the National Law Enforcement Telecommunications System and RISSnet, the secure web-based communication system operated by a collaborative organization of state and local justice officials.
- All components of the Department of Justice have adopted a common language for sharing information among differing computer systems, the Justice XML Data Dictionary. All federal grant programs to criminal justice agencies will also include a special condition calling for the use of this standard.
- The Department of Justice, through the FBI, Office of Justice Programs (OJP) and the Office of Community Oriented Policing Services (COPS), is providing training and technical assistance to criminal justice policy leaders, law enforcement professionals, and information technology professionals in standards and policies to enable information sharing, improve the use of intelligence by law enforcement, and build systems that tie into the nation's existing information-sharing networks.
- The Department of Justice is investing in research and development of new tools and methods to improve the use of intelligence in law enforcement. This work includes the continued development of XML standards, new analytical tools, security standards, and policing methods to improve the safety and effectiveness of police officers. In addition, through OJP and COPS, the Department is sponsoring pilot projects across the nation to improve the interoperability of information systems and show the impact of improved information sharing on fighting crime and terrorism.

Source: http://www.fbi.gov/dojpressrel/pressrel04/factsheet051404.htm

4. Intelligence Information and the Public

- Ensure the protection of individual's civil rights (Recommendation #6)
- Develop trust with communities by promoting a policy of openness to public (Recommendation #14)
- Promote accountability measures as outlined in 28 CFR Part 23 (Recommendation #15)[122]

CONCLUSION

The message of this chapter is twofold: First, when developing an intelligence capacity, there must be clearly thought out and articulated intelligence products. With this clearly defined output, the intelligence function will operate with greater efficacy.

Second, intelligence reports, bulletins, and advisories must be broadly disseminated to all persons who can use the information effectively. This refers not only to intelligence products developed by the agency, but also those products that are distributed from federal sources, regional intelligence centers, and other entities. Without effective dissemination, much of the value of intelligence is lost. All too often, patrol officers, private security, and citizens are excluded from dissemination. Certainly, there must be careful evaluation of the types of information that is disseminated, but nonetheless, a broad array of recipients should be included in the dissemination process.

122 At this writing, changes to 28 CFR Part 23 are being considered, but have not yet been implemented. A key element of the proposed changes is that provisions of 28 CFR Part 23 must be covered by policy. It is important that law enforcement executives and intelligence managers monitor legislative and regulatory activity related to this provision. If revisions to the regulation are implemented, it is highly recommended that appropriate personnel from SLTLE agencies attend new training programs that will be available. Training will be available at no charge, funded by the Bureau of Justice Assistance. See http://www.iir.com.