IACP National Law Enforcement Policy Center

Criminal Intelligence

Concepts and Issues Paper

Published: October 1998
Revised: July 2003

I. INTRODUCTION

A. Purpose of the Document

This document was designed to accompany the *Model Policy on Criminal Intelligence* established by the IACP National Law Enforcement Policy Center. This paper provides essential background material and supporting documentation to provide greater understanding of the developmental philosophy and implementation requirements for the model policy. It is anticipated that this material will be of value to law enforcement executives in their efforts to tailor the model to the requirements and circumstances of their community and their law enforcement agency.

B. Background

A leading expert in the field of terrorism and counter-terrorist tactics makes a compelling argument regarding the need for developing criminal intelligence when he notes that

> *[P]hysical measures don't reduce terrorism-they only move the threat along. Society cannot invest enough resources to protect everything, everywhere, all the time. Someone wanting to set off a bomb in Manhattan to kill scores of people can do it. And reducing terrorism has nothing to do with access control or how thick you make the concrete wall. It requires going after the terrorists and taking their groups apart.*[1]

Unfortunately, from a national level, the United States apparently lacks the intelligence capabilities necessary to adequately combat terrorism according to a major interagency study of federal capabilities and defenses. The 73-page report, commissioned by the U.S. Justice Department, pinpoints a lack of intelligence sharing on domestic terrorists as a significant problem and added that

> *the single most significant deficiency in the nation's ability to combat terrorism is a lack of information, particularly regarding domestic terrorism.*[2]

The events of September 11th also underscore the failure of our national intelligence system and the notion that physical measures to reduce terrorism are not the only, or even the best means to interdict terrorist acts.

While terrorism from international sources such as al-Quieda lead the nation's concerns at this time, the same observations hold true with regard to the prevention and interdiction of many other serious and more traditional crimes. Efforts to identify individuals and groups that may employ criminal means to advance their interests requires a systematic approach to information collection and analysis. Intelligence within the law enforcement context, whether of a tactical or strategic nature, refers to the collection, collation, evaluation, analysis, and dissemination for use of information relating to criminal or suspected criminal activities of a wide variety. Development of a systematic approach to this function within police agencies is essential in order to put what may otherwise be scattered or even unrecorded information and data to use in a constructive and concerted manner.

The collection of information for intelligence purposes has a long history. For hundreds of years, governments and their military forces have engaged in various activities to obtain intelligence about individuals and groups viewed as threatening. Although the origins of intelligence gathering by the police in the United States are difficult to determine, it appears that the intelligence function was first carried out by large city police departments when immigrants first concentrated in urban centers of this country. Nationality groups thought to be threatening by virtue of their suspected involvement in vice, narcotics, racketeering, and organized criminal activities were singled out as the primary target of police intelligence efforts.

The intelligence operations of federal, state and local police agencies shifted focus over the decades based on perceived needs and threats. For example, during Prohibition, intelligence operations concentrated on crimes directly and indirectly related to alcohol smuggling and sales and its connections to organized crime. In the post-World War II era, intelligence was used to gather information on suspected Communist organizations and during the Vietnam War period it shifted more toward information gathering on political activists and dissidents, civil rights demonstrators and antiwar protesters. Intelligence operations have long been used to aid in monitoring and building information on organized crime operations and are still widely used in this manner, although their focus has expanded to include the involvement of international conspiracies involved in drug trafficking. Most recently, intelligence operations have been directed at countering the threat of international terrorist organizations. In the wake of the destruction of the World Trade Center and the continued threat of terrorist activities, the need for law enforcement intelligence operations has become even more apparent. Efforts

A publication of the IACP National Law Enforcement Policy Center
515 N. Washington St., Alexandria, VA 22314-2357

to counter future terrorist acts within U.S. borders is not limited to federal intelligence gathering and interdiction. State and local law enforcement has a large and critical role to play in identifying terrorist cells within the United States and coordinating intelligence on suspected groups and their activities with federal enforcement agencies.

While intelligence plays a key role in law enforcement operations, history tells us that it can also be the instrument of abuse if such operations are not properly organized, focused and directed. Particularly during times of national emergency, one must be particularly vigilant to prevent aggressive enforcement and intelligence gathering from becoming incursions upon constitutional rights. Aggressive intelligence gathering operations that resemble fishing expeditions have been employed improperly in the past to garner sensitive or confidential information on individuals for whom there is no reasonable suspicion of criminal activity. Once documented, such information can develop a life of its own if sufficient safeguards are not built into screening, review and management of intelligence files. If passed on to other law enforcement agencies as intelligence, it can form the basis for abuse of civil liberties and potential civil liability.

In the same manner, intelligence operations are misguided that directly or indirectly gather information on persons based solely on their dissident political activities or views, because they espouse positions or philosophies that are perceived to threaten conventional social or political doctrine, traditionally accepted social mores or similar societal values or institutions, or because they have cultural connections with terrorists. Use of law enforcement intelligence resources to intimidate, inhibit or suppress such activities or harass such individuals under the pretext of legitimate police concern for maintaining social order are at best misguided and, in the worst case scenario, constitute a threat to the principles of law enforcement in a democratic society. Additionally, misguided intelligence gathering is a waste of valuable resources that are desperately needed to ferret out wrongdoers and persons who pose real threats to national and local security.

It is important to have an understanding and appreciation of potential abuses of criminal intelligence operations in order that intelligence gathering can be properly directed and information thus collected properly controlled and managed. That having been said, it is also important to reemphasize the indispensable role that criminal intelligence plays in support of law enforcement and the ultimate protection of society. While the Justice Department report and information that has surfaced since September 11 paint a discouraging picture of this nation's intelligence capabilities—particularly with respect to the new threats of chemical, biological and nuclear terrorists—it tends to overlook many successes of intelligence.

This is probably nowhere better illustrated than in the efforts of local, state and federal agencies in thwarting international and domestic terrorism in the United States. While the 2001 World Trade Center bombings and the Oklahoma City bombing are among those incidents that stand out in our collective memory, they are exceptions to the norm. It is worth noting that as devastating as these were, we often overlook the fact that many attacks of a similar or even a potentially more devastating nature have been thwarted largely through the development and use of criminal intelligence.

Aside from the attacks noted above, the vast majority of such incidents against the United States have been limited to attacks against United States interests abroad. The largest percentage of terrorist attacks in this country thus far have been bombings perpetrated against commercial establishments located in urban areas by special interest groups, such as the Animal Liberation Front, Up the IRS and the Earth Night Action Group. Organizations such as these and right wing groups, such as the Aryan Nation, the Order and Posse Comitatus are among the more threatening domestic groups. At the same time, left wing terrorist groups, such as the Marxist-oriented United Freedom Front, have been generally inactive since the 1980's due in part to the extensive number of arrests of group leaders during the last decade; largely serving as a credit to good intelligence operations.

Organized crime that has traditionally occupied a great deal of the focus of intelligence operations, while still a prominent threat, has experienced serious set backs over recent years due largely to effective intelligence gathering operations and aggressive prosecution.

But domestic and international terrorism, and organized crime are certainly not the only focus of criminal intelligence operations for state and local law enforcement agencies. State and local law enforcement share in the responsibility to counter these threats. Their input into regional and national intelligence databases is essential to this effort.[3]

But, state and local law enforcement agencies also are concerned with more provincial criminal matters. Defining these local criminal enforcement objectives and priorities forms the basis for information needs required to drive the intelligence function of individual agencies. Information gathering by individual officers is at the heart of any intelligence operation. Without the input of the officer on the beat, the generation of intelligence that can be returned to these officers for strategic and tactical purposes is not possible. Support of the agency's intelligence function is, therefore, the responsibility of every law enforcement officer who provides necessary information to fuel the process. And, if raw information provides the indispensable material to fuel the intelligence function, a professionally organized system of information evaluation, collation, analysis, and dissemination is the refinement process that turns this raw information into intelligence in support of law enforcement operations.

Intelligence, even the best of intelligence, does not produce decisions. Decisions on the use of law enforcement manpower and resources are made by command personnel who use intelligence constructively within the context of their professional experience. But, without good intelligence to point the way and weigh the options, law enforcement executives are at a serious disadvantage.

C. Policy

The Model Policy on Intelligence was developed with the foregoing background concepts and recognitions clearly in mind. These are generally incorporated into the model's policy statement, as follows:

> *Information gathering is a fundamental and essential element in the all-encompassing duties of any law enforcement agency. When acquired, information is used to prevent crime, pursue and apprehend offenders, and obtain evidence necessary for conviction. It is the policy of this agency to gather information directed toward specific individuals or organizations where there is reasonable suspicion (as defined in 28 CFR, Part 23, Section 23.3c) that said individuals or organizations may be planning or engaging in criminal activity, to gather it with due respect for the rights of those involved, and to disseminate it only to authorized*

individuals as defined. While criminal intelligence may be assigned to specific personnel within the agency, all members of this agency are responsible for reporting information that may help identify criminal conspirators and perpetrators.

The policy statement above addresses several of the key issues discussed in the introduction to this document. In particular, the policy makes clear the position that intelligence investigations shall be targeted at persons or organizations only when there is reasonable suspicion that they are involved in criminal activity. The means for ensuring that this mandate is followed are best addressed in the procedural and management practices utilized by the intelligence unit. These will be explored later in this paper. The policy statement also makes it clear that the means used to develop such information cannot overlook the rights of individuals guaranteed under the federal and state constitutions. These legal protections and individual rights cannot be placed on hold as a matter of convenience to achieve agency or intelligence objectives. The fact that officers cannot disregard their responsibility to the law or circumvent the rights of individuals as prescribed by law in the course of developing and managing intelligence information is a matter that deserves repetition and reinforcement in a policy on intelligence as well as in the agency's code of conduct and core values.

Third, the policy statement emphasizes the confidentiality issues involved in disseminating intelligence. Distribution of intelligence to authorized persons and agencies is generally described in terms of those who have a "need and right to know." A recipient agency or individual has a "need to know" when the requested information is pertinent to and necessary for the initiation or furtherance of a criminal investigation or apprehension. A "right to know" may be satisfied when the recipient agency or individual has the official capacity and statutory authority to receive the intelligence requested. Both of these conditions may need to be satisfied based on the nature and sensitivity of the information requested and the law surrounding the release of particular types of information or intelligence.

And finally, the policy statement emphasizes the fact that information gathering for intelligence is not only the responsibility of those assigned to the intelligence authority but is driven largely by personnel throughout the agency who contribute information for assessment. The vast majority of information used by an intelligence authority is the product of observations made by or information developed or received by patrol officers and investigators. Without their inputs, the intelligence function would be ineffective. Therefore, the model policy makes it clear to all law enforcement personnel within an agency that they are linchpins in the intelligence process.

D. Definitions

The model policy provides four definitions that are basic to the discussion of this topic. These are as follows:

Criminal Intelligence. Criminal intelligence is defined in the model policy as: "information compiled, analyzed and/or disseminated in an effort to anticipate, prevent, or monitor criminal activity."

Several points should be made concerning this definition. First, intelligence here and throughout the model policy and discussion paper refers to criminal intelligence. That is, the intent of information gathering, analysis and dissemination in this realm deals with the identification of persons who are reasonably suspected of being engaged in or preparing to engage in some form of criminal activity. This, by definition, precludes actions of persons that, although they may be considered troublesome, or otherwise objectionable, do not reasonably constitute a criminal threat. These persons are not legitimate subjects of criminal intelligence gathering.

This definition also precludes the conduct of counterintelligence operations by state and local law enforcement agencies. These are legitimately the domain of federal enforcement and investigative agencies. For example, state and local police should not be involved in the investigation of espionage, sedition, subversion and related national security concerns absent involvement or suspected involvement by the same individuals or groups in other felonious acts such as murder, arson, extortion or kidnapping. Investigation of criminal enterprises or criminal acts may, in some cases, uncover information of a national security interest. At that time, involvement of appropriate federal agencies is warranted even though the local or state law enforcement agency may conduct concurrent or cooperative investigations.

Finally, the definition makes the subtle yet all-important recognition that criminal intelligence is first, in its raw form, information. Basic information, whether collected by the intelligence unit, patrol officers, investigators or others is not intelligence in the literal or practical sense until it has undergone a series of analytical processes that determine its utility for tactical or strategic law enforcement purposes. While the term "intelligence" is used throughout the model policy and generically in the field of law enforcement, intelligence should be distinguished from information or data that through a systematic process may ultimately be converted into intelligence.

Intelligence in its useable form consists of reasoned conclusions, suppositions, and informed judgments based on a collection and analysis of reasonably reliable information. Intelligence is, or should be, more than speculation but may not always constitute a certainty. In most cases, criminal intelligence consists of evaluations of a wide variety of raw pieces of information that provide the basis for informed judgements and, as a whole, create enough information from which to draw reasonable inferences and conclusions. The degree to which intelligence approaches the level of certainty is partially differentiated by whether one is speaking of tactical or strategic intelligence.

Strategic Intelligence. The model policy defines strategic intelligence as: "Information concerning existing patterns or emerging trends of criminal activity designed to assist in criminal apprehension and crime control strategies, for both short-and long-term investigative goals."

Strategic intelligence is a synthesis of varied types of crime and criminal offender information used to develop trends, indicators, forecasts and projections about criminal activity from varied perspectives. Because of its general nature, strategic intelligence is ordinarily developed from information that is collected over a period of time. During this process, new information is continually being added to and integrated with information already in hand. When sufficient data are available, it is possible for an intelligence analyst to identify patterns of criminal activity and related trends that will assist in development of appropriate crime fighting strategies.

Tactical Intelligence. Tactical intelligence is defined in the model policy as: "Information regarding a specific criminal event that can be used immediately by operational units to further a criminal investigation, plan tactical operations and provide for officer safety."

Unlike strategic intelligence, tactical intelligence is more readily usable for operational purposes. However, like strategic intel-

ligence, it can be information derived from an on-going criminal investigation, surveillance, undercover operation, informant's tip or other source. But the nature of the information makes it more suitable for use on an immediate operational level.

For example, in anticipation of a labor strike and picketing at a factory site, it is necessary for the police to know not only the number of picketers expected but also their intentions and the possibility for the outbreak of violence. This type of information, possibly following some partial analysis and/or verification is of direct value in the assignment of patrol personnel to the factory site and adjacent areas. Tactical intelligence can lead directly to an arrest or to recognition that further information is needed. In this instance, if intelligence indicates that certain picketers will be carrying weapons, officers at the site can be alerted to the problem and arrests of specific violators can be made.

Threshold for Criminal Intelligence: The model policy uses the current federal threshold for gathering criminal intelligence as established in 28 CFR, Part 23, Section 23.3, which is "reasonable suspicion."

In order to employ a consistent national standard, the Model Policy Center will continue to endorse this federal standard. However, an amendment to this federal regulation has been proposed that would bring this standard in line with the U.S. Attorney General's Guidelines. If enacted, that guideline would set the threshold at a much lower level of "reasonable indication" and defer to the judgment of professional law enforcement officers as to the application of this threshold. "Reasonable indication" in the proposed amendment "may exist where there is not yet a current substantive or preparatory crime, but where the facts or circumstances reasonably indicate that such a crime will occur in the future." Action on this proposed amendment is anticipated in 2004 so the existing threshold of reasonable suspicion should be employed until such time as the proposed amendment is enacted.

II. PROCEDURES

A. Mission

As much if not more than any other law enforcement agency operation, the intelligence function needs to be clearly focused, and must subscribe to articulated goals and objectives that flow from an espoused statement of purpose. Some of the problems that have plagued police intelligence gathering operations over the years have been the result of information gathering operations that have not been limited by reasonable boundaries or regulated by adherence to a precise mission or self-imposed set of standards. While a policy or mission statement is meaningless without strong management oversight, it is the starting point for direction and control of a professional intelligence function. The model policy suggests the following general mission statement for the intelligence function:

> *It is the mission of the intelligence function to gather information from all sources in a manner consistent with the law in support of efforts to provide tactical or strategic information on the existence, identities, and capabilities of criminal suspects and enterprises generally and, in particular, to further crime prevention and enforcement objectives/priorities identified by this agency.*

The mission statement is operationalized by what is often referred to as a "collection plan" which serves as the authority for, as well as the rules and regulations for the collection and distribution of intelligence and administrative control of unit operations. Moreover, the collection plan provides direction to the intelligence unit by defining, focusing and prioritizing its operations in crime areas that directly affect the community. The plan should be a collaborative product of command personnel including the chief and may include the authority, rules, regulations, policies and procedures relative to the intelligence unit.

In addition to the above, the model policy identifies two areas that are deemed significant enough to deserve particular attention. In the first instance the policy states that

> *Information gathering in support of the intelligence function is the responsibility of each member of this agency although specific assignments may be made as deemed necessary by the officer-in-charge (OIC) of the intelligence authority.*

As noted in the foregoing definitions section, development of intelligence is contingent upon the input of useful raw information. Without the necessary information upon which to work, the intelligence function is ineffective. The bulk of information feeding the intelligence function comes from the observations of facts and information generated by patrol officers and criminal investigators. Some intelligence functions may be in a position to initiate operations directed specifically at gathering information on target individuals and enterprises through a variety of clandestine and overt operations. However, in most cases, the bulk of information necessary to drive the intelligence function is derived from personnel in field service units.

With this in mind, it is important to impress upon all personnel within the agency the significant role that they play in the intelligence function and to provide them with the process for efficiently feeding relevant information into that function. These information collection and distribution procedures will be discussed later in this paper.

Finally, the model policy mission statement directs that

> *Information that implicates, suggests implication or complicity of any public official in criminal activity or corruption shall be immediately reported to this agency's chief executive officer or another appropriate agency.*

During the course of their law enforcement duties, officers from a variety of operational duty assignments may come upon sensitive information that implicates or appears to implicate a public official in illegal practices. These are among the most difficult of situations facing law enforcement officers and administrators. The high profile nature of duties and responsibilities of public officials places a burden upon officers to ensure the integrity of information or evidence of a criminal nature that is brought against that public official. Inaccurate information or false accusations against public officials can have many serious negative implications for the law enforcement agency as well as the public, not the least of which is a depreciation in public trust and support. The law enforcement agency must also be aware of the possibility that the police agency is being used by political interests that may be initiating or inflaming public scandal for their own gain and advancement of political agendas.

At the same time, history is replete with cases of corruption of public officials, particularly with regard to their involvement or complicity in organized criminal enterprises. In many cases, this involvement has become known to those involved in the development of information for the intelligence function. Officers conducting undercover and surveillance operations in particular, may become privy to certain information that suggests the involvement of a public official with suspected or known crimi-

nal offenders. Where large amounts of money are involved, virtually no one is immune to potential involvement in criminal enterprises. This includes law enforcement officials as well as political figures and high ranking bureaucrats in state and local government.

It is therefore important that police officers, criminal investigators, intelligence analysts and any other officers who develop information that may implicate public officials, forward that information directly to the chief executive officer of the agency in order that it may receive appropriate attention at the highest level. The model policy also provides that such information may be forwarded to "another appropriate agency." This provision is designed to address those unusual yet potential situations in which there are suspicions or concerns that the office of the police agency chief executive or other high-ranking officials in the chain of command may be implicated in the criminal activity. In such situations, the office of the district attorney or prosecutor may be a more appropriate source to provide such information.

B. Organization

The model policy provides some guidance with regard to the organization of an intelligence function. It is recognized that the great diversity of law enforcement agencies will by necessity, require that individual intelligence operations conform with local agency capabilities and needs. But there are some general guidelines and recommendations that can be made in this regard that are relevant to most intelligence operations.

In particular, the intelligence function should be under the control and management of one individual (OIC) who oversees direction of its operations and management and administrative oversight consistent with the unit's mission and collection plan. While this individual may, in smaller agencies, also serve in related areas of the department and assume additional command responsibility, there is need for one person to assume responsibility for and command of the intelligence function.

Given the often-sensitive nature of the information collected by this operation, the intelligence OIC should report directly to the chief executive officer of the agency. In so doing, intelligence avoids potential filters through other channels and, because of its generally strategic nature, allows the chief executive additional lead-time to conduct necessary planning. In some situations, particularly in larger agencies, the intelligence OIC may report to a designee of the agency chief executive under routine circumstances. In addition to the sensitivity of the information involved, reporting directly to the office of the agency chief is justified by virtue of the nature of the intelligence function. That is, this organizational arrangement helps to prevent the undue involvement of intelligence unit personnel in line operations. For example, there is often a tendency for investigative officers or patrol commanders to co-opt the services of the intelligence unit to assist in criminal cases. While such assistance may be needed and ultimately authorized, it is far more difficult to maintain the focus of the intelligence function and control its work consistent with identified plans and objectives if it is organizationally or functionally integrated with investigative operations or other elements of the department. If command and control is lacking, it is common to find intelligence analysts being used as augmentations to or support personnel for criminal investigators. This not only serves to siphon off valuable time of intelligence personnel but also risks the possibility of intelligence personnel becoming involved in information gathering operations that are inconsistent with the role, mandates and even the legal and professional standards of the unit.

In both large and small law enforcement agencies, administrators must guard against the tendency to make the intelligence function simply an extension of criminal investigations or related operations. Officers should not be recruited for, or serve in intelligence units under the guise that they are to serve as a select investigative unit. As one expert in the field has said that

> *The unique functions of an intelligence unit pose some serious managerial dilemmas for an intelligence unit commander. Because intelligence represents a specialty in the law enforcement community that few police managers have been properly trained to understand, "intelligence units" are often transformed into elite investigative units. This has in effect undermined the legitimacy of the intelligence concept as a decision-making function and has created unnecessary and often counterproductive competition.*[4]

This is not to say that tactical information cannot or should not be a legitimate product of intelligence units. However, it does serve to suggest that (1) the intelligence function has often been misunderstood and, as a consequence, sometimes mismanaged function and (2) that in order to serve the true decision making goals of an intelligence unit, its management and organizational structure must in some regards be separated from day-to-day operational demands. In smaller agencies, this ideal is more difficult to achieve given often-serious personnel and related resource limitations and the mere fact that there is often less need for and consequently fewer demands upon the intelligence function.

Two means are generally used and recommended to assist an intelligence function to maintain its focus on and adherence to its mission: a manual of policies and procedures and a collection plan. In the first case, the manual provides personnel with a clear understanding of the functions, limitations upon and accepted procedures for unit personnel. By specifying acceptable and unacceptable intelligence practices and procedures to be followed, there is less chance that abuses will occur. The manual should clearly define, among the most important issues, the mission, goals and objectives of the intelligence function, acceptable procedures and limitations for collecting, analyzing/evaluating, auditing, purging, and disseminating intelligence and should establish accountability for these functions.

The collection plan serves as a companion document to the manual in that it operationalizes the intelligence authority's mission by establishing intelligence objectives and intelligence collection targets. This plan should be the product of collaborative efforts on the part of key agency decision makers and may include the perspectives and perceived priorities of members of local or state government. The plan serves to identify and prioritize the primary criminal threats affecting the jurisdiction, identify appropriate methods and necessary resources for developing requisite information to support investigation and enforcement actions and provides the authority for tasking these assignments. This document is dynamic in that targets and priorities will change over time and require periodic review of targets and their respective priorities.

The OIC of the intelligence function should establish a routine reporting schedule to the office of the agency chief executive or his/her designee. Generally such reporting should provide among other things, information on the quantity and nature of intelligence operations and objectives being pursued by the unit, some measurement of the manpower involved and success on objectives, and a review of the nature of any problems facing the intelligence

function either operationally or administratively. In addition to providing periodic reporting, the intelligence authority should have on going access to the chief executive to provide strategic and tactical information updates as circumstances dictate.

Staffing of the intelligence function can be problematic for law enforcement agencies; particularly the small to medium size agencies, given limited resources and real or perceived lack of demand for intelligence. Typically, personnel assignments in these departments are part-time in nature, sharing their time with related functions in crime analysis, investigations, research and planning or related functions. However, the recommended minimum personnel assignment is regarded by some experts as one full time position with no collateral duties.[5] Most are recruited from among sworn personnel within the agency or other law enforcement agencies. Some law enforcement agencies with sufficient demand may be fortunate enough and have adequate resources to employ professional law enforcement intelligence analysts.[6] However, there are a limited number of formally trained intelligence analysts in the United States and a 1992 survey found that of 1,228 such individuals, 90 percent were employed at the federal level.[7] As a consequence, most law enforcement agencies recruit personnel from within their ranks for these positions and attempt to provide in-service training to the degree possible.

In addition to specialized training in such processes as link analysis, strategic analysis, financial analysis, and investigative analysis; and the use of computers to perform these functions, additional personal characteristics or traits have been suggested for those persons vying for criminal intelligence positions. These include intellectual curiosity, tenacity, the ability to rapidly assimilate and recall information, discipline and intellectual courage.[8] Additionally, it has been suggested that intelligence officers should have a basic understanding and appreciation for the philosophical precepts of democracy, the Bill of Rights and the need to protect individual liberties and should, as a condition of employment, agree to periodic polygraph examinations directed towards the discovery of misconduct or abuses of the law and civil liberties.[9] While the latter of these recommendations may test reasonable grounds for the position, it does underline the necessity to ensure that intelligence personnel have a strong understanding and appreciation for the potential abuses and liability associated with their work and the need to work within the parameters of agency policy and procedures.

A broad exposure to law enforcement operations is a plus for prospective intelligence officers depending upon the scope of duties assigned the intelligence staff member. However, it is not a requirement. In fact, civilian employees with sufficient acumen have been used to staff intelligence operations for many years. Many professionals recommend a combination of civilian and sworn personnel to staff the intelligence function in order to attain the proper blend of knowledge, skills and abilities.

C. Professional Standards

The traditional model of policing has generally been one of reaction to reported criminal events. Under this system, a great deal of time, energy and expense has been expended in order to perfect ways in which officers could respond more quickly to such events, whether that be through computer aided dispatch or other means. But it wasn't until the Kansas City Preventive Patrol Experiment[10] and related research that the profession began to question the effectiveness of ever-increasing enhancements to this purely responsive form of police operations. In a solely responsive mode, law enforcement officers spend the largest percentage of their time chasing down calls for service. Far less effort is being devoted to anticipating and intercepting criminal activity or developing the means to thwart crime or solve problems that are the seeds of crime.[11]

Law enforcement intelligence operations are one important means of developing more proactive means of policing. Intelligence that, for example, allows officers to intervene more effectively in on-going criminal enterprises and ferret out criminal activity is simply smarter policing. But criminal intelligence gathering, if not organized properly and subjected to internal and external controls can form an unwarranted or even illegal intrusion upon the rights of individuals. The law enforcement agency's mission, as well as the intelligence unit's policies and procedures and collection plan should reflect both of these concerns and controls. The model policy presents four propositions that should be included in the professional standards of intelligence unit operations.

First the model policy recommends that

> *Information gathering for intelligence purposes shall be premised on circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity. .*

As will be noted later, procedures must be established for the opening of a criminal intelligence file. Authorization for opening such files and initiation of intelligence investigations must be based on reasonable justification. With sufficient justification, a preliminary intelligence investigation may be undertaken to determine whether there is a factual basis for undertaking an in-depth intelligence study. Some suggested parameters of a preliminary intelligence investigation include a national and local criminal history check, query of informants, physical surveillance and interviews of witnesses and victims.[12]

In keeping with this paper's earlier discussion concerning safeguarding individuals against unwarranted intrusions during intelligence gathering operations, the model policy states that

> *Investigative techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.*

This directive is one that requires mature administrative control and sound judgment in order to implement and enforce. This is particularly the case when intelligence operations are involved in attempts to develop information on criminal actions that might occur as opposed to those that have occurred. Most intelligence operations are anticipatory in nature. By their nature, these types of intelligence operations are less focused, often employing the principle of the fishing net rather than the fishing spear.[13] By frequenting locales where known or suspected criminals hang out, by contriving a ruse to see, overhear or otherwise gain knowledge of criminal plans and those persons involved or potentially involved in those plans, or by using other generally passive means, officers may develop sufficient information to pursue more active investigations. In such operations, the question often arises concerning the lengths to which officers should go in order to establish sufficient information to proceed with more active or aggressive intelligence information gathering.

For purposes of policy, only general guidelines can be offered to frame such decisions. The experienced intelligence supervisor must make reasonable judgements based on the circumstances involved and the information available in given situations. In so doing, some perspective can be gained by attempts to weigh the

intrusiveness of proposed intelligence and information gathering measures against the degree of harm of the potential or suspected criminal actions. For example, the use of so-called "sneak and peak warrants,"[14] video surveillance and other relatively intrusive measures would probably be difficult to justify in instances where the degree of harm of suspected criminal activity does not incorporate violence or other serious, high profile felonies.

The model policy also recommends that the intelligence function

> *shall make every effort to ensure that information added to the criminal intelligence base is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.*

In essence, this professional standard attempts to deal with the problem of quality control. This topic will be examined more later in this paper in the context of receipt and evaluation of information. From the perspective of professional standards, however, it may suffice to note that the failure to institute standards of quality assurance can result in serious problems. For example, lack of quality control can result in the inclusion of data in intelligence files that erroneously and unjustly implicates or suggests the implication of individuals in criminal activity. Such errors may result in privacy or civil rights violations and potential civil litigation, particularly where such information is used as the basis for more intrusive or covert intelligence operations. Inclusion of unfounded or erroneous information can also constitute a waste of valuable resources by siphoning them into areas of investigation that are groundless.

The foregoing primarily addresses the issue of quality control regarding the validity and reliability of information in intelligence files. But, the professional standard noted in the model policy also requires that only information relevant to a current or ongoing investigation be included in such files. In the course of conducting intelligence information collection activities, officers invariably come upon a variety of information about target individuals, accomplices and involved or uninvolved third parties. This ranges from information on a person's habits and tastes to items of a personal and highly sensitive nature that may not have any relevance on the potential or actual criminal culpability of the individual. Where this information is relevant to an investigation it can and should be included in intelligence files if found to be valid and reliable. However, information that has no direct bearing on furtherance of an on-going investigation should not be retained in intelligence files.

To assist in ascertaining the validity and reliability of information and maintaining accountability for these matters, the model policy also recommends that police intelligence operations maintain a record of the source of all information received and maintained by the intelligence authority.

Finally, in regard to professional standards, the model policy presents a requirement concerning the dissemination of intelligence information. The model policy states

> *Information gathered and maintained by this agency for intelligence purposes may be disseminated only to appropriate persons for legitimate law enforcement purposes in accordance with law and procedures established by this agency. A record shall be kept regarding the dissemination of all such information to persons within this or another law enforcement agency.*

This policy directive is designed to help ensure the security of information developed and maintained by the intelligence function. Intelligence information is extremely sensitive in most instances. Dissemination of such information should be limited only to persons with a need and a right to such information. Certainly, information should only be forwarded to authorized law enforcement personnel who can ensure that it will be used for legitimate law enforcement purposes and be subjected to at least the same level of safeguards as the sending agency. Since individual states often have specific requirements concerning the release of such information, intelligence personnel must be thoroughly familiar with any local or state statutes of relevance to this issue.

To develop an audit trail, the model policy requires that agencies maintain a record of individuals and agencies with which intelligence information has been shared. In like manner, recipient agencies should always record the source of intelligence received from other agencies. This should be done so that the information may be verified, authenticated or validated if need be at a later date, as well as to indicate to users within the agency that the information was not necessarily collected, screened or evaluated in accordance with established agency policy.

In addition to the above, the issue of sharing intelligence must be subject to particular safeguards and controls given the fact that receiving agencies are reliant upon the validity and reliability of such information. Information passed on without adequate internal quality control review can be received and used as the factual basis for investigations when such conclusions are not warranted.

D. Compiling Intelligence

The compilation of information that may prove to be of value for intelligence purposes, can be an involved undertaking. An aggressive crime prevention and control program requires that all members be aware of the importance of intelligence and contribute to that effort in the manner and to the degree they are capable. Training in the manner in which intelligence information may be gathered and the means for reporting that information should be provided to all operational personnel. Not only does this facilitate the intelligence function but also it may serve to overcome misunderstandings about the nature and uses of intelligence among operational personnel.

For example, there is often an operational distrust of intelligence largely because it develops a separate body of knowledge within the police agency that can and often does lead to changes in law enforcement agency policy and policing strategy. To the degree that strategic intelligence leads to alterations in strategies that are either politically or institutionally unpopular, the intelligence function may face some degree of mistrust among officers. However, this mistrust can be overcome through development of an appreciation and understanding of the role of the intelligence function among line officers and the valuable role that it plays in identifying crime problems, developing strategies for their solution and providing necessary tactical information to assist officers in their enforcement activities.

The methods of collecting information for use in the intelligence function as well as the means of reporting such information are purposely not incorporated in the model policy. These technical and procedural considerations (such as covert surveillance techniques and overt means of information gathering) are beyond the scope of this document but have been adequately addressed elsewhere.[15] However, from a policy perspective, it is important to note those issues addressed in the model policy.

For example, the model policy specifies under what conditions an intelligence file may be opened (i.e., an investigation or

study undertaken). From a general perspective, many agencies limit the collection of intelligence to those criminal problems identified in the collection plan or as authorized by the agency chief executive. In addition to answering whether the information is crime related and fits the mission of the intelligence unit, the intelligence function must identify minimal requirements for opening an intelligence investigation or file. The model policy identifies the following types of information as basic elements of an intelligence file:

- subject, victim(s) and complainant as appropriate;
- summary of suspected criminal activity;
- anticipated investigative steps to include proposed use of informants, photographic or electronic surveillance;
- resource requirements, including personnel, equipment, buy/flash monies, travel costs, etc.;
- anticipated results; and
- problems, restraints or conflicts of interest.

The model policy also makes clear the need for law enforcement officers to submit all intelligence-related information and file materials to the intelligence authority in stating that

> *Officers shall not retain official intelligence documentation for personal reference or other purposes but shall submit such reports and information directly to the intelligence authority.*

This admonition also precludes officers from maintaining intelligence files for their own use whether for the conduct of investigations or for other purposes.

The model policy also reinforces the requirement for maintaining intelligence operations within the limits of the law. These issues surround many aspects of intelligence operations as have been noted in other contexts within this paper. However, failures in this area are most likely when officers are engaged in covert intelligence gathering operations. For this reason, the policy provides the following caution:

> *Information gathering using confidential informants as well as electronic, photographic, and related surveillance devices shall be performed in a legally accepted manner and in accordance with procedures established for their use by this agency.*

Finally, with respect to the compilation of intelligence, the model policy requires that

> *All information designated for use by the intelligence authority shall be submitted on the designated report form and reviewed by the officer's immediate supervisor prior to submission.*

This requirement is designed primarily to help ensure that information submitted to the intelligence function is inclusive of all data necessary to make it useful for intelligence purposes. For example, the ability of intelligence analysts to conduct link analyses and perform other assessments of information in order to make it useful for intelligence purposes is dependent on the scope, detail and accuracy of the raw data and information received. Use of standard reporting mechanisms, to include a supervisory review of all submissions to the intelligence function, is one means of helping to make this possible.

E. Receipt, Analysis and Evaluation of Information

The model policy provides some guidance with regard to procedures for the receipt and evaluation or analysis of information to the intelligence function. Raw data received by the intelligence function must first meet several basic criteria. These include determining whether the information is crime related, whether it is related to the mission of the intelligence function (e.g., is it consistent with the collection plan), and whether the information has been or can be verified. Once affirmative answers have been reached for each of these inquiries, intelligence analysts must determine its reliability and validity. The model policy specifically states in this regard that

> *Where possible, information shall be evaluated with respect to reliability of source and validity of content. While evaluation may not be precise, this assessment must be made to the degree possible in order to guide others in using the information. A record shall be kept of the source of all information where known.*

Information being assessed for intelligence purposes usually lacks the capacity for qualitative assessment. However, some assessment is essential if the information is to be deemed intelligence and used constructively for tactical or strategic purposes.

The model policy recommends that assessments be made of potential intelligence material based on the criteria of reliability and validity. Reliability, sometimes referred to as "source reliability," refers to the degree to which one can depend upon or trust the information source. Validity also referred to as "content validity" relates solely to the trustworthiness of the information received. In many cases, these two elements are closely interrelated. For example, an eyewitness account by a seasoned professional law enforcement officer would normally lead one to assume both strong reliability and validity. But, this may not always be the case and it is good as a matter of practice to evaluate each of these criteria separately.

In meeting this objective, some intelligence operations employ a rating scale or score for each of these assessments. For example, using the above example, an eyewitness police account may be rated "reliable" and scored as "1" on the reliability scale. However, in another scenario, information provided by an informant may be judged as "usually reliable" based on the individual's past performance. In this case, the information may be given a lower reliability rating of "2" indicating that the information can be considered, to a great extent, to be factual and reliable. Using this scheme, a score of "3" would indicate that the source may be sporadic in truthfulness or accuracy and should be regarded with skepticism. Nonetheless, one may wish to retain information with lower scores for a period of time pending its potential verification. However, restrictions should be placed on its dissemination and use until such verification can be made.

Content validity may be similarly rated depending upon the degree to which the information may be corroborated and trusted. Since the source of information factors heavily in the assessment of both the reliability and validity of information used in the intelligence function, the model policy recommends that a record be kept of the source of all information where it is known. The source of information also becomes important where intelligence may be shared outside the originating agency.

The sharing of intelligence between law enforcement agencies is extremely important to the furtherance of intelligence operations on a regional, statewide and national level. But, without some means of evaluating the quality of intelligence in the sharing process and establishing of some controls on the distribution of such information, violations of privacy interests are more likely and invalid or unreliable information is more likely to be regarded as reliable law enforcement intelligence.

In order to control the distribution of intelligence between police agencies, the model policy makes several recommendations. One of these directs that

> *Reports and other investigative material and information received by this agency shall remain the property of the originat-*

ing agency, but may be retained by this agency. Such reports and other investigative material and information shall be maintained in confidence, and no access shall be given to another agency except with the consent of the originating agency.

This directive is an attempt to control the potentially uncontrolled distribution of intelligence between agencies without the knowledge and consent of the originating agency. In addition, prior to distribution, the originating agency should ensure that the recipient individual or agency has a "need and a right to know" such information as defined earlier in this paper. Intelligence should not be distributed without the approval of the intelligence OIC or other agency-designated officer. Further, whenever intelligence reports or information is forwarded to another agency, a record of the transaction should be logged by the originating agency and the transaction predicated upon the understanding that further distribution is prohibited without the originating agency's approval.

The same holds true with regard to the internal distribution of intelligence. Invariably, intelligence operations uncover information of value to tactical or investigative operations within the immediate agency or another local law enforcement agency. For example, in efforts to establish the identity and linkages of members of a street gang to organized crime, intelligence officers may discover that a large quantity of narcotics is scheduled for delivery at a specified location. Such information must be forwarded to the appropriate investigative unit as soon as reasonably possible for appropriate enforcement action. While the intelligence function is not designed or intended to serve as an extension of investigative operations, there will invariably be interface between the two on both a planned and unplanned basis.

Strategic intelligence, on the other hand, is designed with longer term goals in mind, where time is available for developing broad and in-depth information about the operations of criminal enterprises and for purposes of planning more general law enforcement strategies. In this regard, the model policy directs that

Analytic material shall be compiled and provided to authorized sources as soon as possible where meaningful trends, patterns, methods, characteristics or intentions of criminal enterprises or figures emerge.

F. File Status

File status is an important issue in that it has bearing on both the manageability of information within the intelligence function as well as the protection of the rights of persons whose identities are housed within intelligence files.

In the first instance, many intelligence functions tend to resemble the tendency of persons who have difficulty throwing out or giving away old possessions that have outlived their usefulness or value. The underlying motive among many intelligence officers like this is that more information is always better and, even though it may not have immediate value, it may eventually be linked to other information that will make it worthwhile. While on occasion this may prove to be the case, it is the exception rather than the rule. More often, where files remain open without merit or appropriate justification, they become obsolete and may jeopardize the civil rights of persons for whom no rational criminal connections or involvement can be demonstrated.

Where intelligence files remain open indefinitely or without justification and management oversight, they also become part of an on-going work inventory that does not accurately reflect the intelligence function's caseload. They also can serve to inhibit intelligence officers from focusing on priorities and properly managing their time and effort. And, like an extraneous piece of a jigsaw puzzle, obsolete files often serve no other function than to confuse the picture.

In this regard, the model policy suggests that intelligence files be classified as either "open" or "closed." The model policy defines an open intelligence file as one that is actively being worked. It adds: "in order to remain open, officers working such cases must file intelligence status reports covering case developments at least every 180 days." Filing of status reports on a routine basis will help to ensure that files do not become dormant. In order to accomplish this, the intelligence function must maintain an index to intelligence file status in order to ensure that status reports are filed routinely as required.

The model policy defines "closed" intelligence files as

those in which investigations have been completed, where all logical leads have been exhausted, or where no legitimate law enforcement interest is served.

In order to provide a wrap up of case findings and the basis for case closure, the model policy also recommends that

All closed files must include a final case summary report prepared by or with the authorization of the lead investigator.

Some agencies employ additional classifications for their intelligence file, most notably those denoting a "pending" status. While such classifications may be used, they tend to add a layer of confusion into file management. If the use of a pending file status is deemed appropriate for an agency, steps should be taken to ensure that this status can be maintained for only a limited time period.

G. Classification/Security of Intelligence

The importance of intelligence file security should be readily apparent. Concerns for the security of intelligence include matters relating to: the sensitivity of both strategic and tactical information to the law enforcement agency, the identity of confidential informants and other sources of information, the identity of undercover police operatives, the nature of law enforcement tactics and strategies, the status of various sensitive criminal investigations, and protection of the rights of persons who are the subject of intelligence files, among other matters.

In order to protect the security of intelligence, the model policy makes several recommendations. The first of these has to do with the classification of intelligence files. The policy specifies that intelligence will be classified "in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence." In accordance with this recommendation, intelligence files must be classified under the model policy with regard to the sensitivity of information that they contain. A three-tiered system is proposed as follows:

a. Restricted. "Restricted" intelligence files include those that contain information that could adversely affect an on-going investigation, create safety hazards for officers, informants or others and/or compromise their identities. Restricted intelligence may only be released by approval of the intelligence OIC or the agency chief executive to authorized law enforcement agencies with a need and a right to know.

b. Confidential. "Confidential" intelligence is less sensitive than restricted intelligence. It may be released to agency personnel when a need and a right to know has been established by the intelligence OIC or his/her designate.

c. Unclassified. "Unclassified" intelligence contains information from the news media, public records, and other sources of a topical nature. Access is limited to officers conducting authorized investigations that necessitate this information.

The model policy recognizes that intelligence files are modified on an on-going basis and, consequently, that the security classification "must be reevaluated whenever new information is added to an existing intelligence file."

Individual intelligence authorities must make policy determinations regarding the persons and organizations that are generally eligible to receive intelligence in the forgoing categories. However, individual decisions will generally have to be made by the intelligence OIC or his/her designee for release of particular items of intelligence. Factors that have bearing on these decisions are varied but include, for example, assurance that recipients have not misrepresented themselves, that they are authorized to make the request and receive the information, and have a need- and a right-to-know; that disseminations can be made in accordance with law; that the information requested has adequate validity and reliability to be shared, and determination as to whether any conditions concerning the source of the data necessitate limiting its dissemination or adding conditions to its release, among other factors.

When approval of intelligence dissemination has been granted, the outgoing material should be appropriately marked with its security classification and accompanied by any requirements, restrictions or instructions concerning its use or further dissemination. The model policy makes the following statement in this regard:

> *Release of intelligence information in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the express approval of the intelligence OIC and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of this agency's OIC.*

As one authoritative source indicates, "Violation of the third party rule can contribute to serious deterioration of trust and credibility between agencies exchanging intelligence. Respecting the rights of contributing agencies when a third party stipulation is applied to a piece of intelligence cannot be overemphasized."[16]

Before intelligence material can leave the unit, either through internal or external means of dissemination, it must be recorded and indexed by the intelligence authority.[17] Files released under freedom of information provisions or through discovery must be carefully reviewed. Information may be deleted that is not specifically requested or for which the requesting party is not legally entitled under relevant state or federal freedom of information provisions. Information that is properly requested pursuant to these laws and which is otherwise discoverable should be released.

A second form of intelligence security relates to the physical security of intelligence files. The model policy states that

> *All restricted and confidential files shall be secured, and access to all intelligence information shall be controlled and recorded by procedures established by the intelligence OIC.*

Restricted and confidential files should always be maintained in a highly secure environment. Intelligence personnel should be ever mindful of the sensitivity and security of this documentation and consistently follow agency policy as well as any local and state laws regarding intelligence security. Hard copy file security should be practiced at all levels and computer access restricted through physical measures and by means of password and/or other protections. The intelligence facility should be housed in a location that can be fully secured and files secured separately within that location. Access of personnel to this location should be controlled and a record maintained of personnel when they are permitted access. Uncontrolled access to or improper security for intelligence files can have privacy right implications for named individuals and potentially risk harm to witnesses, victims, police officers and informants. In the latter regard, the model policy emphasizes that informant files must be maintained separately from intelligence files just as they should from other investigative files within the agency.[18]

H. Auditing and Purging Files

With time, many intelligence files become little more than historical accounts of unit activity. Intelligence files that are no longer accurate, are not relevant to the mandates of the unit, do not pertain to current intelligence unit interests and activities or contain insufficient supporting documentation are among those that may be purged. When files are deficient in one or more of these areas, consideration may be given to updating or improving them through validation and other means. However, when the basic information contained in these files is of such an age or of such poor quality as to make these efforts either too costly or unproductive, a decision to purge the file may be the most prudent approach. The model policy states in this regard that

> *The intelligence OIC is responsible for ensuring that files are maintained in accordance with the goals and objectives of the intelligence authority and include information that is both timely and relevant. To that end, all intelligence files shall be audited and purged on an annual basis as established by the agency OIC through an independent auditor.*

Further, the model policy states that

> *When a file has no further information value and/or meets the criteria of any applicable law, it shall be destroyed. A record of purged files shall be maintained by the intelligence authority.*

Use of a qualified and experienced outside auditor is often considered the best approach to purging intelligence files in that independent third parties remove much of the bias or the appearance of bias that may be evident when using in-house intelligence personnel. While a yearly review of the files for purposes of purging useless materials is recommended, this does not preclude the destruction of files on an ad hoc basis where appropriate and with approval of the intelligence OIC.

Endnotes

[1] "Interview with Brian Michael Jenkins," *Omni*, November, 1994, Vol. 17, No. 2, pg. 77.

[2] Robert Suro, "U.S. Lacking in Terrorism Defenses: Study Cites a Need to Share Intelligence," *The Washington Post*, Friday, April 24, 1998, pg. A-18.

[3] A discussion of the scope and nature of intelligence and related investigative databases available to state and local government through federal and other auspices is beyond the scope of this document. However, this is a vital area of interest for local and state intelligence operations. For a concise examination of these resources see, for example, "Automated Investigative Databases," *Training Key #460*, International Association of Chiefs of Police, Alexandria, VA.

[4] John J. Carney, "Managing an Intelligence Unit,", in *Issues of Interest to Law Enforcement: Intelligence-The Ultimate Management Tool*, Law Enforcement Intelligence Unit, Sacramento, CA, 1983.

[5] Criminal Intelligence Program for the Smaller Agency, California Peace Officer's Association, *Organized Crime Committee*, October, 1988.

[6] The International Association for Law Enforcement Intelligence Analysts (IALEIA) provides certification programs in this law enforcement discipline and training is offered through a variety of state and national sources to include the state and local law enforcement training program at the Federal Law Enforcement Training Center (FLETC) in Glynco, Georgia.

[7] Peterson, Marilyn B. "Analysts in the 90s: AN IALEIA Survey," *IALEIA JOURNAL*, Vol.

8, No. 1 (1993), p.46; as quoted by Marilyn B. Peterson in "The Professional Law Enforcement Analyst," *Issues of Interest to Law Enforcement: Intelligence into the 21st Century,* Law Enforcement Intelligence Unit, Sacramento, CA, November, 1995.

[8] Peterson, *ibid*. p. 30.

[9] Ferris, James R., "A Model for Police Intelligence Units," in Michael J. Palmiotto (Ed.), *Critical Issues in Criminal Investigation,* 2nd Ed., Anderson Publishing, 1988.

[10] Kelling, George L., Pate, Anthony, Dieckman, Duane, and Brown, Charles E., *The Kansas City Preventive Patrol Experiment: A Technical Report,* The Police Foundation, Washington, DC, 1974.

[11] For a more complete understanding of problem solving and its impact on crime prevention see Herman Goldstein, *Policing a Free Society,* Cambridge: Ballinger Publishing, 1977.

[12] Ferris, op. cite., p.88.

[13] For a comprehensive treatment of the nuances and dilemmas of undercover and intelligence operations see, for example: Gary Marx, *Undercover: Police Surveillance in America,* University of California Press, 1988.

[14] The so-called "sneak and peak warrant" authorizes law enforcement officers to make a clandestine entry, examine the premises and then depart without seizing tangible evidence. They are, in effect, warrants authorizing information-gathering incursions onto a suspect's premises. While they are controversial in some jurisdictions, they have been upheld in at least the prestigious Second Circuit Court of Appeals. See, for example, the Second Circuit's ruling in *United States* v. *Villegas,* 899 F.2d 1324 (2nd Cir. 1990); cert. denied, 498 U.S. 991 (1990), in which the court noted that the federal courts have upheld both the concept of a covert entry and the seizure of intangible evidence. While such warrants are constitutionally acceptable, such warrants for covert entries must not only particularly describe the place to be searched and the visual images to be seized, but also there must be a showing of reasonable necessity for delaying notice of the search and appropriate persons must be notified within a reasonable time after the entry. The failure to meet these requisites will result in the sneak and peak warrant being found to be unconstitutional.

[15] The reader may wish to explore these issues in such publications as *Law Enforcement Policy on the Management of Criminal Intelligence,* International Association of Chiefs of Police, Alexandria, VA, 1985.

[16] *Ibid.,* pg. 45.

[17] For examples of dissemination policy specific to the intelligence function see: *Law Enforcement Policy on the Management of Criminal Intelligence,* IACP. Op. Cite.

[18] For information on informant management and file control see the *Model Policy on Confidential Informants,* National Law Enforcement Policy Center, International Association of Chiefs of Police, Alexandria, VA.

Acknowledgement

This model policy was prepared with the assistance of the IACP Committee for Police Investigative Operations. Special appreciation is extended to the following committee members without whom this effort could not have been accomplished: Peter A. Modafferi, Chairperson, Chief of Detectives, Office of the District Attorney, New City, NY; Gregory R. Albanese, Deputy Chief (ret.), White Plains, NY; Superintendent John P. Boyle, Boston Police Department, Boston, MA; Chief Timothy A. Braaten, Victoria Police Department, Victoria, TX; Chief James J. Charley, Chester Township Police Department, Chester, PA; James H. Convery, Chief Investigator, NJ Division of Criminal Justice, Trenton, NJ; Chief Gregory M. Cooper, Provo Police Department, Provo, UT; Commander Carlo S. Cudio, Los Angeles Police Department, Los Angeles, CA; Robert E. Cummings, Assistant Commissioner, Florida Dept. Of Law Enforcement, Tallahassee, FL; Dennis DeMey, President, Adam Safeguard, Toms River, NJ; Edward J. Doyle, Special Assistant to the Director, Financial Crimes Enforcement Network, Vienna, VA; Thomas Durkin, Asst. VP, Security, Chase Manhattan Bank, Wilmington, DE; William J. Esposito (ret.), Vienna, VA; Emma E. Fern, Criminal Intelligence Analyst, Florida Department of Law Enforcement, Miami, FL; Eugene J. Fields, President, Centurion Services Inc., Harvey, LA; Richard J. Hunt, Section Chief, Intelligence Division, Federal Bureau of Investigation, Washington, DC; Deputy Chief Mike Leyman, Richardson Police Department, Richardson, TX; Chief Robert G. Lowery, Florissant Police Department, Florissant, MO; John McCann, President, McCann & Associates, Bothell, WA; Commander John E. Moran, Los Angeles Police Department, Los Angeles, CA; Deputy Chief Thomas P. O'Connor, Maryland Heights Police Department, Maryland Heights, MO; Chief Thomas O'Loughlin, MA Bay Transportation Authority Police Department, Boston, MA; Gregory J. Regan, Assistant Special Agent in Charge, U.S. Secret Service, Richmond, VA; George A. Rodriguez, Director of Security, Yellow Freight, Overland Park, KS; Captain Kurt F. Schmid, Illinois State Police, Chicago, IL; Michael C. Stenger, Special Agent in Charge, U.S. Secret Service, Washington, DC; Chief Thomas F. Wagoner, Loveland Police Department, Loveland, CO; Chief Ken A. Walker, Lubbock Police Department, Lubbock, TX; Chief Joseph Polisar, Garden Grove Police Department, Garden Grove, CA.

This project was supported by Grant No. 2000-DD-VX-0020 awarded by the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. The Assistant Attorney General, Office of Justice Programs, coordinates the activities of the following program offices and bureaus: the Bureau of Justice Assistance, the Bureau of Justice Statistics, National Institute of Justice, Office of Juvenile Justice and Delinquency Prevention, and the Office of Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the United States Department of Justice or the International Association of Chiefs of Police.

Every effort has been made by the IACP National Law Enforcement Policy Center staff and advisory board to ensure that this model policy incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that no "model" policy can meet all the needs of any given law enforcement agency. Each law enforcement agency operates in a unique environment of federal court rulings, state laws, local ordinances, regulations, judicial and administrative decisions and collective bargaining agreements that must be considered. In addition, the formulation of specific agency policies must take into account local political and community perspectives and customs, prerogatives and demands; often divergent law enforcement strategies and philosophies; and the impact of varied agency resource capabilities, among other factors.