LAW ENFORCEMENT POLICY CENTER

Surveillance

April 2009

IACP®
International Association of Chiefs of Police

The IACP Law Enforcement Policy Center creates four types of documents: Model Policies, Considerations Documents, Concepts & Issues Papers, and Need to Know one-page summaries. Typically, for each topic, either a Model Policy or a Considerations Document is created, supplemented with a Concepts & Issues Paper. This file contains the following documents:

- ***Model Policy****:* Provides police agencies with concrete guidance and directives by describing in sequential format the manner in which actions, tasks, and operations are to be performed.
- ***Concepts & Issues Paper****:* Designed to provide context and background information to support a Model Policy or Considerations Document for a deeper understanding of the topic.

Model Policy

Updated: April 2009

Surveillance

I. Purpose

It is the purpose of this policy to provide general principles for conducting surveillance operations and establishing internal control processes and procedures to ensure the protection of individuals' civil rights and to ensure the efficiency and the effectiveness of surveillance operations.

II. Policy

Surveillance operations are essential for criminal investigations and information collection required to develop intelligence. However, covert and clandestine methods may be neither appropriate nor necessary and, if used, can have associated risks. Surveillance is suitable only for those types of investigations where information of comparable investigative value cannot be obtained by other less intrusive means and is permitted only when reasonable suspicion of criminal activity has been established. It is the policy of this law enforcement agency to employ surveillance methods only where they can be justified in accordance with principles and operational protocols established in this policy.

III. Definitions

Compelling Governmental Interest: The determination that the interests of privacy, freedom of expression, and related constitutional guarantees are outweighed by the nature and magnitude of the likely harm should the suspected criminal activity continue.

Expressive Association: The constitutional right of individuals to gather without undue governmental interference, for the purpose of engaging in activities protected by the First Amendment, such as freedom of speech, assembly, and the exercise of religious beliefs.

Reasonable Suspicion: Articulable circumstances that would cause a trained law enforcement officer to reasonably believe that activity relating to a definable criminal activity or enterprise has occurred, is occurring, or is reasonably likely to occur.

Surveillance: A general term that can be characterized in part by the degree of invasiveness of surveillance tactics and technologies. For purposes of this policy, this includes surveillance in any form— monitoring, surveillance, and undercover operations— whether intended to collect aural or visual information.

- *Monitoring:* Short-term, preliminary observation of an individual, group, or organization to gather information to determine whether criminal activity is taking place, has taken place, or is about to take place.

- *Surveillance:* The continuous or prolonged observation of a targeted individual, group, or organization by clandestine means to gather information relative to an open criminal investigation. Surveillance differs from monitoring in that it typically involves the use of more invasive tactics such as electronic monitoring.
- *Undercover Operation:* An approved criminal investigation using an officer (or officers) generally under an assumed name or cover identity to infiltrate a group or organization in order to obtain information through the development of personal relationships and other approved information-gathering methods.

Sensitive Circumstances: For purposes of this policy, sensitive circumstances exist if there is a reasonable expectation that the operation will involve, or becomes involved in, investigation of criminal conduct by (a) an elected or appointed federal, state, or local government official or political candidate; (b) a religious, political, or media organization or personage; or (c) when evidence reasonably suggests systemic corruption of a governmental function. It also includes involvement in, or a reasonable expectation that, an undercover officer will become involved in (a) facilitation of, or become party to, the commission of a felony or other serious crime; (b) be arrested; (c) participate in any activity that would breach confidential or privileged communications of individuals under investigation or third parties; or (d) activities that carry a significant risk of violence or physical injury.

IV. PROCEDURES

A. Limitations on Monitoring, Surveillance, and Undercover Operations

1. The following prohibitions shall be observed when requesting authorization and reviewing requests for surveillance and undercover operations. The following are prohibited by this law enforcement agency:
    a. Illegal means of collection, maintenance, and dissemination of information.
    b. Collection, maintenance, or dissemination of information without reasonable suspicion.
    c. Collection of information on suspects' political or religious beliefs or sexual activities that is not or cannot be linked reasonably to a criminal activity.
    d. Dissemination of information of investigative interest to any individual or organization that does not have a need and a right to know.
    e. Conducting surveillance or undercover operations on advocacy groups and others engaged in expressive association without a compelling state interest that has been established by a recognized authority or a reasonable suspicion of criminal activity. This includes prohibitions on infringement of constitutionally guaranteed rights of privacy; the ability to receive, hold, and express ideas; to dissent freely; to write and to publish; and to associate publicly and privately for any lawful purpose.
2. Surveillance of individuals or organizations shall not exceed the scope or intent of activities defined in the approved request for surveillance.

B. Request for Authorization

1. A request for authorization to initiate surveillance or undercover operations shall be prepared by the lead investigating officer and must be endorsed by a supervisor and approved by management prior to initiation of operations.
2. Requests shall address, but shall not necessarily be limited to, the following issues:
    a. Specific facts and circumstances upon which reasonable suspicion of criminal activity is based.
    b. Identification of objectives and anticipated end results of the operation.
    c. Anticipated duration of the operation and timeline for activities, where applicable.

d. Means and methods for conducting the operation with particular emphasis on any anticipated or planned clandestine methods and equipment.
e. Other less intrusive measures that have been tried or considered to obtain targeted information and the basis upon which they were rejected.
f. Informants who will or may be used; the informant's criminal history, demonstrated reliability, and anticipated financial compensation or other consideration.
g. Anticipated line-item costs of the operation.
h. Risks associated with the operation, including the following:
    i. Risk of personal injury, property damage, financial loss, or damage to departmental image/reputation that may result in a loss of public confidence, support, or both;
    ii. Risk of civil liability;
    iii. Risk of violating legal rights, including privileged or confidential communications (e.g., attorney-client privilege);
    iv. Risk of officer involvement in illegal activity, including the potential type and scope of involvement;
    v. Other potential risks to officers, suspects, third parties, or the department;
    vi. Risk of not undertaking the operation.

C. Approval Process and Supervision

1. Evaluation of request to conduct surveillance or undercover operations shall be based on, but not necessarily be limited to, assessment of the following factors:
    a. Whether the facts, circumstances, events, and other matters identified in the request are sufficient to establish reasonable suspicion.
    b. Whether less intrusive means that could reasonably be expected to accomplish the same or similar goals have been sufficiently used or considered.
    c. Whether the perceived risks are realistic, complete, and provide reasonable justification for the operation.
    d. Whether the identified operational tactics are reasonably justified based on the stated goals and expected results of the operation.
    e. Whether the anticipated budget for the operation is reasonable in relationship to the anticipated operational outcomes, community benefits, and departmental priorities and budget.
    f. Whether there are unreasonable risks of violating the civil liberties of suspects or third parties, or interfering with privileged or confidential communications absent a compelling governmental interest.
    g. Whether it is reasonably likely that officers will become involved in unlawful investigative tactics or be party to the planning, commission, or instigation of serious criminal acts.
    h. Whether there is a reasonable possibility that the officer will be forced to commit violence that is not required for self-defense.
    i. Whether it is reasonable to believe that the investigation may involve sensitive circumstances.
2. Approval process
    a. Requests for surveillance operations shall be submitted to the appropriate supervisor or commanding officer for purposes of authorization.

b. Requests for undercover operations shall be submitted to the appropriate commanding officer for recommendation and then to the department's chief executive officer (CEO) for final determination.

c. Any surveillance or undercover operation that may reasonably involve sensitive circumstances or a substantial commitment of funds must be approved by the agency CEO and, in accordance with his or her discretion, by the appropriate prosecutorial agency.

d. Under exigent circumstances, a request to conduct surveillance may be submitted verbally to an officer's commander using supporting justification as outlined in this policy and followed by a written request in a timely manner. Undercover operations are not subject to exigency exemptions.

e. Both surveillance and undercover operations shall be approved for a period of time consistent with the scope and goals of the operation. Normally, this should not exceed 120 days but may be subject to continuation beyond that time frame upon review.

3. Supervision and Case Review

a. Surveillance and undercover operations may not continue longer than is necessary to achieve objectives defined in the authorization.

b. Continuation beyond 120 days requires reauthorization by the department CEO after consideration of the supervisory officer's showing of sufficient progress and potential for future success.

c. Case reviews between the lead investigator and his or her supervisor shall be conducted monthly at a minimum. Surveillance or undercover investigations may be suspended or terminated at any time due to insufficient progress in attaining established goals, budget overruns, or for other reasons deemed sufficient by the supervisory or commanding officer.

d. As soon as reasonably possible, officers shall report to their supervisor any investigations that become or are likely to become involved in sensitive circumstances.

e. Officers involved in joint undercover operations shall be held to the principles, tactics, and procedures herein and to those additional requirements specified in this department's policy on Multijurisdictional Investigative Teams.

D. Records Review, Sharing, and Purging

1. Information collected during surveillance and undercover operations shall not be maintained unless it is material to an ongoing investigation authorized by the department.
2. Information collected, including, but not limited to, inquiries, contacts, investigative notes, drafts, and other writings shall be maintained in the investigator's working files until such time that it is linked to the targeted investigation or creates the basis for a separate investigation. Working files shall not be comingled with open criminal case files or intelligence files unless they are purposely being consolidated as a criminal investigation.
3. This department shall not share any investigative case information about subject individuals with intelligence agencies unless the threshold of reasonable suspicion to connect them with present or planned criminal activity has been established.
4. Supervisory and command staff shall ensure that, prior to archiving, criminal case files will be reviewed for information that is misleading, obsolete, otherwise unreliable, or inconsistent with the threshold standard of reasonable suspicion and that such information is purged in a timely manner as prescribed by law or departmental policy.

Every effort has been made by the IACP Law Enforcement Policy Center staff and advisory board to ensure that this document incorporates the most current information and contemporary professional judgment on this issue. However, law enforcement administrators should be cautioned that 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. Readers outside of the United States should note that, while this document promotes procedures reflective of a democratic society, its legal basis follows United States Supreme Court rulings and other federal laws and statutes. Law enforcement administrators should be cautioned that each law enforcement agency operates in a unique environment of court rulings, state laws, local ordinances, regulations, judicial and administrative decisions, and collective bargaining agreements that must be considered and should therefore consult their legal advisor before implementing any policy.

Concepts & Issues

Updated: April 2009

Surveillance

I. Introduction

A. Purpose of the Document

This paper is designed to accompany the *Model Policy on Surveillance* 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. 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 law enforcement agency.

B. Background

Surveillance, in its broadest sense, incorporates the many means available to gather information on individuals, from the traditional forms of watching and tracking activities of suspects to gathering detailed information on suspects through technological means and covert undercover operations. As technological advances are made, many additional forms of surveillance are being added to the police tool kit, particularly through electronic means. In large part, the motivation to develop and use these new technologies has been driven by the need to prevent terrorist attacks, but they are still highly valuable in investigation of such crimes as loan sharking, drug trafficking, trafficking in stolen property, gambling, extortion, smuggling, bribery, and corruption of public officials.

Since the 2001 terrorist attacks on American soil, law enforcement has been operating in a high-stakes environment. The emphasis of American policing has shifted its focus to prevention through early warning, threat assessment, and overall enhancement of information gathering and intelligence sharing. Surveillance is one approach to providing early warning that has established its importance in preventing terrorism and conventional crime. Even in today's environment, there remain legal and practical limitations that officers and their law enforcement agencies must observe if they are to avoid the accusations and charges of privacy violations that have affected others.

Additionally, law enforcement agencies continue to operate on limited budgets that require prudent oversight of expenditures and resource allocations. This necessitates that supervisors and command staff continuously monitor the cost effectiveness of surveillance and similar operations. These are among the primary issues addressed in the model policy on surveillance and this companion paper.

Publications of the IACP Law Enforcement Policy Center
44 Canal Center Plaza, Suite 200, Alexandria, VA 22314

C. Legal Limitations and Restrictions on Surveillance

In *Katz* v. *United States*,[1] the U.S. Supreme Court ruled that a person's Fourth Amendment privacy rights are determined (1) by the individual's actual or subjective expectation of privacy in an area or item and (2) whether society is prepared to accept such expectation as reasonable. However, this two-pronged criterion does not easily resolve many fact-based situations where the competing interests of individuals and the state are played out. In most instances, the courts have attempted to find a reasonable balance between the rights of individuals to privacy and the interests of government to prevent terrorism and other crimes.

As surveillance technology has provided increasingly more sophisticated tools, their adaptation and use by the police has formed the basis for additional court challenges. Charges against the police have most often been lodged in cases in which law enforcement has used warrantless surveillance or searches to accomplish its objectives. Over the years, systematic advancements in electronic surveillance have been the focus of court interpretation.

For example, in the 1992 case of *United States* v. *Smith*,[2] the U.S. Court of Appeals for the Fifth Circuit ruled on whether police interception of a cordless telephone conversation violated the Constitution and Title III of the Omnibus Crime Control and Safe Streets Act. The court dismissed the Title III appeal and turned to the determination of whether cordless phone technology—which uses a radio signal—is more like the use of radio transmission, which is not protected under the Fourth Amendment, or land line communication, which is protected. The court ruled that Smith's subjective expectation of privacy could not be argued as reasonable in using the cordless device but noted that, as cordless telephone technology advances making cordless phone conversations more private, the issue of Fourth Amendment protection will need to be reconsidered.

A similar technology came into question in 2001 in a case involving police surveillance of a home using a thermal-imaging device to detect marijuana cultivation.[3] The U.S. Supreme Court ruled that when a law enforcement agency "uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."[4]

More recently, in an effort to counteract terrorism in the United States, Congress enacted the Patriot Act that revised more than a dozen federal laws to enhance surveillance and intelligence gathering primarily through electronic intercepts. While these are applicable only to federal law enforcement, passage of this act clearly signaled a need to enhance law enforcement surveillance at all levels of government.

Another technology that has been relatively recently adapted to law enforcement use is the Global Positioning System (GPS). Like other evolving technologies before it, GPS has undergone judicial review in a number of jurisdictions with mixed outcomes based on interpretations of state constitutions and case law. The essence of most of these decisions turns on the manner in which the device is used in the factual setting. In general, court decisions tend to allow the warrantless use of GPS devices if they are placed on the exterior of a vehicle; that is to say, their placement does not require entering the passenger compartment of the vehicle or opening the hood, for example, to wire the device to the battery as an energy source. The courts also generally require that warrantless placement of GPS devices be performed while the vehicle, boat, or other conveyance is parked or situated in a public area. Finally, warrantless use of GPS devices is generally easier

[1] *Katz* v. *United States*, 389 U.S. 347, 88 S.Ct. 507 (1967).

[2] *United States* v. *Smith,* 978 F.3d 181 (5th Cir. 1992).

[3] *Kyllo* v. *United States*, 33 U.S. 27, 121 S.Ct. 2038 (2001).

[4] Id. at 2046.

to justify if used to track a vehicle while in a public area—a difficult requirement to meet, but one with solutions that will be noted later.[5]

There are many legal issues that may be raised concerning GPS devices to include, as noted, whether they can be used to track vehicle movements in locations where there is a reasonable expectation of privacy; whether they can track vehicles out of the jurisdiction of a state-issued search warrant; and whether officers can apply a GPS surreptitiously for surveillance if state law requires them to provide the subject with a copy of a warrant—a requirement that would negate the covert advantage offered by the GPS. Some jurisdictions have resolved these issues, while many others have yet to either consider or fully resolve them. Here as in most instances of search and seizure, police are on far more solid legal ground if time and circumstances allow them to obtain a search warrant.[6]

II. PROCEDURES

A. Forms of Surveillance

Given that police surveillance is a proven necessity in many investigations and new technologies will continue to be introduced that can enhance this function, the question becomes how can police manage surveillance operations and the devices employed without invoking judicial resistance that could potentially result in disallowing their use? The answer lies largely in how a department manages and supervises surveillance operations.

First, the level of supervision and oversight required depends on the type of surveillance in question. For the purposes of this discussion, three levels of surveillance have been identified in the model policy based on the common characteristics of their operations. Admittedly, specific surveillance operations do not always lend themselves to easy classification, as some aspects common to one may overlap or be shared with that of another. This conceded, the classifications used herein are termed "monitoring," "covert surveillance," and "undercover operation."

- ***Monitoring:*** Short-term, preliminary observation of activities of an individual, group, or organization for purposes of gathering information. Generally for purposes of determining whether a criminal investigation should be opened, monitoring includes, but is not limited to, transient observation of suspicious persons or activities.
- ***Covert Surveillance:*** The continuous or prolonged observation of a targeted individual, group, or organization by clandestine means for the purpose of gathering information relative to an open criminal investigation. Often this involves the use of invasive tactics such as electronic or related forms of eavesdropping
- ***Undercover Operation:*** An approved criminal investigation using an officer (or officers) generally under an assumed name or cover identity to infiltrate a group or organization in order to obtain information about individuals through the development of personal relationships and other approved information-gathering methods.

[5] Police officers must be familiar with the law and court decisions in their state. For example, Washington State has deemed the installation and monitoring of GPS tracking devices to be a search under the state constitution that requires issuance of a warrant supported by probable cause. See: *State* v. *Jackson*, 76 P.3d 217 (Wash. 2003). Compare to New York State that allows warrantless use of GPS under controlled conditions. See: *New York* v. *Weaver*, 52 A.D.3d 138 (N.Y. 2008) New York Supreme Court, Appellate Division, Third Judicial Department, June 5, 2008. The court noted in its ruling that "…the GPS was not wired into the electrical system of Weaver's van, was not placed in the interior of the vehicle and did not record the vehicle's movements on private property. All three of these factors have been cited by federal courts that have considered police use of GPS devices as requiring a warrant." See also, *U.S.* v. *Garcia*, U.S. Court of Appeals, 7th Cir. No. 06-2741, Feb 2, 2007 (supporting use of GPS memory tracking unit without a warrant based on reasonable suspicion).

[6] The overall issue of police GPS use continues to meet objections from civil liberty groups as witnessed in a recent friend-of-the-court brief filed March 3, 2009, by the Electronic Frontier Foundation and the American Civil Liberties Union of the District of Columbia. The case, *United States of America v. Lawrence Maynard and Antoine Jones* is currently before the U.S. Court of Appeals for the District of Columbia. The brief argues that FBI agents should have obtained a court order before secretly planting a GPS device on the vehicle of a drug trafficking suspect. The GPS device was planted on the subject's vehicle while it was parked on private property. The brief notes in part that "Absent a warrant requirement, the police could track unlimited numbers of members of the public for days, weeks, or months at a time, without ever leaving their desks."

Monitoring is the least intensive surveillance alternative in terms of the potential for implicating Fourth Amendment protections. The forms of observation and information gathering employed here are generally an extension of the types of observation and individual scrutiny that patrol officers utilize on a daily basis. When an individual or group of individuals becomes the target of focused surveillance, information gathered as a result should be shared with a supervisor or other departmental personnel to determine whether sufficient grounds can be established to open a criminal investigation. Officers should not engage in protracted, focused surveillance without informing their shift supervisor.

The remainder of this document focuses on procedures that should be followed when conducting covert surveillance or undercover operations.

B. Operational Planning Concerns and Safeguards

There are several general safeguards and precautions that should be observed when planning or conducting either covert surveillance or undercover operations.

First, the use of illegal means to gather information on individuals or organizations should be prohibited in most cases. Some departments issue blanket prohibitions on officers engaging in illegal acts during covert operations. If this policy is preferred, it naturally limits the types of surveillance and undercover operations that can be pursued. Before implementing such a rule or policy, it should be acknowledged that undercover agents may in some instances be forced, for their own safety, to engage in or be a party to a crime. Failure to do so could result in the officer's death and the death of informants or others. Of course, every effort should be made to avoid such contingencies and means to avert, mitigate, or intervene in such actions should be examined during the operational planning stage. Where criminal acts could reasonably result in bodily harm to innocent third parties, the safety of those individuals should be of paramount concern. When unexpected circumstances pose a reasonable possibility that unacceptable harm may come to persons or property, or the possible harm is disproportionate to the potential good served by continuing the operation, officers should be prepared to curtail the operation even if that means exposing their identity and taking enforcement action if they can do so without unreasonable risk to their safety

An exception to imposing a blanket prohibition against engaging in crime while undercover must be made in instances in which departments approve undercover sting operations and storefront–style undercover operations that by necessity involve the purchase of stolen merchandise. In these cases as well, officers should be familiar with and prepared to prevent or intervene in acts that could result in unacceptable harm.

Whether departments prohibit or accept certain criminal acts performed by undercover officers, they must always be prepared for unintended negative consequences that are an inherent risk in such operations. For example, officers engaged in undercover fencing of stolen vehicles may unwittingly provide a convenient opportunity for individuals to steal vehicles that may not otherwise have been stolen. Unfortunately, there have even been cases where suspects have inflicted serious bodily harm and death in the commission of motor vehicle and other thefts, the proceeds of which they intended to sell to undercover police officers. In short, officers should be acutely aware of the potential for these and other types of negative outcomes that can inadvertently be set in motion by use of covert surveillance or undercover operations.

There are also a number of other potential risks involved in covert and undercover operations of a reputational nature. Should an undercover operation result in violence, death, or other personal or financial injury to innocent third parties, a negative public response may result. If uninvolved third parties are inadvertently caught up in the undercover net cast by the police operation, similar negative public relations can ensue that could damage the reputation of the department and its ability to work with affected elements of the community. This is often the case in drug buy-bust operations and particularly when informants are placed in key roles to interface with suspects. These undesirable outcomes cannot always be foreseen or prevented. However, they should be identified and acknowledged during the planning stages of such operations, and officers and their departments should be prepared to implement safeguards and handle contingencies.

Several policies should also be followed in the design and implementation of covert surveillance and undercover operations as noted in the model policy.

For example, it should be an axiom of covert police activities that the intended operational objective be proportional to or consistent with the risks that could reasonably be anticipated. The physical risks to innocent third parties and police officers; financial costs to the department; risks of Fourth Amendment infringements and possible civil liability or entrapment; possible damage to the department's reputation; and related matters should be compared to the potential benefits that may result from a successful operation. Where the costs or risks of an operation are disproportionate to the good that could reasonably result from the operation's successful conclusion, alternatives to the proposed surveillance should be considered. Moreover, one should routinely explore alternatives that could potentially achieve the same objectives before applying for permission to engage in covert activities. The wide array of information resources now available through both the public and private sectors can often provide enough information to limit or serve as an effective alternative to otherwise costly and more risky forms of surveillance.

One should also ask: What is the extent of the overall threat to the community posed by the targeted criminal activity? Although crime of all types deserves police investigation, some forms may not justify the risks inherent in covert police actions.

The urgency of the case should also be factored into this equation. A criminal activity that must be terminated immediately (for example, anticipated gang violence) versus one that does not entail the same level of urgency (such as a petty theft ring) may be dealt with differently, whether through covert surveillance, undercover operations, or alternative approaches.

In some instances, alternatives can be found where there are legal concerns about certain covert surveillance techniques. While they may require additional time and effort to gain judicial approval, there may be legally acceptable procedures for engaging in certain forms of surveillance that should be followed when reasonably possible. For example, intrusion into areas where there is an expectation of privacy in order to observe and record can be judicially authorized in some jurisdictions by issuance of so-called "sneak and peak" warrants. It is also possible under the law in some states to obtain legal permission to delay service of a warrant until after surveillance has taken place, thus giving officers the opportunity to gather necessary information without alerting the subject under investigation. Such approaches should be explored in cooperation with competent legal counsel prior to proceeding with certain types of covert surveillance, rather than after they have been put into use and information has been collected.

Another issue with respect to operational planning involves the use of informants generally, and juvenile informants in particular. The problems and risks inherent in the use of informants are recognized widely in law enforcement and those problems can be magnified if informants are used in undercover or surveillance roles. Informants are used widely in drug investigations. In these instances, it is often difficult for police to prohibit them totally from some level of criminal activity if they are to be useful and abide by agreements with law enforcement agencies. Depending on the reliability of the informant, there is always the inherent risk of compromising a major police operation and risking the lives of police officers and others when informants are used in undercover or covert surveillance settings.

The use of juvenile informants adds additional potential risks. Any police informant runs some degree of risk of exposure, the exact degree of danger depending upon many factors, such as the type of crime and the experience of the informant. With juvenile informants, such risks may be greatly magnified. A juvenile is often more vulnerable to detection and retaliation than an adult informant. The danger is directly proportional to the seriousness of the criminal activity and the relative street smarts of the youth informant. A juvenile may be less steadfast in motivation and less able to avoid detection or withstand pressure once suspected by the persons upon whom he or she has been sent to inform. Identification by the suspects of the juvenile as a police informant not only poses a severe risk to the safety of the informant but also ends that informant's usefulness and can result in collapse of the entire police operation. There is also the risk to the officer and the department of public outcry and civil liability if the use of the juvenile informant

results in his or her injury or death. Unfortunately, there have been a number of instances nationwide in which this is the result.[7]

Regardless of age, an informant must have the maturity and intelligence to understand the risk involved. No informant should be sent into harm's way without a full understanding of the dangers associated with the mission. Whether the informant is offering services to the police voluntarily or is under some form of compulsion can also make a difference. Some juveniles volunteer information and even offer to act as informants on a continuing basis. Others act as informants in the hope of avoiding prosecution or reducing punishment. Police must judge not only the type but also the level of motivation of the informant. Most importantly, when the decision is made to use an informant, officers must ask whether they have a reasonable plan to monitor the actions and location of the individual and extract the informant from danger in the event of discovery.

Another potential problem related to surveillance operations involves the inadvertent collection of information on subjects and third parties that is sensitive and not relevant to the investigation. Officers should not collect information on suspects' political or religious beliefs or sexual activities unless these activities and beliefs have a direct connection to the criminal investigation at hand and are reasonably believed to be relevant to case development. Often, in the course of conducting electronic or other forms of surveillance, one cannot help but encounter information of this kind. This is frequently the case and a practical necessity of conducting wiretaps and related operations. It is also a factor that must be anticipated when using beepers or GPS devices where, in recording the location of vehicles, it is likely that location information will include places where there is an expectation of privacy. A minimization requirement[8] coupled with judicial oversight (often employed in federal wiretap warrants) may also be extended to the use of GPS devices in some jurisdictions. This and similar issues should be discussed with competent legal counsel.

Finally, monitoring, surveillance, or undercover operations should not target advocacy groups engaged in expressive association unless a compelling state interest can be established by competent legal authority. Expressive association is a term used to identify individuals and groups that are engaged in First Amendment protected practices of speech, assembly, and exercise of religion. Compelling interest means that before engaging in these forms of undercover or surveillance operations, there must be a determination by competent legal counsel that the constitutional guarantees of the individual or group are outweighed by the nature and magnitude of possible harm that could reasonably be expected if the presumed criminal activity of the suspect were allowed to continue. While such surveillance was more common during the civil unrest of the 1960s and 1970s, it remains an area of concern as police agencies today respond to the threat of foreign and domestic terrorism and the ongoing scourge of drug trafficking and distribution.

C. Authorization Procedures

To manage covert surveillance and undercover activities and help protect officers and police departments against some of the risks and problems previously mentioned, officers should submit a request for authorization via written application or similar means to their supervisor for consideration and to management for final review. The authorization request, depending on the nature and significance attached to the proposed operation, should address several issues, to include the following. In exigent circumstances, these issues can be addressed to the appropriate authority by telephone or other means and subsequently documented in written format.

- Review the specific facts and circumstances on which reasonable suspicion of criminal activity is established.

[7] Scott Martelle and Bonnie Hayes, "Chad McDonald's Short, Tragic Life," *Los Angeles Times*, April 5, 1998.

[8] See: U*nited States of America* v. *Brown*, 303 F.3d 582 (5th Cir. 2002), "Although 18 U.S.C. § 2515 requires minimization, it does not 'require government agents to avoid intercepting all nonrelevant conversations when conducting a wiretap investigation.' On the contrary, the practical necessities of conducting a wiretap may, in some circumstances, inevitably lead to the interception of some conversations outside the scope of the wiretap order." (citing *United States* v. *Hyde*, 574 F.2d 856, 869 (5th Cir. 1978)) And, "The government's efforts to minimize interception of non-pertinent conversations 'must be "objectively reasonable" in light of the circumstances confronting the interceptor.'" (citing *United States* v. *Banston*, 182 F.3d 296, 307 (5th Cir, 1999) quoting 18 U.S.C. § 2518(5)).

- Identify the objectives and anticipated end result(s) of the operation.
- Where appropriate, forecast the duration of the operation and proposed timeline for activities. A problem that can arise in surveillance is determining the point of diminishing returns—when the investments of time and materials needed for the operation no longer provide proportionate returns with respect to case development. Individuals involved directly in the operation are not always in the best position to make this determination.
- Identify the means and methods for conducting the operation with emphasis on clandestine technology and tactics. Examples of the potential legal complications associated with using various forms of technical surveillance have been examined. This is an appropriate point in which these and other tactics can be reviewed for legal soundness and officer risk. The potential for and means to avoid potential charges of entrapment should also be noted.
- Discuss whether other less intrusive means have been undertaken or considered to gather needed information and the reasoning behind their rejection or failure to succeed. In some cases, the use of less expensive and less labor-intensive means can be identified to achieve the same objective. For example, use of Internet resources and outsourcing information gathering to private sector groups are among numerous options.
- Provide the criminal history and demonstrated reliability of any criminal informants that the officer plans to use.
- Provide a breakdown of costs in line-item format.
- Include any perceived risks involved in the operation, to include the risks of personal injury, property damage, or damage to the department's reputation; civil liability to officers and the department; violation of constitutional rights to include violations of privileged or confidential communications; and the risks of officer involvement in illegal activity.
- In light of all factors noted, identify the reasonable impact if the covert surveillance or undercover operation is not undertaken.

Supervisory personnel must weigh the cost-benefits of each of these and related issues in order to make a decision about whether or how to proceed with a surveillance or undercover operation. Proposed covert surveillance that exceeds commonly accepted operational, financial, or related factors and all undercover applications should be forwarded to the department chief executive for final decision.

One of, if not the most important determination that must be made prior to approval of any surveillance operation is whether there is reasonable suspicion to proceed. Surveillance and undercover operations in particular, are suitable for those types of investigations where information of a comparable investigative value cannot be obtained by other less intrusive means and should be permitted only when reasonable suspicion of criminal activity has been established. This threshold is met when information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise.

Additionally, operations that will or may reasonably involve sensitive circumstances should receive departmental approval and, at the discretion of the chief executive, approval of the prosecutor. Sensitive circumstances in this context relates to surveillance that will or may involve criminal conduct by elected or appointed federal, state, or local government officials or political candidates; religious, political, or media organizations or personages; or when there is reason to believe that systemic government corruption will be discovered. It also includes the involvement of, or reasonable expectation that, an undercover officer will facilitate or otherwise become party to the commission of a felony or other serious crime; be arrested; participate in any activity that would breach confidential or privileged communications of individuals under investigation or third parties; or become involved in activities that carry a

significant risk of violence or physical injury to the officer or others. Other factors that should be considered in the approval process include the following:

- Whether less intrusive, risky, or costly measures have been sufficiently considered that could be expected to accomplish the same goal.
- Whether the operational tactics are justified based on the goals and objectives of the operation and the nature of suspects involved.
- Whether the budget for the operation is reasonable and in line with the department or unit's budget.

These factors should, to the degree possible, be identified in the application for surveillance or undercover operations. Here, and with all applications, supervisory or command staff members should modify or disapprove the application depending on their assessment of the circumstances.

Approval of a surveillance or undercover operation should be limited to a specific time frame (generally not more than 120 days) during which progress on initiatives should be periodically reviewed. Continuation beyond this designated time frame should require reauthorization by the department recognizing that covert operations should be continued only so long as necessary to achieve stated goals.

Case review is important to the success of surveillance and undercover operations. Reviews by the lead investigator should be conducted at least every 30 days and should cover achievements and problems related to the points previously noted in the application. Covert surveillance and undercover operations should be subject to modification, suspension, or cancellation depending on success of initiatives and evaluation of other developments.

D. Records, Review, Sharing, and Purging

Information collected during covert surveillance and undercover operations should not be retained in an active file unless it is material to an ongoing, approved departmental investigation. Information that cannot be linked to an approved or developing investigation should be maintained in an investigator's working folder until such time that it is linked to an investigation or creates a separate investigation. Such information should not be comingled with case files or intelligence files.

Officers should also be cautious of providing information of investigative interest to any individual or organization that does not have a need and a right to know. In all cases, information must not be shared about subject individuals unless the threshold of reasonable suspicion to connect them with present or planned criminal activity has been established. This is particularly important when providing information to centralized state or regional intelligence centers and fusion centers where information of this and other types can be further distributed beyond the department's control. Investigative information once disseminated tends to take on greater authority than it may merit when viewed by other jurisdictions.

International Association of Chiefs of Police
44 Canal Center Plaza, Suite 200
Alexandria, VA 22314
703.836.6767 | FAX 703.836.4743
www.theIACP.org