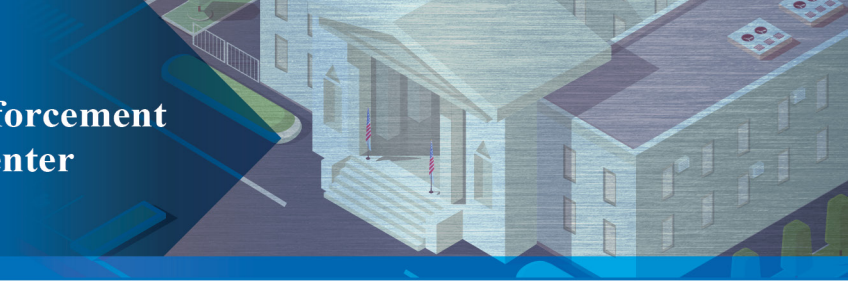


Confidential Informants

December 2020

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.
- *Considerations Document*: Offered as an alternative to the bright-line directives found in a Model Policy. Instead of providing exact policy language, the Considerations Document outlines items that agencies should address and provides options that agencies should examine when developing their own policies on the topic.
- *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.
- *Need to Know...*: Synthesizes the key points of the topic into a brief, one-page overview. This document is developed by Policy Center staff following the final approval of the policy and paper.



Model Policy

Updated: December 2020

Confidential Informants

I. PURPOSE

In some instances, a successful investigation cannot be conducted without the use of confidential informants (CIs). While the use of CIs can be an effective tool, it can be undermined by misconduct of the CI or improper management by the handler. The purpose of this policy is to provide protocols for the control and use of CIs.

II. POLICY

It is the policy of this law enforcement agency to take necessary precautions when utilizing CIs by developing sound informant control procedures.

III. DEFINITIONS

Confidential Informant (CI): An individual, under the direct supervision of an enforcement officer, who is provided with a reasonable expectation of confidentiality, and who furnishes information about suspected criminals or criminal activity for consideration, either financial, prosecutorial, or judicial; or a person who actively participates in a criminal investigation or intelligence operation under the direct supervision of an enforcement officer with or without compensation.¹

Confidential Informant File: File maintained to document all information that pertains to a CI.

Unreliable Informant File: File containing information pertaining to an individual who has failed at following an established written CI agreement and has been determined to be generally unfit to serve as a CI.

Compelling Public Interest: For purposes of this policy, situations in which failure to act would result or likely result in loss of life, serious injury, or have some serious negative consequence for persons, property, or public safety and therefore demand action.

Handler: The officer primarily responsible for supervision and management of a CI.

¹ Agencies should consult local laws and regulations to determine to what degree confidentiality can be provided.

IV. PROCEDURES

A. Initial Suitability Determination

An initial suitability screening will be conducted on any individual being considered for a role as a CI. This screening includes the following steps:

1. An officer requesting use of an individual as a CI shall complete an Initial Suitability Report. The report shall be submitted to the appropriate individual or entity, as determined by the agency chief executive, to review for potential selection as a CI. The report shall include sufficient detail regarding the risks and benefits of using the individual so that a sound determination can be made. The following information shall be addressed in the report, where applicable:
 - a. Age, sex, and residence
 - b. Employment status or occupation
 - c. Affiliation with legitimate businesses and illegal or suspicious enterprises
 - d. Extent to which potential information, associations, or other assistance could benefit a present or future investigation
 - e. Relationship with the target of an investigation
 - f. Motivation in providing information or assistance
 - g. Risk of adversely affecting an existing or future investigation
 - h. Extent to which provided information can be corroborated
 - i. Prior record as a witness
 - j. Criminal history, to include whether he or she is the subject of a pending investigation, is under arrest, or has been charged with a crime
 - k. Risk to the public or as a flight risk
 - l. Substance abuse concerns
 - m. Relationship to anyone in law enforcement
 - n. Risk of physical harm to the potential CI or their immediate family or relatives for cooperating with law enforcement
 - o. Any prior or current service as a CI with this or another law enforcement organization
2. Prior to an individual's use as a CI, a supervisor or other designated authority shall review the Initial Suitability Report and determine if the individual is authorized to serve as a CI.
3. Each CI's suitability shall be reviewed annually, at a minimum, during which time the CI's handler shall submit a Continuing Suitability Report addressing the foregoing issues in IV.A.1.a.–o (above), where applicable.
4. Any information that may negatively affect a CI's suitability during the course of their use shall be documented in the CI's file and forwarded to the appropriate authorized personnel as soon as possible.
5. Supervisors shall review informant files regularly with the handler and shall attend debriefings of CIs periodically as part of the informant management process.
6. CI contracts shall be terminated, and the CI file placed in inactive status when the CI has not been used for one year or more. Inactive CIs may be reactivated as needed.

B. Special CI Approval Requirements

Certain individuals who are being considered for use as a CI require special review and approval. In all instances, the agency's chief executive or their designee and the office of the prosecutor or state's attorney should be consulted prior to the use of these individuals as CIs. These individuals include the following:

1. Juveniles
 - a. Use of a juvenile under the age of 18 as a CI may be undertaken only with the written authorization of the individual's parent(s) or guardian(s).
 - b. Authorization for such use should be granted only when a compelling public interest can be demonstrated.
2. Individuals obligated by legal privilege of confidentiality
3. Government officials
4. Wards of the corrections authority
 - a. This category includes persons who are in the custody of local or state departments of corrections or under their supervision in the community through probation, parole, supervised release, or other programs. It may also include persons who are current or former participants of the federal witness security program.
 - b. Use of such individuals as CIs requires additional approval from the department of corrections.
5. Individuals engaged in criminal activity within the jurisdiction of other law enforcement agencies.

C. General Guidelines for Handling CIs

General guidelines for handling CIs are as follows:

1. CIs shall be treated as assets of the agency, not the individual handler.
2. CIs shall not be used without authorization of the agency through procedures identified in this policy.
3. CIs shall not be used to gather information purely of a political nature or for other information-gathering efforts that are not connected with a criminal investigation.
4. All CIs shall sign and abide by the provisions of the agency's CI agreement. The CI's handler shall discuss each of the provisions of the agreement with the CI, with particular emphasis on the following:
 - a. CIs are not law enforcement officers. They have no arrest powers, are not permitted to conduct searches and seizures, and may not carry a weapon while performing activities as a CI.
 - b. CIs found engaging in any illegal activity beyond what is authorized by the agency and conducted while under the supervision of a handler, will be subject to prosecution.
 - c. CIs are prohibited from engaging in actions or activities that could be deemed entrapment. The meaning of the term and implications of such actions shall be explained to each CI.
 - d. CIs are prohibited from engaging in self-initiated information or intelligence gathering without agency direction and approval.
 - e. Every reasonable effort will be taken to ensure the confidentiality of the CI but, upon judicial order, he or she may be required to testify in open court.
 - f. CIs may be directed to wear a listening and recording device.
 - g. CIs shall be required to submit to a search before and after a controlled purchase.

- h. CIs who participate in unplanned or unanticipated activities or meet with a subject(s) under investigation in a location outside of the jurisdictional boundary of the handling agency shall promptly report that activity or meeting to their handlers.
- 5. CI activity outside jurisdictional boundaries:
 - a. CIs shall not engage in intelligence gathering or meet with a subject(s) under investigation in locations outside of the jurisdictional boundaries of the handling agency, unless authority is granted by this agency's chief executive or their designee.
 - b. Investigators handling CIs who engage in operational activity in locations outside the jurisdictional boundaries of the agency shall coordinate with counterparts in law enforcement agencies that have jurisdiction in that location where the CI will operate *before* any activity occurs, or in a timely manner *after* unanticipated activity occurs and is brought to the attention of the handler.
 - c. Any decision to *defer or delay* notice to or coordinate with an outside agency having jurisdiction in the area where a CI has or may operate must be documented, reviewed, and approved by the agency's chief executive or their designee.
- 6. Officers shall take the utmost care to avoid conveying any confidential investigative information to a CI, such as the identity of other CIs, surveillance activities, or search warrants, other than what is necessary and appropriate for operational purposes.
- 7. No member of this agency shall knowingly maintain a social relationship with a CI, or otherwise become personally involved with a CI beyond actions required in the performance of duty. Members of this agency shall not solicit, accept gratuities from, or engage in any private business transaction with a CI.
- 8. Meetings with a CI shall be conducted in private with another officer present and shall be documented and subsequently entered into the individual's CI file.
- 9. Handlers shall develop and follow a communications strategy and plan with the CI that minimizes, to the greatest extent possible, the risk of discovery or compromise of the relationship between the agency and the CI. This plan should also aim to prevent the detection, compromise, or interception of communications between the handler and the CI.
- 10. Procedures shall be instituted to assist CIs with concealing their identity and maintaining their safety. Care should be given not to expose CIs to unnecessary safety risks.
- 11. Whenever possible, officers shall corroborate information provided by a CI and document efforts to do so.
- 12. The name of a CI shall not be included in an affidavit for a warrant unless judicial authority is obtained to seal the document from the public record or the CI is a subject of the investigation upon which the affidavit is based. Additionally, officers shall scrupulously avoid providing details of CI actions or involvement in arrest reports and other documents available to the public.
- 13. Handlers are responsible for ensuring that information of potential value to other elements of the agency is provided promptly to authorized supervisory personnel and/or other law enforcement agencies as appropriate.
- 14. Individuals leaving employment with the agency have a continuing obligation to maintain as confidential the identity of any CI and the information he or she provided unless obligated to reveal such identity or information by law or court order.

D. Establishment of an Informant File System

An informant file system shall be established as follows:

1. The agency chief executive shall designate a file supervisor who shall be responsible for developing and maintaining master CI files and an indexing system.
2. A file shall be maintained on each CI deemed suitable by the agency.
3. An additional file shall be established for CIs deemed unsuitable during initial suitability determinations or at a later time.
4. Each file shall be coded with an assigned informant control number for identification within the indexing system and shall include the following information:
 - a. Name, aliases, and date of birth
 - b. Height, weight, hair color, eye color, race, sex, scars, tattoos, or other distinguishing features
 - c. Name of the officer initiating use of the informant and any subsequent handlers
 - d. Photograph and criminal history record²
 - e. Current home address and telephone number(s)
 - f. Residential addresses in the last five years
 - g. Current employer, position, address, and telephone number
 - h. Social media accounts
 - i. Marital status and number of children
 - j. Vehicles owned and their registration numbers
 - k. Places frequented
 - l. Gang affiliations or other organizational affiliations
 - m. Briefs of information provided by the CI and the CI's subsequent reliability
 - n. Special skills and hobbies
 - o. Special areas of criminal expertise or knowledge
 - p. A copy of the signed informant agreement
5. CI files shall be maintained in a separate and secured area.
6. The file supervisor shall ensure that information concerning CIs is strictly controlled and distributed only to officers and other authorities who have a need and a right to such information.
7. CI File Review
 - a. Sworn personnel may review an individual's CI file only upon the approval of the agency's chief executive or their designee.
 - b. The requesting officer shall submit a written request explaining the need for review. A copy of this request, with the officer's name, shall be maintained in the individual's CI file.
 - c. Officers shall not remove, copy, or disseminate information from the CI file.
 - d. CI files shall be reviewed only in designated areas of the law enforcement facility and returned as soon as possible to their secure file location.

² Fingerprints may also be required if the CI's true identity is suspect.

8. All disclosures or access to CI files shall be recorded by the file supervisor, to include information such as the requesting officer or agency, the purpose of access or disclosure, the information conveyed, and the date and time of access or dissemination.
9. No portion of an individual's CI file shall be entered into any other electronic or related database without controls sufficient to exclude access to all but authorized personnel with a need and a right to know.

E. Monetary Payments³

Monetary payments shall be managed as follows:

1. All monetary compensation paid to CIs shall be commensurate with the value of the information or assistance provided to the agency.
2. All CI payments shall be approved in advance by the officer in charge of confidential funds.
3. Officers shall provide accounting of monies received and documentation for confidential funds expended. Any documentation of monies paid or received should not contain the true identity of the informant but should use the CI's control number.
4. Two officers shall be present when making payments or providing funds to CIs.
5. The appropriate individual, as designated by the agency's chief executive, shall ensure that the process for authorization, disbursement, and documentation of CI payments, as well as the accounting and reconciliation of confidential funds, is consistent with agency policy.
6. If a CI is authorized to work with another law enforcement or prosecutorial agency, financial payments shall be coordinated between the agencies in a manner that is proportionate to the assistance rendered to each agency and consistent with provision IV.E.1. of this policy.
7. Written records of receipts are retained, or justification for the exception is documented when a written receipt is not available.

³ See International Association of Chiefs of Police, National Law Enforcement Policy Center, *Model Policy on Confidential Fund* (Alexandria, VA), <https://www.theiacp.org/resources/policy-center-resource/confidential-fund>.

Every effort has been made by the IACP 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. 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. 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.

© Copyright 2020. Agencies are encouraged to use this document to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia, U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.

Considerations

Updated: December 2020

Confidential Informants

I. PURPOSE

This document is intended to provide agencies with items for consideration when developing their policies regarding confidential informants (CI). Agencies should develop procedures for the control and use of CIs to ensure they are used effectively and to prevent improper management or use. Additionally, the screening, selection, and management of CIs should adhere to all applicable laws and regulations.

Many CIs have a criminal history, have close associations with other criminally involved individuals, or have opportunities to access knowledge about criminal activities. While these relationships can be useful in yielding high rewards for a criminal investigation, CI handlers and their supervisors must maintain thorough records and adhere to departmental and legal regulations in order to best protect their CIs, themselves, and their department from any potentially legal or otherwise harmful consequences.

II. POLICY

Agencies should develop a policy statement to concisely explain to agency personnel and the public, the agency's policy on confidential informants.

Sample: It is the policy of this law enforcement agency to take necessary precautions when utilizing confidential informants by developing sound informant management procedures.

III. DEFINITIONS

Confidential Informant (CI): An individual, under the direct supervision of enforcement officer, who is provided with a reasonable expectation of confidentiality, and who furnishes information about suspected criminals or criminal activity for consideration, either financial, prosecutorial, or judicial; or a person who actively participates in a criminal investigation or intelligence operation under the direct supervision of a enforcement officer with or without compensation.¹

Confidential Informant File: File maintained to document all information that pertains to a CI.

CI Handler: The officer primarily responsible for supervision and management of a CI.

Unreliable Informant File: File containing information pertaining to an individual who has failed at following an established written CI agreement and has been determined to be generally unfit to serve as a CI.

¹ Agencies should consult local laws and regulations to determine to what degree confidentiality can be provided.

IV. PROCEDURES

A. General Procedures

Prior to implementing a CI program, agencies should develop guidelines regarding:

1. Confidentiality according to applicable laws and regulations, including legal limitations to which protections can be offered.
2. When individuals should be classified as confidential and provided with a reasonable expectation of confidentiality, including establishing validation and verification requirements. Confidential informants should be provided with a reasonable expectation of confidentiality.²

B. Initial Suitability Determination

Agencies should consider developing policies and procedures for determining individuals who are suitable CIs. Considerations may include:

1. Requiring officers requesting the use of a CI to complete an initial suitability report, which should include information regarding the individual's:
 - a. Age, sex, and residence;
 - b. Employment status or occupation;
 - c. Affiliation with legitimate businesses and illegal or suspicious enterprises;
 - d. Affiliation with groups whose activities may impact law enforcement functions, such as street-level criminal organizations, terrorist organizations, or known extremist groups;³
 - e. Relationship with the target of an investigation;
 - f. Motivation in providing information or assistance;
 - g. Risk of adversely affecting an existing or future investigation;
 - h. Veracity, including the extent to which provided information can be corroborated;
 - i. Prior record as a witness;
 - j. Criminal history, to include whether they are the subject of a pending investigation, are under arrest, or have been charged with a crime;
 - k. Risk to the public or as a flight risk;
 - l. Substance abuse concerns;
 - m. Relationship to anyone in law enforcement;
 - n. Risk of physical harm to the potential CI or their immediate family or relatives for cooperating with law enforcement;
 - o. Prior or current service as a CI with this or another law enforcement organization, if any;
 - p. Degree of helpfulness, such as the extent to which potential information, associations, or other assistance could benefit a present or future investigation.
2. Confirming that potential CIs are accurate and reliable prior to granting the protection of confidentiality.
3. Determining who has the authority to approve the initial suitability report and authorize the individual to serve as a CI.

² In contrast, sources of information and cooperating defendants should not be provided with confidentiality, absent exigent circumstances.

³ In some areas, this may include intelligence held by law enforcement agencies relating to the potential CI.

4. Reviewing and documenting any information that may negatively affect a CI's suitability during the course of their use and forwarding this information to designated agency personnel as soon as possible.
5. Ensuring supervisory oversight of the program, to include reviewing the CI files with the handler and periodically attending debriefings of CIs.
6. Terminating CI contracts and placing their files in inactive status when CIs have not been used in a year or more. Inactive CIs may be reactivated as needed.
7. Developing procedures for CIs who require special review and approval, such as consulting the agency's chief executive or their designee and the office of the prosecutor or an attorney.⁴ Individuals who may require special review include:
 - a. Juveniles:
 - i. Use of a juvenile⁵ as a CI may be undertaken only with the written authorization of the individual's parent(s) or guardian(s), and
 - ii. Authorization for such use should be granted only when a compelling public interest can be demonstrated.
 - b. Individuals obligated by legal or professional ethics' privilege of confidentiality, such as a medical doctor in relation to a patient, a priest in relation to a parishioner, or a lawyer in relation to a client;
 - c. Government officials, where there may be a conflict of interest with the post they hold;
 - d. Wards of the corrections authority;
 - i. Including persons who are in the custody of the departments of corrections or under their supervision in the community through probation, parole, supervised release, or other programs. It may also include persons who are current or former participants of a witness security program.
 - ii. Use of such individuals as CIs requires additional approval from the department of corrections.

C. Handling CIs

Agencies should provide guidance for the proper supervision, handling, and management of CIs. Guidance should include:

1. Treating CIs as assets of the agency rather than the individual handler.
2. Requiring agency authorization prior to use of CIs.
3. Ensuring CIs are not used to gather information for political gains.
4. Developing guidance for handling CI activity outside of jurisdictional boundaries,⁶ including ensuring the following:
 - CIs are not permitted to engage in intelligence gathering or meet with a subject(s) under investigation in locations outside of the jurisdictional boundaries of the handling agency, unless

⁴ Individuals who may not be used as CIs may, in some cases, serve as sources of information.

⁵ The definition of a juvenile can vary. However, in the United States, an individual under the age of 18 is designated as a minor.

⁶ When developing procedures for handling CI operations outside jurisdictional boundaries, agencies should consult laws and regulations as well as any interagency agreements. Where feasible, agencies should attempt to coordinate with surrounding agencies prior to implementing such procedures.

- authority is granted by the handling agency's chief executive or their designee, and, where appropriate, authorization from the outside agency's chief executive or designee.
- CIs who participate in unplanned or unanticipated activities or meet with a subject(s) under investigation in a location outside of the jurisdictional boundary of the handling agency are instructed to promptly report that activity or meeting to their handlers. Where appropriate, the outside agency should be informed of any such activities.
 - Investigators handling CIs who engage in operational activities outside the jurisdictional boundaries of the agency receive guidance to coordinate with counterparts in law enforcement agencies that have jurisdiction in the location where the CI will operate before any activity occurs, or in a timely manner after unanticipated activity occurs and is brought to the attention of the handler.
 - Any decision to defer or delay notice to or coordinate with an outside agency having jurisdiction in the area where a CI has or may operate must be documented, reviewed, and approved by the handling agency's chief executive or their designee, as well as the outside agency's chief executive or designee, where appropriate.
5. Requiring all CIs to sign and abide by the provisions of the agency's CI agreement. The handler should ensure the CI is aware of not only the provisions of the agreement but also the legality of it, especially those provisions that indicate CIs:
- Are not law enforcement officers, have no arrest powers, are not permitted to conduct searches and seizures, and may not carry an agency-issued weapon while performing activities as a CI.
 - Found engaging in any illegal activity beyond what is authorized by the agency and conducted while under the supervision of a handler, may be subject to prosecution.
 - Are prohibited from engaging in actions or activities that could be deemed entrapment, and that the CI understands the meaning of the term and implications of such actions.
 - Should notify the agency handler in a timely manner when engaging in self-initiated information or intelligence gathering.
 - May be required to testify in open court upon judicial order, though every reasonable effort will be taken to ensure the anonymity or confidentiality of the CI.⁷
 - May be directed to wear a listening and recording device.
 - May be required to submit to a search before and after a controlled purchase, controlled delivery, or a meeting.
6. Ensuring officers take the utmost care to avoid conveying any confidential investigative information to a CI, such as the identity of other CIs, surveillance activities, or search warrants, other than what is necessary and appropriate for operational purposes.
7. Prohibiting agency personnel from maintaining any type of inappropriate relationship with a CI, or otherwise becoming personally involved with a CI beyond actions required in the performance of duty, including but not limited to sexual relationships, soliciting, accepting gratuities from, and engaging in any private business transaction or relationship with a CI.
8. Ensuring all handler meetings with CIs are conducted with another officer present and documenting meetings for the CI's file.

⁷ Confidentiality and anonymity should be defined according to laws within an agency's jurisdiction, including legal limitations to which protections can be offered.

9. Developing agency communication procedures for handlers working with CIs. These communication methods should aim to protect the safety and anonymity/confidentiality of CIs, as well as prevent the detection, compromise, or interception of communications between handlers and CIs. Consider methods such as Criminal Justice Information Services (CJIS) compliant software to help protect the safety of the CI.⁸
10. Corroborating information provided by a CI whenever possible, and documenting efforts to do so.
11. Maintaining the confidentiality/anonymity of the CI's identity insofar as reasonably and legally possible.
12. Developing procedures to assist handlers in determining what information should be shared with other law enforcement personnel, such as criminal intelligence, which may be pertinent to another investigation. Agencies should equip handlers with guidelines to help them decide what should be shared, considering both the risk that information-sharing may pose to the handler's CI or investigation and the value of the information or intelligence to other law enforcement.
13. Consulting local laws and regulations to determine if any ongoing confidentiality requirements for individuals leaving agency employment are in place.⁹ Agencies in jurisdictions wherein former employees are required to maintain confidentiality obligations should communicate this information to departing employees.

D. Establishing an Informant File System

When establishing a file system to maintain and track CI files, agencies should provide guidance to personnel, such as:

1. Designating personnel responsible for developing and maintaining the master CI files and indexing system.
2. Maintaining a file on each CI deemed suitable by the agency and an additional file for each CI deemed unsuitable.
3. Developing a system for identifying files, such as coding each file with an assigned informant control number for identification within the indexing system, including the following information:
 - Name, aliases, and date of birth;
 - Height, weight, hair color, eye color, race, sex, scars, tattoos, or other distinguishing features;
 - Name of officer initiating use of the informant and any subsequent handlers;
 - Photograph and criminal history record. Fingerprints may also be required if the CI's true identity is suspect. However, fingerprints may be excluded if already recorded by this or another law enforcement agency;
 - Current home address and telephone number(s);
 - Residential addresses in the last five years;
 - Current employer, position, address, and telephone number;
 - Social media accounts;
 - Marital status and number of children;

⁸ When developing communication methods for handlers and CIs, agencies should be aware that electronic communications with CIs, such as emails or text messages, may be subject to public records requests or discovery. Agencies should seek legal counsel to determine whether this is the case in their jurisdiction, as well as whether there are exemptions for communications with CIs.

⁹ In some jurisdictions, former employees with knowledge of confidential information may be liable to prosecution for failing to maintain confidentiality, absent legal exceptions.

- Vehicles owned and their registration numbers;
 - Places frequented;
 - Gang affiliations or other organizational affiliations;
 - Briefs of information provided by the CI and the CI's subsequent reliability;
 - Special skills, hobbies, or significant interests;
 - Special areas of criminal expertise or knowledge;
 - A copy of the signed informant agreement.
4. Maintaining CI files in a separate and secure area.
 5. Designating personnel responsible for ensuring that information concerning CIs is strictly controlled and distributed only to officers and other authorities who have a need and a right to such information.
 6. Developing procedures for the review of CI files, such as direction to:
 - Seek appropriate approval before reviewing a CI file;
 - Submitting a written request explaining the need for review and including a copy of the request and the requestor's name in the CI file;
 - Refrain from removing, copying, or disseminating information from the file;
 - Treat and handle files as confidential and return them as soon as possible to their secure location;
 - Review CI information that may be subject to change and update CI files as necessary.
 7. Designating personnel to record all disclosures or access to CI files, to include information such as the requesting officer or agency, the purpose of access or disclosure, the information conveyed, and the date and time of access or dissemination.
 8. Ensuring that files containing CI-identifying information are not entered or shared in other agency databases unless access is restricted only to authorized personnel. Confidentiality of CI information is paramount.
 9. Maintaining CI-provided intelligence records separately from CI-identifying information and developing procedures for sharing intelligence with special care to avoid identifying CIs. The CI's identity and the information they provide should *always* be kept separately.

E. Monetary Payments

Guidance for monetary payments should be clearly articulated to agency personnel. Policies and procedures may include ensuring the following:

1. All monetary compensation paid to CIs is commensurate with the value of the information or assistance provided to the agency.
2. Financial payments for CIs authorized to work with another law enforcement or prosecutorial agencies are coordinated between the agencies in a manner that is proportionate to the assistance rendered to each agency.
3. All CI payments are approved in advance by the appropriate personnel.
4. Appropriate personnel provide accounting of all monies received and documentation for confidential funds expended.
5. At least two officers are present when making payments or providing funds to CIs.
6. Personnel are designated to manage the process for authorization, disbursement, and documentation of CI payments, as well as the accounting and reconciliation of confidential funds.

7. Written records of receipts are retained, or justification for the exception is documented when a written receipt is not available.

F. Training

Developing a standardized training curriculum for CI handlers is important. Providing proper training and oversight to CIs and CI handlers is critical to the success of a CI program. In developing training curriculum, agencies should consider:

1. Developing criteria to determine which officers are suited to becoming a CI handler and how CI handlers will be selected. These considerations may include:
 - Rank
 - Years and type of experience
 - Nature of current role, i.e., patrol, detective, etc.
 - Personality traits
 - Willingness and motivation
 - Agency commendations
 - Disciplinary record
2. Determining whether CIs should be formally or informally trained and/or oriented to what the agency is requesting of them.
3. Assessing what level and types of training are relevant to CI handlers.
4. Developing procedures for ongoing training and support of CI handlers, particularly those who are using CIs for the first time.
5. Assessing whether agency procedures should be developed on how to profile, identify, approach, and recruit CIs.
6. Training and teaching CIs on their role and expectations. This may include:
 - Differentiating between CIs (individuals relaying information) and agents (individuals performing an action).
 - Examining the legalities of certain CI actions. For example, agent provocateurs can be compelled to testify in court. It is important for your department to consult its national and state laws to provide a comprehensive review.
7. Tracking detailed training records for both CI handlers and CIs.

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 no model policy can meet all the needs of any given law enforcement agency. 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. 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.

© Copyright 2020. Agencies are encouraged to use this document to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia, U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.

Concepts & Issues

Updated: October 2020

Confidential Informants

I. INTRODUCTION

A. Purpose of Document

This paper was designed to accompany the Model Policy and Considerations document on Confidential Informants established by the IACP 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 and Considerations document. This material will be of value to law enforcement executives in their efforts to tailor the model to the requirements and circumstances of their communities and their law enforcement agencies.

B. Background

A Confidential Informant (CI)¹ is defined as an individual requiring anonymity who provides useful information, directed assistance, or both, that enhances criminal investigations and furthers the mission of the agency, usually in exchange for financial or other consideration. Individuals who serve as witnesses or citizens who provide information regarding criminal activity are generally not considered CIs. This distinction is based in part on the fact that CI arrangements involve the development of a relationship between the individual and the agency that focuses on the trading of information for some form of payment, to include prosecutorial consideration.

Although CIs can provide investigators with specific information that is not available from other sources, it must be remembered that CIs often have a criminal history, have close associations with other criminally involved individuals, or have opportunities to access knowledge about criminal activities. Agencies must keep in mind that CIs can render a significant negative impact on a law enforcement investigation, harm an agency's credibility, and endanger officers' lives if not properly managed.

To be of value as a CI, an individual must have one or more of the following characteristics:

- Knows, has been associated with, or has intimate knowledge of one or more active criminals.
- Has an occupation or residence that lends itself to gathering information about criminals and their plans to commit crimes.

¹ The term "confidential informants" may have a negative connotation. Therefore, some agencies may elect to use another term such as "cooperating individuals."

- Has status in the criminal justice system. This includes, but is not limited to, individuals who are on pretrial release or bail, probation or parole, convicted pending sentencing, or incarcerated. Oftentimes, such criminal history also affords the individual a level of social status or respect among their criminally involved peer groups. In many instances, this provides the CI with requisite “credentials” that show he or she can be trusted by individuals engaged in criminal activity.

In addition, the CI should meet three criteria before performing work for the law enforcement agency. The CI must:

- Be willing to work under the direction of an officer and to perform certain acts as directed. In these situations, the officer assigned primary responsibility for the CI is generally referred to as the CI’s “handler.”
- Be willing to exchange information for monetary or other lawful consideration.
- Not be an employee of a law enforcement agency.

II. CONCERNS

A. Potential Hazards Associated with CIs

Successfully directing and monitoring CIs requires that officers treat them courteously, offer encouragement and praise, make it clear that the agency has high expectations, and develop a trust-based relationship. However, officers must maintain an acute awareness of potential problems such as those described as follows:

- **Lying** – CIs may exaggerate or fabricate the criminal acts of targets. Some may report truthfully but lie about the fact that they used illegal methods to obtain the information.
- **Duplicity** – CIs can make deals with targets as easily as they can with law enforcement, using both sides to their advantage. They might not be faithful to either side yet remain trusted by both. CIs might provide criminal associates with information about the identity of undercover agents, including what cars they drive, hours they work, their tactics, and agency procedures. Finally, CIs might sell the same information to two different agencies, causing the agencies to unwittingly conduct simultaneous investigations.
- **Fraud** – CIs can find themselves in a position to leverage information for their own benefit. For example, they might sell government property used in investigations or pledge it as collateral for loans.
- **Blackmail** – Officers who become too involved or engaged in an inappropriate relationship with CIs might begin to sympathize with their problems and knowingly fail to adhere to agency policy. Eventually, the CI might obtain incriminating information concerning the officer that can then be used for the benefit of the CI.
- **Other Inappropriate Relationships** – Engaging in an inappropriate relationship with a CI can lead to other compromising situations for officers, especially as CIs and handlers spend extended lengths of time working together. Seemingly innocuous yet unprofessional situations may occur in varying increments. Whether the relationship is of a sexual, emotional, and/or financial basis, any relationship other than a professional one can compromise a handler’s authority and ability to manage their CI. Inappropriate relationships may lead to severe consequences to an investigation, and legal and/or employment consequences for officers.

B. What Motivates CIs?

Understanding what motivates the CI can be the key to retaining control over their activities. As a result, before enlisting the services of a CI, the handler must determine not only who the individual is, but also why they want to become a CI. It is important that the handler accepts the CI’s motivations and either works within that context or

chooses not to contract with the individual. Finally, these perceived motives must be monitored over time. A change of motivation may alert investigators to potential problems in the way the CI is operating or may signal the CI's desire to end the relationship with the agency.

Among the most significant motivators are money; revenge, spite, or retaliation based on perceived mistreatment by others; elimination of competition through diversion of suspicion; fear, to include the fear of current or former associates; self-aggrandizement and a desire to enhance sense of self-importance; prosecutorial or judicial leniency; and repentance or a desire to make amends for past wrongdoing.

C. CI Screening

Law enforcement agencies can reduce the risk of selecting unsuitable CIs by developing sound CI screening and management procedures. Before an officer may use a CI, the officer should complete an initial suitability report pertaining to the potential CI and submit it to the appropriate authority in the agency for review and approval. This report provides a relatively thorough review of the potential CI's risks and benefits to the agency. Continued supervision and evaluation are also necessary to prevent or mitigate inappropriate selection.

The potential CI's initial suitability report should be completed and approved by the appropriate agency authority before the individual is used as a CI. The objective of the initial suitability report is twofold: (1) it develops essential preliminary information on a potential CI to create a profile for the master file; and (2) it documents answers to certain basic questions that will provide a sufficient basis to intelligently judge an individual's utility and suitability as a CI. Determination of suitability can be achieved only if reporting officers are diligent in providing sufficient information and making informed judgments about the risks and benefits associated with each individual.

When completing an initial suitability report, potential items that should be considered include the individual's relationship with the target; the potential for gaining useful information; probable motivation of the individual; the individual's prior criminal history; and whether the individual or their family or relatives would be at risk if the individual were to serve as a CI. In addition, the report should document the following information, where applicable, the individual's:

- Age, sex, and residence;
- Employment status or occupation;
- Affiliation with legitimate businesses and illegal or suspicious enterprises;
- Extent to which potential information, associations, or other assistance could benefit a present or future investigation;
- Risk of adversely affecting an existing or future investigation;
- Extent to which provided information can be corroborated;
- Prior record as a witness;
- Criminal history, to include whether he or she is the subject of a pending investigation, is under arrest, or has been charged with a crime;
- Risk to the public or as a flight risk;
- Substance abuse concerns;
- Relationship to anyone in law enforcement;
- Any prior or current service as a CI with this or another law enforcement organization.

To be of value, initial suitability reports must detail the specific benefits of using a potential CI, as well as identified risk factors. Written comprehensive suitability assessments are not only valuable for screening and management by the initial handler but can also be of value to other officers who may want to use the CI. The initial suitability reports are also essential to determine the nature and scope of monitoring required for a particular CI.

Each CI's suitability should be reviewed annually, at a minimum, and all handler-CI contacts should be documented and included in the CI file. The use of continuing suitability reports and documentation of CI contacts help determine whether the risk of using a CI has changed since the initial evaluation. Moreover, any information that would negatively affect a CI's suitability during the course of his or her use should be forwarded to the appropriate authorized personnel. Regular review of CI files by supervisory officers and their periodic participation at CI debriefings are valuable checks on the worth of CIs and the manner in which they are being managed by their handlers.

D. Special CI Categories

There are several categories of CIs that require special evaluation and approval. In each of these cases, the agency's chief executive officer or their designee and the office of the prosecutor or state's attorney should be consulted prior to the use of these individuals as CIs.

Juveniles – Juveniles require a great deal of deliberation prior to their use. Juveniles may be less steadfast in motivation, less able to avoid detection, and less able to withstand pressure once suspected by the individuals upon whom they have been tasked to inform. As a result, juvenile CIs run a higher risk of being exposed, potentially placing them in physical danger. This danger is directly proportional to the seriousness of the criminal activity and the relative youth of the CI. For example, a streetwise 17-year-old recruited to inform about unlawful tobacco use in a high school is probably going to be in less physical danger than a 12-year-old student sent to inform upon drug dealers. However, even an apparently minor case may involve considerable physical risk to a juvenile CI.

Perhaps the best-known case involving a juvenile CI is that of 17-year-old Chad MacDonald. In 1998, police in California arrested MacDonald on drug charges. He agreed to act as a CI, wearing a recording device during at least one drug buy and providing police with information about local drug trafficking. A short time later, he was found dead in an alley, apparently tortured and strangled, and his girlfriend was found raped and shot to death in a canyon. MacDonald's death was believed to have been the result of his association with law enforcement as a CI, and the family brought a civil action against the jurisdictions involved. The incident resulted in the passage of "Chad's Law," a California state law that prohibits the use of individuals 12 years old or younger as CIs. It also prohibits the use of individuals under the age of 18 unless a court order is obtained, with the exception of their use in enforcement of statutes prohibiting the purchase of alcohol or tobacco by juveniles.

Considering the significance of these issues, officers have a responsibility to make sound judgments when considering the use of juvenile CIs. In some cases, the parent or guardian may authorize the juvenile's use as a CI without fully understanding the risks inherent in CI operations. When this happens, the parent or guardian's authorization to use the child as a CI cannot be relied upon by law enforcement as the basis for informed consent. As a result, parental permission—even when required by policy, practice, or law—does not always provide law enforcement officers with sufficient justification and should not be used as the sole condition for using juveniles as CIs.

Some law enforcement agencies have chosen to ban the use of juveniles as CIs entirely, while others subject such decisions to more rigid command scrutiny. Therefore, it is suggested that, unless an officer is guided by state or federal law or agency policy, they must be able to clearly define a compelling public interest that will be served before a juvenile may even be considered for such a role. Compelling public interest, for the purposes of this discussion, includes situations where the failure to use a juvenile CI would result or likely result in loss of life; serious injury; or some serious negative consequence for persons, property, or public safety and therefore demands action. Furthermore, that justification should be reviewed; approval must be obtained by the agency's chief executive or their designee; and written authorization must be obtained from the juvenile's parents or guardians.

Individuals Obligated by Legal Privilege of Confidentiality – The most common examples of individuals in these occupational classes are members of the clergy, attorneys, and medical doctors. However, state laws vary on the classes of occupations afforded privileges of confidentiality. Such privileges may extend in various ways to licensed

mental health counselors, clinical social workers, and alcohol and drug abuse counselors, among others. In these and other realms, obligations and limits may be ill-defined. This is particularly the case in regard to various types of pastoral counselors and school guidance counselors. Additionally, there are a number of federal and state regulations that require physicians, clinicians, and others who are normally afforded confidentiality to report certain acts (for example, child abuse) or grant them the discretion to report certain conditions (for example, reporting a positive HIV test result to a parent or legal guardian). Federal regulations and state laws also govern confidentiality of medical information and mandate disclosure and reporting under certain circumstances. As a result, a decision to accept or solicit information from sources such as these can be a complicated legal matter.

Government Officials – This category includes individuals in high-level and sensitive local, state, and federal governmental positions who have access to privileged information. Individuals in these types of positions may come forward with information rather than being recruited as CIs and are generally referred to as “whistleblowers.” Law enforcement dealings with these individuals require a great deal of caution and inquiry into the person’s background and potential motives, as the person may harbor a grievance against one or more individuals within the government or the governmental entity as a whole. Law enforcement agencies and their employees must also be wary of whistleblowers who may simply be using law enforcement authority to further political motivations and agendas.

Individuals in these positions may reach out to law enforcement authorities because of a real or imagined inability to address internal problems at their agency and view law enforcement as the only alternative. However, the issues in question might not rise to the level of criminal offenses. In many cases—such as those involving patronage, cronyism, influence trading, or conflicts of interest—they are ethical matters or allegations concerning breaches of administrative or civil law. In other cases—such as those involving bribery, graft, embezzlement, and kickbacks—the criminal offense involved may fall within the purview of state or federal regulatory authorities or the Federal Bureau of Investigation. As a result, allegations brought forward by governmental employees should be referred to the local prosecutor and subsequently to the state’s attorney general through the chief law enforcement executive or his or her designee.

Wards of the Corrections Authority – This category includes individuals who are in the custody of local or state departments of corrections or under correctional supervision in the community through probation, parole, supervised release, or other programs. It may also include individuals who are current or former participants in the federal witness security program.

Individuals who are serving sentences have been used in many cases to gather information on targeted subjects in local jails and correctional institutions. While their credibility is often questioned in court proceedings, they can, and often do, provide information that can benefit investigations whether or not their testimony is required in open court. The motives of these individuals must always be considered, as they invariably offer to serve as CIs in return for reduced sentences or similar rewards. As such, their use is dependent on approval from the correctional authority.

E. Final Determination on CI Use

When all the available information on a potential CI has been assembled, a determination must be made concerning the risks and benefits of utilizing the CI during specific investigative operations. The following are items that should be considered when making this decision.

- **The criminal enterprise to be targeted.** Consider the following:
 - *How serious are the crimes involved?*
 - *Are the crimes or those participating in them violent or likely to become violent?* Certain types of crimes and perpetrators pose a greater threat to a CI than others.
 - *How urgent is the specific case?* Is the particular criminal enterprise against which action is being considered one that must be terminated immediately, such as a proposed imminent terrorist attack? Or is

it one that can be allowed to continue for a time in order to develop further leads without endangering the safety of the community, such as a petty theft ring?

- *Is the enterprise of such a nature that it may be combatted by means other than the use of CIs?* Some types of criminal activity can be addressed only through information obtained from the inside, but other situations may lend themselves to the use of other methods, such as external electronic surveillance. Thus, the degree of necessity for the use of CIs should be a major consideration in the decision as to whether or not they should be used.

- **The risk to the CI.** Consider the following:

- *What is the extent, imminence, and severity of the risk to the CI if their undercover role is discovered?* Would discovery result in serious injury or death? For example, would discovery merely cause the CI to be excluded from further participation in the activity? Or would the CI be subject to physical abuse, including possible torture and murder?
- *What is the CI being asked to do?* For example, is the CI being asked to observe passively and report, or to take an active role, such as wearing a recording device or transmitter? The more active the role, the greater the threat of discovery and related consequences.
- *What safeguards are in place to prevent the CI's role from being discovered?* Is knowledge of the operation and of the CI's identity properly restricted in the agency to those with a need and a right to know? If there are written records of the CI's identity, are they properly restricted from unnecessary access or circulation? Are statements to the media worded in such a way that the CI's role is not apparent?
- *Have secure methods of communication with the CI been established?* One cause of discovery by criminals is observation of contact between a CI and law enforcement.
- *If the CI is to remain embedded in the criminal enterprise after providing information, is the information that was provided being protected from revelation to unnecessary individuals?* Further, if action is taken based upon that information, is there a plausible alternative basis for that action that will conceal from the criminals the fact that a CI has been utilized?
- *Will law enforcement be able to extract the CI from danger in the event of discovery?* Does law enforcement have the capability to determine that the CI is suspected or discovered? If so, what plans are in place to extract the CI before being harmed?

- **The nature of the CI.** Consider the following:

- *How reliable is the CI (in terms of information provided)?* Do they consistently provide accurate and relevant information or have unusual access to an important target?
- *How dependable is the CI (in terms of manageability)?* Can the CI be managed by the officer safely? For example, a CI would be undependable in this way if they endanger an officer, engage in criminal activity, or otherwise violate protocol. However, they could deliver consistently accurate information or have a unique way of gaining access to the proposed target. Thus, in certain exceptional situations, it may be productive to use a CI who has been deemed undependable, although this poses greater risk to the officer and/or the agency. The decision to use an undependable CI should be made only by the chief executive or his or her designee after determining that the potential outcome is worth the extraordinary risks involved.
- *How old is the CI?* The younger the CI, the greater their vulnerability, the greater the risk of failure, and, the greater the culpability of law enforcement if the CI comes to harm.
- *Regardless of age, is the CI mature and intelligent enough to understand and consent to the risks involved?* Prior to their selection, the agency should ensure that the CI has a full understanding of the

dangers associated with their assignment. Individuals with intellectual or developmental disabilities or with diminished mental capacity generally should not be used as CIs.

- *In the case of juvenile CIs, are parents or guardians aware of the proposed activity, and do they consent to it?* Some parents will not consent, and such a refusal may require termination of any consideration of the use of that juvenile. Law enforcement should note that, even when parents have consented, if the juvenile CI is harmed, the parents may later claim that they did not understand the full implications of the consent.
- *What is the CI's level of experience and ability—is the CI sufficiently acquainted with the criminal enterprise and those engaging in it to handle contingencies that may arise while cooperating with law enforcement?* For example, will the CI be able to conceal their actual status from criminal associates? Will they be quick-witted enough to deflect suspicion if it arises?
- *Is the CI offering services to law enforcement voluntarily, or are they under some form of compulsion?* As noted earlier, some individuals volunteer information and even offer to act as CIs on a continuing basis. Others act as CIs in the hope of avoiding prosecution or reducing punishment. Law enforcement must judge not only the type but also the level of motivation of the CI.
- *How vulnerable is the CI?* For example, interaction with drug dealers and drug users may pose a threat to the informant who suffers from substance misuse and addiction. A period of detoxification may be necessary before the CI begins work, but working in a drug market after detox may put the informant at greater risk of relapse or overdose. Consider the situation holistically and evaluate any unique circumstances a particular CI may face.

F. Managing of CIs

It is incumbent on law enforcement agencies to institute the necessary controls, protect and support its CI handlers, and understand the legal limitations involved in using CIs. Even these generally accepted rules can be problematic in terms of implementation. The following are several issues related to the management of CIs that must be considered.

Development of Agency Policies and Procedures – After an agency decides to use CIs, the first item to address is the issuance of written directives that set forth policies and procedures. Next, the agency must define the roles and responsibilities of all individuals in the chain of command, from the chief executive to the handler. For instance, the chief executive or their designee should select an individual to have responsibility over the following:

- Development and maintenance of master CI files;
- Creation of an indexing system;
- Access to CI files, to include the approval of requests from sworn personnel to review an individual's CI file.

Training – Law enforcement personnel who will be interacting with CIs should be provided orientation and training in the appropriate techniques for working with CIs. Training should include a thorough briefing on agency policies, procedures, and required documentation, as well as explicit instructions on recruiting CIs; directing and monitoring CI activities; interviewing and debriefing CIs; preparing CIs for court; evaluating CI performance; and other relevant topics.

Similarly, CIs should also receive orientation and training that outlines what is expected of them, including an explicit list of acceptable and unacceptable behaviors. Training for CIs should address the CI's specific objectives, compensation procedures, communication with and reports to the handler, cover stories, security, legal constraints, and other topics.

Written Agreements – Agencies should ensure that every CI signs a document drafted by the agency, in consultation with legal counsel.² The handler should thoroughly review each provision of the agreement with the CI, placing particular emphasis on the following points:

- CIs have no law enforcement powers and are not permitted to carry weapons while performing activities as CIs.
- CIs will be arrested if found engaging in any illegal activity beyond what is authorized by the agency and conducted while under the supervision of a handler and will receive no special legal considerations.
- CIs shall not take, and the agency will not condone, any actions that may be considered entrapment.

The first point – that CIs are not law enforcement employees – should be reinforced by several specific items in the CI agreement. For example, the agreement should affirm the CI's status as independent from the agency and should acknowledge that, as such, they are not entitled to workers' or unemployment compensation. The agreement should also prohibit the CI from using the agency as an employment or credit reference without prior approval.

Regarding the third point, entrapment is a frequently cited defense in drug cases. Entrapment occurs when the government plans the offense and induces someone to commit it—someone who would not have otherwise done so except for the government's persuasion, fraud, or trickery. If a CI entraps or appears to entrap a defendant, the court may throw out all or part of the case. Furthermore, to prove that entrapment did not occur, the CI may have to testify, thereby revealing their identity. In addition, certain illegal actions on the part of a CI might raise the defense of "outrageous conduct," which is related to entrapment. The defense may assert that the government's conduct was so outrageous or shocking to fundamental fairness that due process would bar a conviction.

Criminal Involvement by the CI – It is often very difficult for law enforcement to completely prohibit all levels of criminal involvement by CIs, particularly in drug investigations. The willingness of law enforcement and prosecutors to allow certain forms or levels of criminality in order to gain criminal intelligence from CIs or use them in controlled buys or other roles is an issue that has been widely debated. Each agency must address this directly in its policy if they are to employ CIs in drug or other investigations. However, it should be made clear that CIs are prohibited from committing crimes beyond those that are authorized by the law enforcement agency and while under the supervision of a handler. The CI will receive no special consideration regarding crimes outside of this limited exception.

Who Controls the CI? – CIs should be viewed as assets of the law enforcement agency, not the individual handler. As such, the agency must ultimately control the use of CIs. This includes documenting the CI's identity, reviewing contacts between the CI and their handler, assessing the CI's reliability and usefulness, ensuring that confidential funds are used appropriately and accounted for properly,³ and ensuring that important CI information is available to all personnel who have a need and right to know.

Limitations on Targets of CI Investigations – CIs should not be used to gather information purely of a political nature or on individuals without a reasonable basis to believe that the person is involved in criminal activity.

Defining and Maintaining Proper CI-Handler Roles – The cooperative relationship between law enforcement and CIs can, at times, blur the line of authority between handlers and CIs who are working toward a common objective or in a shared mission. Increased informality can breed casualness and a relaxation of the formal boundaries that must exist between the handler and the CI.

As such, handlers should not establish social relationships or become personally involved with a CI beyond that which is required in the performance of duty. Handlers should also not reveal confidential or sensitive information

² See Appendix A for a sample agreement.

³ See International Association of Chiefs of Police, National Law Enforcement Policy Center, Model Policy and Concepts & Issues Paper on Confidential Fund, Alexandria, VA. Available at <https://www.theiacp.org/resources/policy-center-resource/confidential-fund>.

about law enforcement operations, plans, or activities unless it is absolutely necessary for the operational purposes of the CI.

Meetings with CIs – Whenever possible, the handler shall be accompanied by another officer when meeting with a CI. Some may disagree with this recommendation. Those who favor a one-officer approach cite these advantages: CIs who are particularly sensitive about confidentiality may be more likely to cooperate; the potential for personality conflicts is reduced; and more information or cooperation may be forthcoming. While exceptions may be necessary, the more significant advantages of the two-officer approach include maintenance of a more objective relationship with the CI, a greater chance of avoiding setups, a more accurate assessment of the CI's performance, and defense of any allegations of improper behavior.

Two-officer meetings are essential when there is the potential for an inappropriate relationship between a CI and handler, when the CI is a juvenile, and when the CI presents other exceptional risks. The latter may include situations where the CI is suspected of trying to set up the handler; is emotionally unstable; is a substance abuser; is on probation or parole; or has a reputation for perjury, bribery, or related offenses. In all instances where the potential for an inappropriate sexual or romantic relationship between a CI and the handler exists, meetings with at least two officers is highly recommended. While many situational factors should be considered, it is recommended that at least one of the officers be the same gender as the CI. This will help protect officers in claims of sexual improprieties against the handler from the CI.

If the CI must meet with their handler alone, a second officer may monitor the meeting through remote surveillance methods to achieve the same benefits as a two-officer meeting. Agencies that permit an officer to meet with a CI alone should require a contact report immediately following each meeting.

CIs Operating Outside the Jurisdiction of the Agency – On occasion, it may be necessary for a CI to gather intelligence or meet with subjects of an investigation in settings outside of the jurisdiction of the handling agency. Whether the CI is operating in a neighboring agency's jurisdiction, in a different state, or even in a foreign country, the handler should take care to ensure that the actions, safety, and identity of the CI can be protected; information gathered can later be admitted in court; and the CI, as well as the handler, will not face adverse consequences for actions that may be appropriate in one jurisdiction, but questionable—or, worse, illegal—in the jurisdiction where the CI is operating. Therefore, CIs should obtain permission to conduct these activities in advance.

In most instances, the handler should consult and coordinate with appropriate counterparts in agencies that have jurisdiction in the area where the CI will operate before the CI travels to or takes any action in that outside area. Coordinating activities ahead of time can provide a measure of safety for the CI, will help ensure that planned tactics and actions are legal in that jurisdiction, and should allow for the development of action plans and contingencies. In situations where the handler is not aware of the CI's activities outside the jurisdiction, the appropriate agency should be notified as soon as possible after the activity occurs.

In rare instances, a compelling reason may exist for not contacting counterparts that have jurisdiction in the area where the CI will operate. In such cases, senior leadership in the handling agency should be advised, and the reason for not sharing information should be documented. All operational and personal risks should be evaluated and mitigated to the highest degree possible. If a decision is made not to coordinate with or notify counterparts, extra precautions should be taken to ensure the CI's actions on the behalf of law enforcement are not detected, the CI's safety is not unduly put at risk, and contingency plans are developed.

Communication Plans – Handlers need to develop a communication plan and strategy tailored to the specific CI being handled. The strategies and tools adopted by the handler should not draw unnecessary attention to the CI or contacts with handlers and should fit in with the environment and persona of the CI. In addition, the communication plan should be easy to understand and implement and should ensure intelligence is reported in a secure manner. Poorly developed or hastily crafted communication strategies and practices can expose sensitive investigations, potentially compromise undercover operations, and place a CI at great personal risk. This is particularly true when operating against a sophisticated target or group.

Although in-person contacts with CIs are necessary, there are advantages to limiting meetings between CIs and handlers to avoid having the relationship inadvertently discovered. Thus, handlers should employ available tools (e.g., smartphones, email accounts) that will support the timely and secure bidirectional communication of information. The selection of tools should be based on the type of information being reported, the severity of the crimes being investigated, and the level of sophistication of the CI and any potential adversaries. Handlers should also be sensitive to vulnerabilities and risks inherent in all commercially available communication services. Prior to selecting and equipping a CI and handlers with communication tools, it is suggested that a subject-matter expert or technically trained investigator be consulted.

Supervisory Responsibilities – Proper supervision of handlers and CI management, as well as thorough reporting of all contacts with the CI, is essential. An alert, well-trained supervisor may recognize problems with a CI's behavior that the handler does not, may be able to determine that a handler is identifying too closely with the CI or a criminal lifestyle, or may notice if a handler is under excessive stress because of their association with the CI. In these situations, the supervisor should intervene as soon as possible in an attempt to prevent any potential conflict.

A key component of successful CI management is the periodic evaluation of CI activities and their results by supervisors. At a minimum, annual reevaluations of CI performance and suitability should be conducted. Other reporting requirements should be established by individual agencies, such as weekly supervisor/handler briefings, quarterly reports, or semiannual inspections. Agencies should ensure that their existing reporting requirements and inspection policies are adequate to cover the sensitive area of managing CIs and that adjustments are made as necessary.

G. Establishing and Defending Probable Cause

It is essential that law enforcement officers understand how probable cause may be developed for lawful arrests and searches involving the use of CIs. While hearsay is admissible to establish probable cause, the legal determination of probable cause requires detailed knowledge of the objective information and the source of the information.

In *Aguilar v. Texas*, the United States Supreme Court created a two-part test for establishing reliability in a case where information received from a CI was the basis for probable cause for a warrant.⁴ This required (1) establishing the credibility of the CI; and (2) establishing the reliability of the CI's information.

Later, *Illinois v. Gates*, which expressly overruled the *Aguilar* test, established the “totality of the circumstances” test to determine whether probable cause exists.⁵ In this case, an anonymous letter was considered adequate to establish probable cause. The letter contained no information that established the CI's credibility; rather, credibility was inferred from the level of detail the letter provided. *Gates* eliminated the requirement that both parts of the *Aguilar* test—reliability and basis of knowledge—be met for an affidavit based on a CI's hearsay. Currently, while a clear demonstration of the CI's reliability will reduce the need to show the CI's basis of knowledge, a detailed basis of knowledge might conversely eliminate the need to demonstrate past reliability. Thus, under *Gates*, courts will look to the strength of corroboration to satisfy probable cause absent a showing of the CI's credibility or basis of knowledge.

The issue of probable cause is intertwined with an agency's concerns over the protection of the CI's identity. In general, officers need not reveal a CI's identity on applications for arrest or search warrants, particularly when the “totality of the circumstances” attests to the presence of probable cause. Short of that, the judicial authority should be petitioned to seal the document from public record. Where documents such as arrest reports are available to the public, they should scrupulously avoid providing details of a CI's involvement in the arrest. However, in this and all other legal matters, the agency should consult legal counsel well versed in applicable federal and state law.

⁴ *Aguilar v. Texas*, 378 U.S. 108 (1964).

⁵ *Illinois v. Gates*, 462 U.S. 213 (1983).

At trial, however, agencies may find that disclosing the identity of their CI is the only way to obtain a finding of probable cause. The need for disclosure will depend on the circumstances of each case. The courts will attempt to strike a balance between the need to protect the CI—as well as protect the law enforcement agency’s need for CIs in general—and the defendant’s Sixth Amendment right to confront witnesses. Some jurisdictions may attempt to solve this dilemma by conducting in-camera hearings, where the trial judge questions the CI privately about the nature of the CI’s possible testimony.

When the court determines the CI’s identity is essential to a finding of probable cause, their identity must be disclosed or the evidence will be suppressed. When ordered to produce a CI in a hearing or trial for questioning by defense counsel, the law enforcement agency and prosecutor’s office must weigh the ramifications of disclosing the CI’s identity against the damage of terminating the charges and case. The following are some of the circumstances in which a court may rule that a CI’s identity be disclosed:

- The government’s evidence was derived solely from the efforts of the CI, making the CI’s testimony essential to prosecution. Testimony would need to occur to avoid legal issues such as hearsay (testimony from a secondhand source such as a CI handler) and circumventing the Confrontation Clause in the Sixth Amendment.⁶
- The CI witnessed a drug transaction or participated in negotiations related to the transaction.
- The CI was an active participant in events leading up to the offense.

To avoid the necessity of disclosing the identity of CIs at trial, law enforcement agencies should consider using CIs in ways that will minimize the link between the CI’s identity and probable cause. In drug cases, for example, methods would include the following:

- Using the CI only for introductions and having an undercover officer develop the relationship with the target and execute the transaction.
- Instructing the CI to leave as soon as possible after negotiations or transactions begin.
- Making the CI’s testimony cumulative. If the target can be persuaded to bring a friend, the CI’s testimony might be cumulative to what others present would say, and the CI’s identity might not need to be revealed.
- Prohibiting CI involvement in the planning functions of an operation beyond providing information.

In the vast majority of cases that involve CIs, every effort is made to keep them out of the courtroom. However, when the CI must appear as a witness, the handler will need to ensure the CI is well prepared. Accurate agency records are essential in preparing the CI for intense questioning in court. Questions must be anticipated about the CI’s background; details of the CI’s relationship with the defendant; specifics about the agency’s relationship and transactions with the CI; and, in drug cases, a host of additional questions regarding drug transactions and their documentation.

H. CI File Management

After a background investigation has been conducted on a potential CI, and the supervisor or other authorized authority has approved the CI’s use, the agency should open a file on the new CI. A CI file system has several uses, including:

- Providing a source of background information about the CI,
- Maintaining a complete history of the information received from the CI,
- Enabling review and evaluation by the appropriate supervisor of information provided by the CI,
- Minimizing incidents that could be used to question the integrity of handlers or the reliability of the CI,

⁶ Daniel A. Selwa, Attorney at Law, “Hearsay and the Sixth Amendment: Why the CI Has to Testify,” April 2017, <https://www.sclawyers.net/2017/04/04/hearsay-sixth-amendment-ci-testify/>.

- Helping to prevent unwanted duplicate uses of the same CI,
- Documenting any specific authorizations and permissions that relate to the activities and/or handling of the CI.

Key Elements of a CI File System – Master CI files should be established—one on CIs and one on unreliable informants—and an indexing system should be developed and maintained. These files should be established under the direction of a single individual, as previously determined by the agency chief executive. Within the master files, a separate folder should be maintained on each CI used by officers. Each of these individual files should be coded with an assigned CI control number.

Essentially, the master files on CIs are the operational or “working files.” Included in each individual’s CI file are the signed CI agreement, briefs of information provided, and indications of the information’s reliability. These individual files also contain the CI’s name and other identifiers—for example, fingerprints, photographs, and criminal history record. The CI’s status as active or inactive should be clearly indicated. If a CI is determined to be unreliable, that CI’s folder should be placed in the master file on unreliable informants.

For the indexing system, a summary should be prepared to correspond to each CI file. These summaries should be coded with the CI’s control number but should not include the CI’s name, photograph, or other identifying descriptors.

Securing CI Files – Tight security of CI files is imperative for officer and CI safety and to ensure the integrity of the entire CI management system. CI files should be maintained in a secured area. Access should be restricted to the agency chief executive, the individual deemed to be in charge of the CI files, or their designees. A written request from other sworn personnel should be approved by the individual in charge of the CI files before access to an individual’s CI file is permitted. Of course, CI files should be closed to the public. Other precautions may include the following:

- Keeping the files segregated from any other files and under the control of a supervisor,
- Requiring that all files be viewed in the same location,
- Screening requests for access to CI files based on a need to know,
- Requiring that records are kept of all access to CI files,
- Auditing the files (for example, semi-annually) to ensure they are maintained properly and that security procedures are being followed.

III. CONCLUSION

While the information obtained from CIs can be undeniably beneficial to law enforcement operations, their use comes with significant concerns. Therefore, CIs should not be used unless (1) all other information sources have been thoroughly explored and found lacking; (2) the potential gains clearly outweigh the risks involved; and (3) the agency has developed and is committed to following sound, written policies and procedures to govern the use and control of CIs.

APPENDIX A: SAMPLE CONFIDENTIAL INFORMANT AGREEMENT⁷

During my association with the {Agency} as a confidential informant (CI), I, the undersigned, do hereby agree to be bound by the following conditions and procedures while so associated:

1. I agree that I have no law enforcement power under the State of {State} or any local governmental subdivision and have no authority to carry a weapon while performing my activity as a CI.
2. I acknowledge that I am not authorized to engage in any criminal activity except as authorized by the {Agency} and under the supervision of the officer with whom I am associated, hereby referred to as my handler, and will not be granted immunity from prosecution for any additional crimes committed.
3. I acknowledge that I am associated with the {Agency} as a CI on a case or time basis as an independent contractor and that any payment I receive from the {Agency} will not be subject to federal or state income tax withholding or social security. All reporting of income is the responsibility of the CI.
4. I further acknowledge that as a CI and an independent contractor, I am not entitled to worker's compensation or unemployment compensation from the State of {State} and I shall not hold {Jurisdiction} liable for any injuries or damages incurred by reason of my association with the {Agency}.
5. As an independent contractor, I further acknowledge that I may not take or seek any independent action on behalf of the {Agency} or {Jurisdiction} and that I may not represent myself as an employee of same, nor enter into any contract or obligation on their behalf, unless specifically authorized to do so.
6. I further agree not to divulge to any person, except my handler, my status as a CI for the {Agency} unless required to do so in court and shall not represent myself to others as an employee or representative of the {Agency}.
7. I further agree not to use the {Agency} or any of its officers as credit or employment references unless prior approval is obtained from my handler.
8. I further agree that my association with the {Agency} does not afford me any special privileges.
9. I further agree to be truthful and not withhold information when interacting with the {Agency} and will not commit perjury.
10. I further agree that after making a purchase of anything of evidentiary value, I will deliver such evidence to my handler as soon as possible.
11. I further agree to maintain a strict accounting of all funds provided to me by the {Agency} as part of my activity as a CI. I understand that misuse of funds could be grounds for criminal prosecution.
12. I further agree to notify my handler if I have or may gather information, collect anything of evidentiary value, or engage in meetings with an individual(s) under investigation in a location outside of the jurisdictional boundaries of the {Agency}.
13. I acknowledge that I have read and fully understand the provisions of this agreement.

Dated this ____ day of ____ 20 ____.

Signatures:

Confidential Informant⁸ _____

Handler _____

Witness⁹ _____

⁷ This sample is provided only as an example. Prior to implementing such an agreement, agencies should consult with their agency's legal advisor, any local jurisdiction laws, and/or the appropriate Prosecutor's Office.

⁸ If the form contains the CI's true name, the form should be marked and treated as confidential information.

⁹ Two signatures are required to protect the handler. The witness should be another sworn law enforcement officer, typically a supervisor.

© Copyright 2020. Agencies are encouraged to use this model policy to establish one customized to their agency and jurisdiction. However, copyright is held by the International Association of Chiefs of Police, Alexandria, Virginia, U.S.A. All rights reserved under both international and Pan-American copyright conventions. Further dissemination of this material is prohibited without prior written consent of the copyright holder.

Need to Know ...

Updated: October 2020

Confidential Informants

Confidential informants (CIs) can be valuable sources of information in criminal investigations. However, in order to manage the associated risks that accompany the use of CIs, agencies should establish sound informant control policies and procedures.

- A **confidential informant (CI)** is defined as an individual under the direct supervision of a member/enforcement officer who is provided with a reasonable expectation of confidentiality and who furnishes information about suspected criminals or criminal activity for consideration, either financial, prosecutorial, or judicial; or a person who actively participates in a criminal investigation or intelligence operation, under the direct supervision of a member/enforcement officer, with or without compensation.
- Prior to using an individual as a CI, the agency should complete an **initial suitability report**. This report should be used to highlight both the risks and the benefits of using the individual as a CI.
- The **motivation** of a CI should be determined prior to their use in the field and should be a major consideration when determining if the individual is suitable to serve as a CI. CI motivation should be monitored throughout the CI's relationship with the agency.
- Certain types of individuals should require additional consideration and authorization prior to their use as a CI. These include **juveniles**; individuals obligated by legal privilege of confidentiality, such as doctors and lawyers; government officials; and persons who are in the custody of local or state departments of corrections.
- CIs should be used only to **gather information** on individuals or activities connected with a criminal investigation.
- CIs should obtain permission from their handlers prior to engaging in intelligence-gathering or other activities outside of the **jurisdictional boundaries** of the handling agency. This allows the handler the opportunity to coordinate with the appropriate agency in the location where the CI's activities will occur.
- CIs should be required to sign a **written agreement**. This agreement should outline several items, including that the CI is not a law enforcement officer and therefore has no arrest powers and is not permitted to conduct searches and seizures; serves as an independent contractor and is not entitled to worker's or unemployment compensation; and shall not withhold information when interacting with the agency or commit perjury.
- Handlers should develop **communication plans** with the goal of minimizing the risk of discovery of the CI's identity.
- Whenever possible, information provided by CIs should be **corroborated** through other investigative means.
- Supervisors play an essential role in the CI process. Attendance at **periodic debriefings** of CIs allows supervisors the opportunity to identify any potential items of concern, including undesirable CI or handler behavior.



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