118.03 Criminal Intelligence Information

1. PURPOSE

a. To establish internal controls and proper oversight for the collection, retention, dissemination, and disposition of criminal intelligence in conformance with the privacy interests and constitutional rights of individuals, groups, associations or other legal entities.

2. APPLICABILITY

a. This section applies to all Denver Police Department (the "Department") criminal intelligence systems whether or not funded as part of any multi-jurisdictional systems funded by Omnibus Crime Control and Safe Street Act of 1968 discretionary assistance awards or Bureau of Justice Assistance (BJA) formula grant program sub-grants the purpose of which is specifically to support the operation of a criminal intelligence system.

b. The policies and procedures contained in this section are in compliance with all guidelines enumerated in 28 Code of Federal Regulations Part 23, Criminal Intelligence Systems Policies. There are additional provisions, some of which are more restrictive, but none that are in conflict with the federal guidelines. The Denver Police Department shall not include, in any criminal intelligence file, information which has been obtained in violation of any applicable Federal, State or local law or ordinance, the policies of the Denver Police Department, or this section.

c. Systems that are specifically excluded from the requirements of this section and 28 Code of Federal Regulations Part 23 are:

(1) Criminal history files
(2) Contact card systems
(3) Mug shot systems
(4) Offense and accident report systems
(5) Criminal investigatory case files

3. POLICY

a. The collection, retention, dissemination, and disposition of criminal intelligence is one of the essential functions of law enforcement public service. All Department employees shall adhere to guidelines established in this section to ensure the security, confidentiality, and proper maintenance and dissemination of criminal intelligence. Criminal intelligence information will not be collected or retained except as specified in this section.

b. This policy is based on the careful review and consideration of:

(1) The guidelines identified in Title 28 Code of Federal Regulations Part 23 - Criminal Intelligence Systems Operating Policies, with policy clarifications provided by the Dept. of Justice - Bureau of Justice Assistance, Office of Justice Programs, and Office of General Counsel.

(2) California Attorney General's Criminal Intelligence Files Guidelines, also known as the Law Enforcement Intelligence Unit Guidelines.

(3) Best practices of Intelligence Unit policies from multiple law enforcement agencies.

4. GOALS

a. Provide liaison, coordination, and resource assistance in the collection, storage, exchange or dissemination, and analysis of criminal intelligence information in on-going investigations or prosecution of serious criminal activity.

b. Provide criminal intelligence information to law enforcement and criminal justice agency personnel on individuals and organizations involved with criminal organizations and enterprises.

c. Provide analysis of organized crime and criminal enterprises in Colorado. This includes identification and/or projection of major changes in crime trends.

5. DEFINITIONS

a. Criminal intelligence

(1) Data that has been processed - collected, evaluated, collated and analyzed - to be used in connection with and in furtherance of law enforcement investigative purposes. Intelligence involves data collection from both overt (information available to the general public) and covert sources. It may include general threat information not necessarily directed at a specific arrest or prosecution. Criminal intelligence data also includes information collected through undercover operations and through photographic, electronic, or other media. All criminal intelligence data shall be collected and maintained in a manner consistent with this policy.

(2) Criminal intelligence includes information that relates to an individual, organization, business, or group reasonably suspected of being involved in the actual or attempted planning, organizing, financing, or committing of one or more of the following criminal acts:

(a) Narcotic trafficking/manufacturing

(b) Unlawful gambling

(c) Loan sharking

(d) Extortion

(e) Vice and illegal pornography

(f) Infiltration of legitimate business for illegitimate purposes

(g) Stolen securities

(h) Bribery

(i) Major crimes including homicide, sexual assault, burglary, auto theft, kidnapping, destruction of property, robbery, fraud, fencing stolen property, and arson

(j) Manufacturing, use, or possession of explosive devices for illegal purposes

(k) Threats of violence, or acts of violence against or in connection with, persons or property

(l) Rioting / Inciting to riot, as those terms are defined in C.R.S. §§ 18-9-101(2), 18-9-102 and 18-9-104

(m) Computer crimes

(n) Counterfeiting

(o) Identity theft

(p) International and/or domestic terrorism, which, for purposes of this section, shall be defined as acts dangerous to human life that are a violation of the criminal law and that are intended to influence the policy of a government by intimidation or coercion

(q) Any other criminal offense not listed above which is not directly related to purely expressive behavior and is consistent with the purpose and intent of this policy.

b. Criminal Intelligence Files. Criminal intelligence information that has been collected, processed, retained in a criminal intelligence information file, and that may be shared within the law enforcement community. Criminal intelligence files include information regarding:

(1) Individuals who:

(a) Are reasonably suspected of being involved in the planning, organizing, financing, or commission of criminal activity, as set forth in paragraph 5(a)(2) above; or

(b) Are reasonably suspected of being involved in criminal activities with known or suspected criminal organizations.

(2) Organizations, businesses, and groups that:

(a) Are reasonably suspected of being involved in planning, organizing, financing, or commission of criminal activity, as set forth in paragraph 5(a)(2) above;

(b) Are reasonably suspected of being illegally operated, controlled, financed, or infiltrated by known or suspected criminal organizations; or

(c) Use illegal activities and/or enterprises as a principal means to obtain resources, support for their existence, or further their organizational goals.

c. "Criminal organization," as used in this section, consists of a group of individuals associated together in fact for a common purpose of engaging in a course of criminal conduct or activity as set forth in paragraph 5(a)(2), above.

d. Non-Criminal Identifying Information (NCI)

(1) The names of individuals, organizations, groups or businesses that are not suspected of criminal involvement, but whose identification is relevant to a criminal investigation. Examples of (NCI) would be:

(a) A member of a gang (known for narcotics trafficking) is arrested for narcotics violations while driving a car registered to his father (who is not suspected of involvement in the gang or narcotic activity). The name of the gang member and the name of the gang may be entered in the database. The father can only be entered as "non-criminal identifying information" relevant to the criminal suspect and must be clearly labeled as such.

(b) A surveillance on a criminal suspect shows the individual entering a place of

business that is not suspected of criminal activity of the suspect. The business can only be entered as "non-criminal identifying information" relevant to the criminal suspect and must be clearly labeled as such.

e. "Purge," as used in this section, shall mean the complete destruction of a physical file and the permanent deletion from any Intelligence Bureau computer files, systems or databases.

f. Reasonable Suspicion of Criminal Activity

(1) "Reasonable suspicion" is present when sufficient facts are established to give a trained law enforcement officer or criminal investigative agency, officer, investigator, or employee a particularized and objective basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal enterprise or activity, as set forth in paragraph 5(a)(2) above. The Intelligence Bureau is responsible for establishing the existence of reasonable suspicion of criminal activity through the examination of supporting information submitted, which is subject to routine inspection and audit procedures established by the Department. In determining whether "reasonable suspicion" is present, a law enforcement officer or criminal investigator may consider, within the totality of circumstances, the fact that the individual or organization has been involved in serious criminal activity or conduct in the past. Past criminal activity, without more, shall not be sufficient to satisfy the reasonable suspicion requirement. If "reasonable suspicion" is based, in whole or in part, on information obtained through electronic, video, or audio means, that fact and the existence of such information shall be noted in the criminal intelligence file.

6. PROCEDURES FOR MANAGING CRIMINAL INTELLIGENCE FILES

a. SUPERVISION OF DATA ENTRY

(1) All criminal intelligence data shall be reviewed by an Intelligence Bureau supervisor or commanding officer prior to entry into any criminal intelligence file. The supervisor or commanding officer shall determine that the criminal intelligence data conforms to these policies and was not obtained in violation of any applicable Federal, State, or local law or ordinance, Department policies, or this section. Criminal intelligence data will not be placed in any criminal intelligence file unless approved by an Intelligence Bureau supervisor or commanding officer. The badge number of the approving supervisor or commanding officer will become part of the file.

b. INFORMATION SUBMISSION CRITERIA

(1) The Department shall only collect or maintain criminal intelligence information concerning an individual or organization if there is reasonable suspicion that the

individual or organization is involved in criminal conduct or activity, as set forth in paragraph 5(a)(2) above, and the information is relevant to that criminal conduct or activity. The existence of reasonable suspicion will be based on specific, articulable facts that will be documented in the criminal intelligence file.

(2) The Department shall not collect or maintain information about the political, religious, social views, associations or activities of any individual or any group, association, corporation, business, partnership, or other organization, unless such information directly relates to criminal conduct or activity and there is a reasonable suspicion that the subject of the information is or may be involved in that criminal conduct or activity.

(3) Non-Criminal Identifying Information (NCI) - Under the following circumstances, the names of individuals, organizations, groups or businesses that are not suspected of criminal involvement, but that provide relevant descriptive, identifying information regarding the criminal suspect, may be entered as "Non-Criminal Identifying Information." A non-criminal identifying label should say that "This individual or organization has been entered into the system for identification purposes only -- he, she or it is not suspected of any criminal activity or involvement." This label will act as a disclaimer of criminal association and will not be used to meet reasonable suspicion requirements to create a file or record for that individual or organization.

c. EXCLUDED MATERIAL. Only lawfully collected information based on a reasonable suspicion of criminal activity and that meets the Department's criteria for file input should be stored in the criminal intelligence file. Information that shall be specifically excluded from criminal intelligence files includes:

(1) Information on an individual or group merely on the basis that such individual or group support unpopular causes.

(2) Information on an individual or group merely on the basis of race, gender, age, or ethnic background.

(3) Information on an individual or group merely on the basis of religious or political affiliations, or beliefs.

(4) Information on an individual or group merely on the basis of personal habits and/or predilections that do not break any criminal laws or threaten the safety of others.

(5) Information on an individual or group merely on the basis of involvement in expressive activity that takes the form of non-violent civil disobedience that amounts, at most, to a misdemeanor offense.

d. FILE CRITERIA. All information retained in the criminal intelligence file will meet the criteria prescribed by the Department. There are two types of intelligence records - Permanent and Temporary files.

(1) Permanent Intelligence Files. Criminal Information may be retained in the permanent intelligence files for up to five (5) years. At that time, criminal information will be automatically purged unless new criminal intelligence has been developed establishing reasonable suspicion that the individual and/or organization continues to be involved in a definable criminal activity or enterprise. When updated criminal intelligence is added into the permanent files on a suspect individual or organization already listed in the database, such entries reset the five year standard for retention of that file. Permanent intelligence files must be periodically reviewed for compliance with this policy consistent with paragraph 9 below.

(2) Temporary Intelligence Files. Criminal Information may also be entered into temporary criminal intelligence files when there is reasonable suspicion of criminal activity, but that finding is based, in part, upon "unreliable" or "unknown" sources, or where the content validity of the information is "doubtful" or "cannot be judged." All temporary intelligence files shall be specifically designated as such and must be reviewed by a supervisor every sixty (60) days for validity. This interim review must be documented in the temporary intelligence file. Temporary intelligence files shall be retained no longer than one year. At that time, temporary files must be either purged or converted into permanent intelligence files. All temporary intelligence files will be kept distinctly separate from the general database.

e. INFORMATION CLASSIFICATION

Information to be retained in the files of the Department shall be labeled for source reliability and content validity prior to entry or submission. Circulating information that has not been evaluated, where the source reliability is poor or the content validity is doubtful, is detrimental to our agency's operations and is contrary to the individual's right to privacy. The classification of criminal intelligence information is subject to continual change, the passage of time, the conclusion of investigations, and other factors that may affect the security classification or dissemination criteria assigned to particular documents.

Documents within the intelligence files should be reviewed on an ongoing basis to ascertain whether a higher degree or lesser degree of document security is required and to ensure that information is released only when and if appropriate.

(1) Source Reliability - The reliability of the source is an index of the consistency of the information the source provides. The source shall be evaluated according to the following:

(a) RELIABLE - The reliability of the source is unquestioned or has been tested in the past.

(b) USUALLY RELIABLE - The reliability of the source can usually be relied upon. The majority of the information provided in the past has proved to be reliable.

(c) UNRELIABLE - The reliability of the sources has been sporadic in the past.

(d) UNKNOWN - The reliability of the source cannot be judged; either experience or investigation has not yet determined authenticity or trustworthiness.

(2) Content Validity - The validity of information is an index of the accuracy or truthfulness of the information. The validity of the information shall be assessed as follows:

(a) CONFIRMED - The information has been corroborated by an investigator or another reliable independent source.

(b) PROBABLE - The information is consistent with past accounts.

(c) DOUBTFUL - The information is inconsistent with past accounts.

(d) CANNOT BE JUDGED - The information cannot be judged. Its authenticity has not yet been determined by either experience or investigation.

(3) Sensitivity - The sensitivity of the information shall be classified according to the following standards:

(a) SENSITIVE - Information, including, but not limited to, active police investigations, informant identification information, corruption, and those reports which require strict dissemination and release criteria.

(b) RESTRICTED - Information obtained through intelligence channels that is not classified as sensitive and is for law enforcement use only. Restricted information may include previously classified sensitive information for which the need for a high level of security no longer exists.

(c) UNCLASSIFIED - Information that is public in nature. This includes arrest and criminal record information and other information contained in records of official actions.

7. INFORMATION DISSEMINATION

a. Intelligence Bureau officers shall disseminate criminal intelligence information only where there is a need to know and a right to know the information in the performance of a law enforcement activity.

(1) Except as noted in paragraph (2) of this section, officers shall disseminate criminal intelligence information only to law enforcement authorities who shall agree to follow procedures regarding information receipt, maintenance, security, and dissemination that are consistent with these principles.

(2) Paragraph (1) of this section shall not limit the dissemination of an assessment of criminal intelligence information to a government official or to any other individual, when necessary to avoid imminent danger to life or property.

b. Criminal intelligence information may only be shared with other law enforcement agencies with the express written approval of an Intelligence Bureau supervisor or commanding officer. The release of this information shall be based on a need to know and right to know basis. The facts establishing the requestor's need to know and right to know shall be documented in the criminal intelligence file. The agency and/or officer requesting the information, the officer approving the sharing, the law enforcement purpose for the request, the date of the request, and the date of the provision of the information shall all be noted in the file. The agency and/or officer requesting the information shall agree in writing to be bound by the Department policy relating to the storage, retrieval and dissemination of the information provided.

(1) In maintaining criminal intelligence information, the Department shall ensure that administrative, technical, and physical safeguards (including audit trails) are adopted to ensure against unauthorized access and against intentional or unintentional damage. A record indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the bureau shall be kept. Information shall be labeled to indicate levels of sensitivity, levels of confidence, and the identity of requesting agencies and control officials. The officer releasing information shall document in the criminal intelligence file the existence of an inquirer's need to know and right to know the information being requested, either through inquiry or by delegation of this responsibility to a properly trained participating agency, which information release is subject to routine inspection and audit procedures established by the bureau.

(2) Criminal intelligence information shall only be shared with other members of the Department on a need to know basis. The officer requesting the information and the justification for the request shall be noted in the file.

c. Intelligence Bureau personnel will not release any original intelligence documents. Whenever information from a criminal intelligence file is disclosed, in any form, either orally, in writing, or through inspection of files, the Intelligence Bureau must comply with the requirements set forth in paragraph 7(b) above.

d. Need to know

(1) Requested information is pertinent and necessary to the requesting agency in initiating, furthering, or completing the performance of a law enforcement activity.

e. Right to know

(1) Requester is acting in an official capacity and has statutory authority to obtain the information being sought.

f. Intelligence Bureau information will be released according to the following classification and release authority levels:

(1) SENSITIVE - Information in this class may only be released with permission of the Intelligence Bureau commanding officer to law enforcement agencies that have a demonstrated right to know and need to know.

(2) RESTRICTED - Restricted information may be released by Intelligence Bureau personnel to law enforcement agencies that have a demonstrated right to know and need to know.

(3) UNCLASSIFIED - Any Intelligence Bureau personnel may release this information to a Denver Police Department officer or other law enforcement agency. The Chief of Police is the official records custodian and the Chief must approve the release of information to the public or media.

8. SECURITY OF FILES

a. Criminal intelligence files will be physically secured in locked cabinets or in electronic files that are equipped with security protection measures. Those files and databases will be secured during off-hours and when the office is vacant.

b. Key access to the Intelligence Bureau will only be granted to assigned Bureau personnel.

c. Locks, combinations and system passwords will be changed upon the transfer of any member.

d. Bureau personnel will adopt a “clean desk” policy to include the removal of sensitive documents from view when not in use. The orientation of computer monitors will be such as to preclude casual observation by visitors and there will be control of sensitive conversations.

9. REVIEW AND PURGE PROCEDURES

a. Reviewing and purging of all information that is contained in the Department criminal intelligence files and kept under paragraph 6 above will be done on an ongoing basis, but, at a minimum, will be accomplished annually. The dates when reviews occurred shall be noted in the criminal intelligence file. The maximum retention period is five years, and a criminal intelligence file must be purged after five years unless the information in that criminal intelligence file has been updated consistent with this section. The Department may update the criminal intelligence file and extend the retention period at any time, based on reasonable suspicion of new criminal activity documented in the criminal intelligence file.

b. The decision to purge information should by guided by the following considerations:

(1) Whether or not the information in the criminal intelligence file continues to comply with the reasonable suspicion standard set forth in paragraph 5(f)(1) above.

(2) Defined retention periods for permanent and temporary files.

(3) Specific credible threats to government officials and/or law enforcement officers.

c. Any information that is found to be collected or retained in violation of this section, or found to be inaccurate, misleading, or obsolete, shall be purged. Any recipient agencies shall be advised of such changes and that the subject information has been purged.

10. TRAINING

a. The commanding officer of the Intelligence Bureau and any bureau, section or unit with responsibility to gather criminal intelligence information shall ensure that all officers assigned to the bureau, section or unit have received training regarding this section. Training will be documented in the officer’s training records.

b. The commanding officer of the Intelligence Bureau and any bureau, section or unit with responsibility to gather criminal intelligence information shall ensure that all officers assigned to the bureau, section or unit receive annual update training regarding this section and any recent court decisions and best practices regarding criminal intelligence information. Training will be documented in the officer’s training records.

c. An outline of the training will be kept on file at the Intelligence Bureau and the Training Academy.

d. An annual review will also be conducted of this section and the policy will be updated based on recent court decisions and national best practices.

11. INDEPENDENT OVERSIGHT

a. Implementation of this policy shall be subject to an audit by an independent agency. This audit shall review data collection, categorization, maintenance, dissemination and Intelligence Bureau practices, as well as training procedures, to verify compliance with established rules and policies.

b. The individual who conducts the audit for the independent agency shall be familiar with these policies and procedures, and the policies and procedures set forth in paragraph 3(b) above. The individual who conducts the audit for the independent agency shall have access to all Intelligence Bureau files and data necessary to perform the audit function, and will be provided with the financial resources necessary to complete the audit and report. The audit shall be conducted on a quarterly basis for the first year, a semi-annual basis for the second and third years, and annually thereafter.

c. The individual who conducts the audit shall prepare a written report which will be provided to the commanding officer of the Intelligence Bureau, the Chief of Police, the City Attorney and the Public Safety Review Commission.

d. The commanding officer of the Intelligence Bureau shall prepare a written response to the audit report within ten (10) days of receipt and copies of that response will be provided to the Chief of Police, the City Attorney and the Public Safety Review Commission. The Public Safety Review Commission shall have the right to submit to the Mayor its comments regarding the audit report and the Intelligence Bureau's response within ten (10) days after receipt of the Intelligence Bureau's response.

e. Any conflict between the findings in the audit report and the response prepared by the commanding officer of the Intelligence Bureau shall be resolved by the Mayor.

f. In the event the audit report determines that a criminal intelligence file was improperly opened in violation of paragraph 6(c) above, and that finding is sustained by the Mayor, the Intelligence Bureau will notify in writing the subject of that criminal intelligence file that a file was improperly opened and will be purged. Upon request, the subject will be provided with a copy of his/her criminal intelligence file, with necessary redactions to protect the privacy of third-parties and the safety of law enforcement officers.