





POLICIES AND PROCEDURES MANUAL

	CRIMINAL INTELLIGENCE	
	POLICY NUMBER: 40-2	ISSUING AUTHORITY 
	EFFECTIVE DATE: January 1, 2025	Christine A. Elow Police Commissioner

I. GENERAL CONSIDERATIONS AND GUIDELINES

The analysis and use of actionable intelligence should be practiced with care by those departments assuming this function. Although these efforts may significantly assist in the detection and prevention of major criminal activities, the application of vetted procedures and protocols is essential to ensuring that the information conforms to legal requirements and that the public's confidence in the department is not jeopardized.

Intelligence analysis for these purposes should be premised on circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity. These efforts should be specific in focus and clearly directed to address actual or articulable potential criminal concerns. Additionally, department policy and Massachusetts General Law should address the intrusiveness of the investigatory efforts regarding the prevention of criminal conduct or its planning. Department policy should also establish the means by which such information is shared and distributed among public safety professionals.

To balance law enforcement's need to gather and maintain critical intelligence with the privacy of individuals to whom such data relates, the federal government has outlined policy guidelines applicable to all criminal intelligence units operating through support under the Omnibus Crime Control and Safe Streets Act. (See 28 C.F.R. Part 23.) Through this policy, the Cambridge Police Department adopts those standards for the department's intelligence function operating with or without federal funding.

II. POLICY

It is the policy of the Cambridge Police Department to:

- A. analyze, process, disseminate, and maintain information directed toward specific individuals or organizations where there is a reasonable suspicion of their involvement in planning or engaging in criminal activity;
- B. participate with other law enforcement agencies in analyzing and sharing information; and
- C. afford all subjects every constitutional and statutory right guaranteed under the law by ensuring individual privacy, civil rights, civil liberties, and other protected interests.

III. DEFINITIONS

- A. *Criminal activity*: Specific, prohibited conduct committed in violation of federal or state law where the consequence of conviction by a court is punishment, especially where the punishment is a serious one such as imprisonment.
- B. *Criminal intelligence*: Information gathered, analyzed, recorded/reported, and disseminated by law enforcement agencies concerning types of crime, identified criminals, and known or suspected criminal groups.
- C. *Reasonable suspicion*: There are trustworthy facts and inferences that would lead a reasonable person to believe that there is a concrete possibility that a crime was, is, or will be committed; and sometimes the suspect is armed and dangerous.

IV. PROCEDURES

- A. 40.2.1 (M) Criminal Intelligence Data Collection
 - 1. Criminal intelligence activity and the use of criminal justice, as well as non-criminal justice sources and individuals, are as follows.
 - a. All intelligence gathering activities intended to assist in the detection and prevention of crimes shall be premised on circumstances that provide a reasonable suspicion that specific individuals or organizations may be planning or engaging in criminal activity.
 - (1) Such criminal activity may include, but not be limited to, narcotics, human trafficking, and terrorism.
 - (2) Criminal activity may be limited in scope or broad and organized.
 - b. All intelligence gathering activities shall conform to any applicable federal or state laws and shall consider the importance of maintaining the public's confidence and trust.
 - c. Intelligence gathering efforts shall be specific in focus and shall be clearly directed to address actual or articulable potential criminal concerns.
 - d. To address the intrusiveness of investigatory efforts, information shared between the department and other departments shall be limited to where there is a need to know and a right to know the information in the performance of a law enforcement activity.
 - e. Information shared with the public shall be carefully managed and limited to protect the privacy rights of the community at large. These efforts will be coordinated with the department's Director of Communications/Public Information Officer.
 - f. The acquisition and application of electronic surveillance equipment and techniques is strictly limited by City of Cambridge Ordinance Chapter 2.128 *Surveillance Technology Ordinance*. Care shall be taken to comply with this directive.
- B. 40.2.2 (M) Intelligence Analyses Procedures
 - 1. Criminal intelligence analysis procedures include the following.

a. Sources from which information is collected.

- (1) Information collected shall be limited to criminal conduct or activities that present a potential public safety threat to the City of Cambridge community. The supervisor of the Crime Analysis Unit or designees may evaluate incoming information to ensure that intelligence analysis is limited to criminal conduct or relates to activities that present a potential threat to the City of Cambridge community.
- (2) The collection and dissemination of intelligence information about the political, religious, or social views, associations, or activities of any individual or any group, association, business, or other organization, is prohibited unless such information directly relates to criminal conduct or activity and there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.
- (3) The need to ensure that an individual's constitutional rights, civil liberties, civil rights, and privacy interests are protected throughout the intelligence process is crucial to the long-term success of criminal intelligence sharing and maintaining the public's trust. Protecting these rights, while at the same time providing for homeland security and public safety, requires a commitment from everyone in the department and other collaborating agencies.
- (4) The department may consult with legal counsel on matters related to criminal intelligence when seeking privacy or legal guidance.

b. Disseminating analysis findings.

- (1) All requests for information shall be assessed on a *need to know* and *right to know* basis, as outlined below in section IV.C.4.
- (2) The supervisor of the Crime Analysis Unit or designees have an obligation to notify the appropriate law enforcement agency when it is determined that information ascertained by the Crime Analysis Unit may result in imminent danger to persons or property.

C. 40.2.3 (M) Criminal Intelligence Procedures

1. Procedures that address receiving or collecting and sharing of criminal intelligence information with appropriate entities include the following.

a. Purpose and responsibility of personnel.

- (1) Intelligence is the systematic gathering, evaluation, processing, and sharing of information related to criminal and homeland security activities that may present a threat to the community. Typically, these activities include organized crime, vice, drugs, organized civil disorder, terrorism, and criminal conduct. The purpose of this function within the police department is to anticipate, monitor, and prevent criminal activity.
- (2) It is the responsibility of all department personnel, upon receipt of information that may result in imminent danger to persons or property, whether through a reporting party, observation, or other means, to communicate immediately and appropriately,

verbally and in writing, to the shift commander if immediate action is necessary, and to the Lieutenant of Investigations and the supervisor of the Crime Analysis Unit or designees and confirm receipt. The information shall then be vetted.

- (3) Relevant information may be collected from a variety of sources including patrol officers, community members, cases, and public websites.
- (4) Relevant information may be collected from publicly available social media websites that would be readily available to any member of the public. Any information collected from social media websites that a reasonable person would have expected to be private must be collected in accordance with applicable law and the City of Cambridge Ordinance Chapter 2.128 Surveillance Technology Ordinance.
- (5) All personnel, as part of their job duties, are expected to observe and report any suspicious or potential criminal activity.

2. Procedures for evaluating intelligence information.

- a. Any intelligence information received by the department that is to be disseminated internally or externally shall be assigned a *level of confidence*. The level of confidence gives the recipient an indication of how the submitter feels about the content of the information. Level of confidence is a two-part process.

- (1) *Source reliability* refers to the reliability of the source of the information. The following codes shall apply.

- (i) Reliable: the reliability of the source is unquestioned or has been well tested in the past.
- (ii) Usually Reliable: the source can usually be relied upon.
- (iii) Unreliable: the reliability of the source has been sporadic in the past.
- (iv) Unknown: the reliability of the source cannot be judged.

- 1. Information obtained with source reliability determined to be unreliable or unknown may need to be held until further corroboration is obtained.

- (2) *Content validity* refers to the accuracy or truthfulness of the information. The following codes shall apply.

- (i) Confirmed: the information has been corroborated by an investigator or another reliable source.
- (ii) Probable: the information is consistent with past accounts.
- (iii) Doubtful: the information is inconsistent with past accounts.
- (iv) Cannot be judged: the information cannot be judged.

- 1. Information obtained with content validity determined to be doubtful or unable to be judged may need to be held until further corroboration is obtained.

3. Procedures for safeguarding, securing, and storing information.
 - a. Any information documented in a report will be securely stored in the department Records Management System with restricted access.
 - b. Any criminal intelligence not stored in the Records Management System, such as informational flyers, intelligence briefings, emails, or operational plans will be handled and shared by department personnel in an appropriate manner.
 - c. All documents produced by the Crime Analysis Unit will bear the sensitivity classification level appropriate for that product.
 - (1) Law Enforcement Sensitive: will be used when the document contains criminal investigative information, intelligence, or CORI-protected information. This level is restricted only to law enforcement personnel having a specific need to know and right to know.
 - (2) Sensitive: will be used when the product contains CORI-protected information but does not contain criminal investigative information or intelligence. This level can be released to non-law enforcement personnel with a CORI certification and non-disclosure agreement.
 - (3) Not For Public Release: will be used when the product does not contain CORI-protected information, criminal investigative information, or intelligence. This level can be released to private sector and non-law enforcement partners.
 - (4) For Public Release: will be used when the product does not contain CORI-protected information, criminal investigative information, intelligence, or information considered to be Not for Public Release. This level can be released to anyone. To generate the most widespread awareness for an investigation, efforts will be coordinated with the department's Director of Communications/Public Information Officer to publish information to the media, online with the department and city accounts, and other organization partners. The department's Director of Communications/Public Information Officer should be made aware of any notifications made to Massachusetts Most Wanted and other websites or accounts that can be accessed by any members of the public.
 - d. In the interest of protecting the confidentiality, privacy, and civil liberties of all subjects, the department will make all reasonable efforts to comply with 28 CFR Part 23. (LEIU Criminal Intelligence File Guidelines and the Justice Information Privacy Guidelines.)
4. Requirements and procedures for the distribution of information.
 - a. Criminal intelligence shall be appropriately documented, reported, and disseminated on a need to know/right to know basis.
 - b. Need to Know: A recipient agency or individual has a need to know when the requested information is pertinent to and necessary for the initiation or furtherance of a criminal investigation or apprehension. The need to know also takes into consideration the risks to officers and their safety.

- c. Right to Know: The right to know is satisfied when the recipient agency or individual has the official capacity and statutory authority to receive the intelligence information.
 - d. All requests for restricted and sensitive information as outlined in this policy must be directed to and approved by a supervisor in the Investigations Unit or designee.
 - e. A record shall be kept indicating who has been given information, the reason for release of the information, and the date of each dissemination outside the department.
5. Procedures for purging information.
- a. The maximum retention period for criminal intelligence is five years; at that time the record must be either purged or undergo a review-and-validation process.
 - (1) If a record is reviewed and validated, it will receive a new retention period of up to five years.
 - (2) For a record to be validated, the submitting agency must determine that the subject is still reasonably suspected of involvement in current criminal activity and that the record continues to meet the 28 CFR Part 23 submission criteria.
 - (3) A record may be validated at any time during its retention period; however, simply updating the identifying information about the subject during the retention period is not enough by itself to indicate the subject is still reasonably suspected of involvement in current criminal activity.
 - b. By the end of each calendar year, the supervisor of the Investigations Unit and the supervisor of the Crime Analysis Unit or designees shall review all information maintained in the records management system to determine which information is to remain on file, modified, updated, or purged.
 - (1) Records that have been identified to be purged from the system shall be reviewed by the supervisor of the Investigations Unit and supervisor of the Crime Analysis Unit. No record may be destroyed without prior approval from the Superintendent of the Investigations Unit, deputy superintendent of the Crime Analysis Unit, or the Police Commissioner.
 - (2) All records that have been approved for purging shall be destroyed by the Supervisor of the Investigations Section or Supervisor of the Crime Analysis Unit, and this responsibility shall not be designated to any other officer.
 - c. The supervisor of the Investigations Unit and supervisor of the Crime Analysis Unit shall be responsible for documenting in a written report the results of the annual review. The report will reflect all actions taken including identifying those records that are being maintained and describing the reason for retaining those records.
 - d. Out-of-date flyers and other time-limited intelligence that is no longer useful will be destroyed or deleted as soon as possible.
6. Annual review of procedures and processes.

- a. The annual report shall be forwarded to the Police Commissioner or designee, and a copy of the report will be retained in the Records Management System.