



Eric Hawkins
Chief of Police

ALBANY, NEW YORK
POLICE DEPARTMENT
165 HENRY JOHNSON BOULEVARD
ALBANY, NEW YORK 12210



1789

INFORMATION COORDINATION UNIT
GENERAL ORDER NO: 3.7.00

Issue Date: January 17, 2019	Effective Date: August 24, 2015
Revision Date: November 29, 2016	CALEA: 40.1.1, 40.2.1, 40.2.2, 40.2.3
Volume 3: Operations	Chapter 7: Information Coordination Unit
Distribution: All Personnel	NYSLEAP: 50.7
Issuing Authority: Chief Eric Hawkins	Page: 1 of 7

PURPOSE: The purpose of this policy is to establish the authority for information requirements and reporting responsibilities of this agency's crime analysis function.

POLICY: It is the policy of the Albany Police Department to provide accurate and timely crime and related information to all units and personnel of the department. The Information Coordination Unit will constantly strive to develop information resources, distribution systems, and analytical techniques to provide the best possible informational support to the police department.

DEFINITIONS: **Crime Analysis** – Crime analysis means a system to collect information on crimes and criminals from a variety of sources to identify crime patterns, methods of operation, and events associated with criminal activity; and disseminate that information to assist in crime control and prevention activities, and long range planning.

I. ADMINISTRATION

A. The Information Coordination Unit (ICU) is housed within the Albany Crime Analysis Center (ACAC), and staffed with both sworn and non-sworn personnel tasked with the rapid organization and dissemination of accurate crime data to complement the crime reduction strategies of the department and surrounding police agencies.

B. ICU is under the direct command of the Commander of Investigations.

1. The Sergeant of ICU shall be responsible for overseeing the daily activities of the following functions:

- a. ICU Detectives;
- b. Crime Mapping; and
- c. Crime Analyst Supervisor, who is directly responsible for overseeing the daily activities of the Crime Analysts.

C. The Director of the Albany Crime Analysis Center (ACAC) at the New York State

Division of Criminal Justice Services (DCJS) works concurrently with both sworn and non-sworn members of ICU, as well as other key partner agencies.

1. NYS DCJS supports many department processes including, but not limited to data connectivity between multiple agencies.
2. Analysts utilize various analytical tools, software, mapping programs and other resources to link crimes, suspects, locations, and any additional relevant data, in order to provide the department and other local police departments with vital and accurate information in a timely manner.

D. Criminal Information and Intelligence Resources:

1. Crime information and intelligence is made available to department personnel on the Department's Internal Homepage via the following links:
 - a. Intelligence;
 - b. Special Wants;
 - c. Weekly Wants;
 - d. ID Suspects; and
 - e. The Investigative Tools Link (by clicking on ICU Resources).

E. An integral tool to the ICU and ACAC is Interactive Crime Mapping. This technological resource is used to visualize and identify patterns and "hot spots," thereby enabling supervisors to allocate appropriate personnel and resources to address issues in the areas of the City most in need, at the moment they are needed most.

1. Mapping technology is made available to department personnel on the Department's Internal Homepage, by clicking on the Mapping link.
2. Mapping technology is also available to the public via the City of Albany Police Department Website, by clicking on the Crime Mapping link.
 - a. This link allows citizens to have free access to updated information about reported incidents in each neighborhood, annual crime statistics, as well as an opportunity to anonymously provide information about their neighborhood.

II. DATA COLLECTION

A. Crime analysis data may be extracted from sources which available to the department. These sources include, but are not limited to:

1. Offense Reports;
2. Field Interview Reports;
3. Investigation Reports;
4. Computer Records;
5. Crime Analysis of Other Agencies;
6. Meetings;
7. Commercial Databases; and
8. Other sources as they become available.

B. At a minimum, the following shall be documented for analysis:

1. Crime data pertaining to frequency;
2. Type, temporal and geographic distribution;
3. Victimization;
4. Target characteristics;
5. Method of operation; and
6. Suspect and vehicle descriptors.

III. DATA ANALYSIS

A. The type of analysis conducted shall depend upon the nature of the problem and the data that is available. Relevant factors for crime analysis include, but are not limited to:

1. Frequency by type of crime;
2. Temporal and geographic distribution;
3. Method of operation;
4. Physical evidence;
5. Target;
6. Suspect and suspect vehicle descriptors; and
7. Factors related to community problems.

B. Crime analysis reports shall be formatted to present the data in the clearest manner possible, including but not limited to:

1. Graphs;
2. Spreadsheets;
3. Spot maps;
4. Fliers;
5. Bulletins; or
6. Narrative reports.

C. Many crime trends are initiated by operational members within the department as daily crime sources are reviewed.

1. In cases where any member identifies a possible crime trend they should route such findings to the appropriate units/personnel as soon as possible.
2. In cases where advanced crime analysis or analytical investigative skills are required, the request should be forwarded via the chain-of-command to the ICU D/Sergeant and CIU Lieutenant.

IV. CRIMINAL INTELLIGENCE

A. The Albany Police Department recognizes that the gathering of intelligence information, to include the evaluation, dissemination, and security of such information, is an important aspect of the law enforcement function.

1. Individuals or groups known to be or suspected of being involved in criminal acts, or who are known to be or suspected of being involved in the threatening, planning, organizing, or financing of criminal acts shall be

considered a threat to the community.

2. The Albany Police Department shall maintain a criminal intelligence function with the purpose of collecting and analyzing information on groups and individuals who are known to be or suspected of being involved in activities that present a threat to the community.
3. All members are encouraged to develop and gather effective and lawful intelligence data whenever appropriate.
4. All information determined to be criminal intelligence shall be maintained in criminal and investigative databases by the Albany Police Department's Information Coordination Unit (ICU) database.

B. Procedures:

1. The criminal intelligence function is a component of CIU, and shall be under the direct command of the Commander of Investigations.
2. Members of the Albany Police Department and departmental equipment may be used as necessary for the collection of raw data, strategic intelligence, tactical intelligence, and as support for legitimate overt and covert law enforcement operations. Criminal intelligence shall in no way be used to collect information for any reasons not specifically related to crime or suspected criminal activity.
3. To ensure the legality and integrity of its operations, information is only to be gathered relative to legitimate investigative objectives relating to the control and prevention of criminal conduct, and activities that present a threat to the community.
4. The collection of intelligence information shall be strictly limited to information concerning individuals or groups known to, or suspected of, threatening, planning, organizing, financing or committing criminal activities that constitute a threat to this community. Examples of such criminal activity include, but are not limited to:
 - a. Organized crime activity;
 - b. Illegal drug activity;
 - c. Vice related activity;
 - d. Terrorism;
 - e. Gang related activity;
 - f. Activities promoting community unrest; or
 - g. Other activity that poses a potential threat to the community.
5. Any authorized employee may initiate an inquiry by contacting CIU and/or ICU Sergeant but information will be disseminated only on a need to know/right to know basis.

C. Information Documentation and Dissemination:

1. If information is received on a subject, the subject's status shall be checked through the SAFETNet (Secure Automated Fast Event Tracking Network).
 - a. If the subject has been previously entered into SAFETNet by another agency, the originating agency shall be contacted prior to

the release or dissemination of any information.

- b. ICU personnel shall then determine the restrictions on dissemination of information and shall link information accordingly in the databases.

2. Criminal intelligence shall be disseminated only to law enforcement or criminal investigative authorities that will agree to follow procedures regarding information receipt, maintenance, security, and dissemination.

- a. This shall not limit the dissemination of an assessment of criminal intelligence to a government official or to any other individual, when necessary, to avoid imminent danger to life or property.

3. Restrictions on release of information shall be enforced, with the exception that a contributor of information may view the data they submitted regardless of the designated dissemination level.

4. Agencies may have access to any information they submit and are responsible for the content, validity, and usefulness. The CIU Commander or his/her designee shall determine who has a need to access the agency's records and to what extent.

5. Telephone, e-mail, and facsimile requests for criminal intelligence shall be addressed only after the requester's identity has been verified.

- a. Online access confirmation may be through the use of passwords or other security devices.

- D. Prior to entry into the database, the ICU sergeant or his/her designee, shall ensure that the information collected is limited to criminal conduct or relates to activities that present a potential threat to the jurisdiction, as well as ensure that it is criminal intelligence information collected is in compliance with this policy and applicable laws in order to protect the rights and privacy of individuals.

1. If necessary, the reviewing supervisor shall contact the submitting officer to gather additional information that may be needed to facilitate entry into the system.
2. Information that is not in compliance shall not be entered into the system.
3. The criminal intelligence function shall in no way be utilized to collect information for any reasons not related to crime or suspected criminal activity.

- E. Bulletins shall be disseminated within the system to appropriate personnel and shall typically remain active for (30) days. Expired bulletins shall be deactivated and stored in department databases.

- F. The ICU sergeant, or his/her designee, shall typically deactivate bulletins containing intelligence information that is out of date or no longer serves as a valid informational source. This information shall be purged from the system in accordance with the following procedures:

1. All intelligence files on suspected criminals and criminal activity shall be reviewed regularly by the ICU supervisor and his/her staff.

2. Records shall be made inactive and removed from department databases and purged when no new information has been received which would indicate continued criminal activity or the possibility of continued criminal activity in the future.
 3. The decision to purge information may also be guided by the following considerations:
 - a. The number of requests for the file/individual;
 - b. The validity of the data;
 - c. The reliability of the data;
 - d. Federal/State Law;
 - e. The time in the file;
 - f. Present or future strategic or tactical operations; and,
 - g. Reasonable suspicion criteria and investigative interest.
- G.** Officers wishing to submit information for possible entry into the intelligence system shall reduce the information to writing by completing a SIR, a Supplemental Report or an Investigation Report and forwarding it to their supervisor for approval.
1. These reports shall then be forwarded to the CIU supervisor through the appropriate chain of command.
 2. The ICU supervisor, or his/her designee, shall review the information to determine whether it should be forwarded and entered into the databases.
 3. No information shall be entered into the database without the approval of an ICU or CIU supervisor, or his/her designee.
 4. Inquiry requests by authorized persons may be made to the CIU/ICU detectives and/or CIU/ICU Sergeants by phone, in writing, or electronic format.
 - a. Information shall be disseminated only on a need to know/right to know basis.
 - b. Criminal intelligence shall be disseminated only to law enforcement or criminal investigative authorities
- H.** Periodically, personnel shall receive training and instruction on the department's policies and procedures relating to the collection, processing, and sharing of intelligence information and information regarding suspicious activity that presents a threat to the community.
1. This review and instruction may be in the form of in-service training, roll call training, or online training.
- I.** Annually, a review of the procedures and processes in relation to the collection, processing, and sharing of criminal intelligence shall be completed by the ICU D/Sergeant.
1. This review shall be completed by no later than February 1st of each calendar year, and documented on an IDC to the Chief of Police.
 2. Based upon the documented annual review, the Chief of Police shall determine if modifications to policies and procedures are required.

J. File Security:

1. Access to the databases shall be limited to those persons authorized by the Commander of Investigations. This shall include ICU sworn and non-sworn personnel.
2. Access to the entry, deletion, and/or modification of the department databases relating to suspicious incidents and criminal intelligence relating to criminal and homeland security activities shall be restricted to the Commander of Investigations, ICU personnel, or to other personnel as authorized by the Chief of Police.

V. DISSEMINATION

- A.** To be of maximum benefit, crime analysis shall be distributed to the appropriate units/personnel as soon as possible.
1. Except for special requests, most crime analysis shall be distributed department wide.
 2. While some crime analysis data can be distributed electronically, some reports may need to be distributed in hard copy because of attachments that may need to be included.
 3. Copies of all crime analysis shall be forwarded to the Chief of Police, either by electronic or hard copy means.
- B.** Unit/Station commanding officers shall maintain active working relationships with his/her counterparts from other law enforcement agencies through meeting attendance and information exchange to identify crime trends and patterns that cross jurisdictional boundaries.
1. Information relayed to other law enforcement agencies shall indicate it is for official police use only.
- C.** The timeliness and format of crime analysis reports is vital to the usefulness of information generated. To that end, such reports shall:
1. Be tailored to meet the particular requirements of patrol, investigative and administrative personnel;
 2. Arrive in a timely manner that allows a reasonable time for officers to develop and implement countermeasures and response strategies for the problem at hand;
 3. Present in an objective manner that distinguishes conclusions from theories and indicates the degree of reliability of report conclusions; and
 4. Make recommendations for combating identified problems.
- D.** The ICU D/Sergeant, along with unit/station commanding officers, shall directly brief the Chief of Police on emergent crime patterns or trends during the daily crime meeting and/or the weekly operational meetings.