City of Johns Creek Police Department

Subject:	Intelligence		*Number:* 02-39
Reference	See also "Special Investigations – Administration and Operations" and "Informant Management / Investigative Funds"		*Amends:*
Effective: *Revised:*	04/08 03/10 01/13 04/15	*Review Date:* Annually	*# of Pages:* 5

PURPOSE:

To provide guidelines for the collection, processing maintenance, and sharing of suspicious incidents and criminal intelligence relating to individuals or organizations involved in criminal and homeland security activities that present a threat to the community.

POLICY: (02-39)

It is the policy of the Johns Creek Police Department to only collect and maintain intelligence containing information limited to individuals or members of and/or organizations involved in criminal conduct and as it relates to activities that present a threat to the community. In addition, all employees of this department share in the responsibility for collection, processing and sharing of suspicious incidents and criminal intelligence relating to criminal and homeland security activities. The collection/submission, access, storage, and dissemination of criminal intelligence information must respect the privacy and constitutional rights of individuals, groups, and organizations.

DEFINITIONS:

Intelligence Information: Information relating to specific crimes and criminal activities. Typical examples of areas of concern are organized crime, vice, illegal drug trafficking, terrorism, gangs, intelligence which may have an impact on the safety and well-being of the community and civil disorders. It is not information collected for political or other purposes unrelated to crime.

Homeland Security: The department's local contribution to a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur. It also refers to the department's role in responding to other hazards to the community resulting from adverse weather conditions, health emergencies or other unusual incidents.

Right to Know: Legality of disclosure/failure to disclose intelligence data. Right to know exists only when (1) state or federal statutes mandate release to the person requesting such data, or (2) mandated by judicial action, specifically by subpoena.

PROCEDURES:

Operations and Administration (2-39-01)

1. The functions of intelligence information collection, processing, and dissemination is the responsibility of the Operations Manager under the Office of the Chief. The Intelligence Officer works closely with the Community Response Team and Criminal Investigations Division and may delegate his/her responsibility to other units or employees, if applicable.

    a. During the course of a day, any employee of the department may be exposed to information regarding criminal activities or terrorism threats within and outside of the jurisdiction. Such information may only be a small part of the bigger whole and may seem insignificant on its face. The information, however, should be recorded in an appropriate manner and forwarded through their chain of command to the Criminal Investigations Division Commander or his designee.

        (1) Employees will receive periodic training on criminal intelligence process, their role in criminal intelligence and the sharing of information.

    b. Such information regarding immediate future or planned criminal activities should be reported to the criminal intelligence unit and/or shift commander or other superior officer as soon as possible.

    c. Employees are encouraged to use the field contacts module in the records management system or submit a

miscellaneous report to document information and submit criminal intelligence information.

2. Intelligence information collected by department employees shall be channeled through the criminal intelligence unit before processing or disseminating to ensure information collected is limited to criminal conduct or relates to activities that present a potential threat to the community.

    a. Information submitted will be analyzed for relationships with other intelligence data and when relationships are shown, the proper law enforcement officer/agency will be advised of the information.

    b. Charts and graphs may be used to show flow and relationships when practicable.

    c. Once the criminal intelligence has been vetted the criminal intelligence officer will document the intelligence information in the records management intelligence activity module. The information shall be assigned to the community response team, CID or uniform patrol or forwarded to proper law enforcement jurisdiction

Type and Quality of Information (02-39-02)

1. Intelligence files may be established for persons, vehicles, organizations, and events. Files should include all available information that pertains to criminal and/or homeland security activities.

2. All information submitted to the intelligence files must be rated according to the source of the information and reliability of the information. This also includes information received via the confidential tip line for both email and voice recordings.

3. Information retained in the criminal intelligence files, which include homeland security activities, shall be evaluated for source reliability and content validity.

The following terms and guidelines are used:

Source Reliability

1. Reliable - The reliability of the source is unquestioned or has been well tested in the past.
2. Usually Reliable - The reliability of the source can usually be relied upon as factual. The majority of information provided in the past has proved to be reliable.
3. Unreliable - The reliability of the source has been determined unreliable or sporadic in the past.
4. Unknown - The reliability of the source cannot be judged. The

authenticity or trustworthiness has not yet been determined by either experience or investigation.

Content Validity

1. Confirmed - The information has been corroborated through sources and or verified by investigation.
2. Probable - The information is consistent with past accounts.
3. Doubtful - The information is inconsistent with past accounts.
4. Cannot be judged, not evaluated.

4. When relationships are seen among files, reports, etc. copies will be made and cross-reference to the related file.

Dissemination and Utilization of Collected Intelligence (02-39-03)

1. Intelligence information collected by department employees shall be regarded as sensitive and maintained as such. It should not be shared with members of the news media or other persons not associated with law enforcement unless approved by the criminal intelligence unit or Chief of Police or his/her designee. The collection/submission, access, storage, and dissemination of criminal intelligence information must respect the privacy and constitutional rights of individuals, groups, and organizations.

2. Information shall be disseminated only to law enforcement officers on a need-to-know basis.

   a. Inter-Departmental Intelligence Exchange

   Pertinent information shall be disseminated to the appropriate operational units of the department. This may be done verbally, by memorandum, intelligence bulletin and/or e-mail and any dissemination shall be documented as stated in this policy. Operational units are encouraged to provide feed-back to the intelligence component on the utility of information received.

   When an arrest is made as a result of intelligence provided by department members, the officer providing the information shall be notified.

3. All disseminations shall be recorded by disseminating an intelligence bulletin or documenting an activity in the intelligence management module giving at a minimum the following information:

   a. Name of law enforcement officer to whom dissemination was made.

b. Data of dissemination.
c. Purpose of dissemination.

5. Equipment

   a. Certain equipment is necessary to conduct intelligence operations.
   b. Necessary equipment should be readily available to those who are in need of such equipment.
   c. To prevent unauthorized use and loss of the surveillance and undercover equipment, the distribution and use of the equipment shall be approved by a Criminal Investigations Division Supervisor or the Community Response Team.
   d. All equipment shall be used within legal guidelines.
   e. It shall be the responsibility of officers using the equipment to attain an understanding of the operation of any equipment used.

6. Investigative funds shall be handled as outlined in Policy 02-42 "Informant Management / Investigative Funds"

Liaison with Other Agencies (02-39-04)

1. The criminal intelligence unit shall be primarily responsible for maintaining liaison with federal, state, and other local law enforcement agencies for the purpose of sharing intelligence.
2. Membership in intelligence organizations shall be assigned as needed by the criminal intelligence unit or designated representatives of the department.

Maintenance and Security (02-39-05)

1. [redacted]

2. A review of the files should be conducted periodically so as to remain current. Information which is determined to be outdated, unreliable to the extent of providing nothing actionable, will be destroyed in such a manner so as to prevent its recollection and distribution by unauthorized persons.

These methods could include permanent purging, burning and/or shredding. All destruction of Intelligence files will be under the personal direction of the Criminal Intelligence Unit.

(a) A database system will be maintained with a notation of the type and date the file was purged.

3. On an annual basis, a review of the procedures and processes associated with criminal intelligence will be conducted by the Operations Manager/Criminal Intelligence Unit or his/her designee.

42.1
42.1.5
42.1.6
43.1