Alagood, Robert Kyle

From: Price, Michael
Sent: Thursday, April 05, 2012 2:32 PM
To: Patel, Faiza; Goitein, Elizabeth; Michael Eggenberger; jeramie.scott@nyu.edu; Alagood, Robert Kyle; Levinson-Waldman, Rachel
Subject: FW: Policies of the Minneapolis Police Department's Strategic Information Center
Attachments: SIC Policy.doc

More from Sgt. Palmer at the Minneapolis Police Dept. – see attached for the policies and procedures governing intelligence collection by MPD's "Strategic Information Center." Sgt. Palmer also left a voicemail to follow up on the email, saying that he "thinks the policies comply with federal and state law." I actually agree. He also said he would continue to look for the other items we requested.

Best FOI experience ever!

Michael, could you take a look and let me know how SIC ties into the Minneapolis fusion center? There's a section on information dissemination, and it would seem like the Strategic Information Commander has to sign off on the release of information to other entities, but no mention of the fusion center.

Thanks,

Mike

Michael Price
Counsel, Liberty & National Security Program
Brennan Center for Justice
161 Avenue of the Americas, 12th Floor
New York, NY 10013
(646) 292-8335
michael.price@nyu.edu

From: Palmer, William [mailto:William.Palmer@minneapolismn.gov]
Sent: Thursday, April 05, 2012 11:49 AM
To: Price, Michael
Subject: FW: Policies of the Minneapolis Police Department's Strategic Information Center

Sgt. William J. Palmer
Minneapolis Police Department
Public Information Officer
350 South 5th Street Room 130
Minneapolis, Mn 55415
direct 612-673-2896 cell 612-919-9362 fax 612-673-2613
william.palmer@ci.minneapolis.mn.us

@MPD_PIO_Palmer

Here are policies that dictate what our "intelligence" function is and IS NOT permitted to do. We have made every effort to comply with both Federal and State law along with applicable case law.

-----Original Message-----
From: Rugel, Jeff
Sent: Wednesday, April 04, 2012 14:40
To: Palmer, William; Huffman, Amelia; Harris, Donald
Cc: Allen, Robert D.
Subject: RE: DP

Attached is the SIC policy. We do not collect intelligence information on political or religious groups or their members absent criminal activity.

Lt. Jeff Rugel

-----Original Message-----
From: Palmer, William
Sent: Wednesday, April 04, 2012 11:24
To: Huffman, Amelia; Rugel, Jeff; Harris, Donald
Subject: FW: DP

Captain and Lt's.
We have received the attached request for data. It stems, I am sure, from the activities of the NYPD that came to light recently.

As far as our community outreach is concerned I think that the efforts of Officer Brudenell should be shown whenever possible even if that is not directly what is being requested. If there are other ways to showcase the Community Engagement Team as a model for others that would be greatly helpful Lt. Harris.

I have absolutely no knowledge that the types of investigations being alluded to in this request reflect anything that the MPD has been involved with but we have to show this in any way we can. It is difficult to prove the negative.

As far as the intelligence gathering that is done I will have to rely on Lt. Rugel to provide what information can be released in general terms based upon the agreements that exist (if any) regarding fusion centers etc.

Captain Huffman, if there is something obvious that I am missing please let me know.

Sgt. William J. Palmer
Minneapolis Police Department
Public Information Officer
350 South 5th Street Room 130
Minneapolis, Mn 55415
direct 612-673-2896 cell 612-919-9362 fax 612-673-2613 william.palmer@ci.minneapolis.mn.us

@MPD_PIO_Palmer

-----Original Message-----
From: Meyers, Linda
Sent: Wednesday, April 04, 2012 10:39
To: Palmer, William
Subject: DP

Hi Bill,

Attached is a lengthy request that I need guidance on how to process. Way over my head!

Thanks!

Linda

STRATEGIC INFORMATION CENTER
POLICY & PROCEDURE

Section 1 Introduction

1. Purpose

A. To establish internal controls and proper oversight for the collection, retention, dissemination, and disposition of criminal information in conformance with state and federal law while protecting the constitutional rights of individuals, groups, associations, or other legal entities.

2. Objectives

A. Provide liaison, coordination, and resource assistance in the collection, storage, exchange, dissemination, and analysis of criminal intelligence in active investigations and/or prosecution activities.
B. Provide criminal intelligence to law enforcement and criminal justice agency personnel on individuals and organizations involved with criminal organizations and enterprises.
C. Provide analysis of organized crime including identification and/or projection of major changes in crime trends or patterns.

3. Policy

A. The collection, retention, dissemination, and disposition of confidential criminal intelligence data is one of the essential functions of law enforcement. All Minneapolis Police Department employees shall adhere to guidelines established in this section to ensure, confidentiality, and proper dissemination of criminal intelligence. Criminal intelligence shall not be collected or retained except as specified in this policy.
B. This policy is based on careful review and consideration of:
C. Title 28 Code of Federal Regulations Part 23- Criminal Intelligence Systems Operating Policies
D. Law Enforcement Intelligence Unit (LEIU) model policy and procedures
E. International Chief of Police Intelligence model policy and procedure
F. Best practices of Intelligence Unit policies from multiple law enforcement agencies.
G. Minnesota State Data Practice Laws

Section 2 Procedures for Managing Criminal Intelligence

1. Organization

A. Primary responsibility for the direction of intelligence operations; coordination of personnel; and collection, evaluation, collation, analysis, and dissemination of intelligence is housed within the Strategic Information Center (SIC) under direction of the SIC Commander.
B. The SIC supervisors shall report directly to the SIC Commander or his/her designate in a manner and on a schedule prescribed by the SIC Commander.
C. To accomplish the goals of the intelligence function and conduct routine operations in an efficient and effective manner, the SIC supervisors shall ensure compliance with the policies, procedures, mission, and goals of the agency.
D. Criminal intelligence data shall be reviewed by the SIC supervisors for validation prior to entry into any criminal intelligence file.

2. Professional Standards

A. The intelligence function is often confronted with the need to balance information-gathering requirements for law enforcement with the rights of individuals. To this end, members of this agency shall adhere to the following:
B. Information gathering for intelligence purpose shall be premised on circumstances that provide a reasonable suspicion (as defined in 28 CFR, Part 23, and Section 23.3 c) that specific individuals or organizations may be planning or engaging in criminal activity.
C. Investigation techniques employed shall be lawful and only so intrusive as to gather sufficient information to prevent criminal conduct or the planning of criminal conduct.
D. The intelligence function shall make every effort to ensure that information added to the criminal intelligence database is relevant to a current or on-going investigation and the product of dependable and trustworthy sources of information. A record shall be kept of the source of all information received and maintained by the intelligence function.
E. Criminal intelligence information shall not be collected or maintained 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 reasonable suspicion that the subject or the information is or may be involved in criminal conduct or activity.
F. Information gathered and maintained by the division for intelligence purpose may be disseminated only on a "need to know" and "right to know" basis.

3. Excluded Material

A. Only lawfully collected information based on reasonable suspicion of criminal activity and which meets the units file input should be stored in the criminal intelligence file. Specifically excluded material includes:
B. Information on an individual or group merely on the basis that such individual group support unpopular causes.

C. Information on an individual or group merely on the basis of race, gender, age, or ethnic background.
D. information on an individual or group merely on the basis of religious or political affiliations, or beliefs
E. Information on an individual or group merely on the basis of personal habits and/or predilections that do not break any laws or threatens the safety of others.
F. Information obtained in violation of any applicable federal, state, or local rules, statutes or ordinances.

4. File Status

A. All information retained in the criminal intelligence files will meet the criteria prescribed by this policy and managed by the SIC supervisors.
B. The SIC file system shall adhere to federal and state laws and all Minneapolis Police Polices related to content, dissemination, and retention policies.
C. A yearly audit shall be conducted by the SIC supervisors of the filing system.

Section 3 Types Of Files

1. Permanent Intelligence Files:

A. Criminal intelligence may be retained in the permanent intelligence files for up to five (5) years.
B. After 5 yrs criminal intelligence will be automatically deleted unless new criminal intelligence has been developed revalidating ongoing criminal activities of that individual and /or organization.
C. When updated criminal intelligence is added into the permanent files on a suspect individual or organization already listed in the database, such entries revalidate the reasonable suspicion and reset the five year standard for retention of that file.

2. Temporary Intelligence Files:

A. Criminal information may also be entered into intelligence files on a temporary basis when there is reasonable suspicion or criminal activity, but more information may still need to be developed to fully expand a criminal investigation.
B. Temporary intelligence files should be retained no longer than one (1) year. At this time, temporary files must be either purged or converted into permanent intelligence files
C. Temporary files may be entered into the system when:

    1. Subject / Entity is unidentifiable- Subject (although suspected of being engaged in criminal activities) has no known physical descriptors, identification numbers, or distinguishing characteristics available.

2. Involvement is questionable- involvement in criminal activities is suspected by a subject / entity which has either:
3. Possible criminal associations
4. Criminal history- individuals, organization, business, or group that has a history of criminal conduct, and the circumstances currently being reported indicates they may again become criminally active.
5. Reliability /Validity Unknown- the reliability of the information sources and/or the validity of the information can not be determined at the time of receipt; however, the information appears to be significant and merits temporary storage while verifications attempts are made.

Section 4 Filing System

1. Intelligence Files

A. Intelligence files are files on persons or organizations believed to be involved in criminal activity.
B. File Numbering: All files shall be numbered sequentially in the order they are created.
C. File numbers associated with intelligence files that are purged in accordance with section 7 of this policy shall not be re-used.

2. Analytical Files

A. Analytical files are the result of an intelligence analyst linking persons, locations, and/or events related to a crime or series of crimes.
B. Analytical files containing information to be disseminated to MPD personnel may be published through the Daily Intelligence Bulletin where they will be filed for one year. Analytical files containing information about a known person or persons may be added to the individual intelligence files for long term storage.

3. Electronic Storage & Security

A. Criminal intelligence files and analytical files will be secured in electronic files that are equipped with security protection measures. Only persons authorized by the SIC Commander may have access to the files. Those files and database will be secured during off-hours and when the office is vacant.

Section 5 Classification of Intelligence

1. Classification Of All Files

A. Intelligence files will be classified in order to protect sources, investigations, and individual's rights to privacy, as well as to provide a structure that will enable this agency to control access to intelligence. The classification of any file shall be reevaluated whenever new information is added to an existing intelligence file.

2. Source Reliability

A. The reliability of the source is an index of the consistency of the information the source provides. The sources shall be evaluated according to the following:

- **Reliable-** the reliability of the source is unquestioned or has been tested in the past. *All law enforcement agencies are classified as completely reliable*
- **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.
- **Unreliable-** the reliability of the sources has been sporadic in the past
- **Unknown-** the reliability of the source cannot be judged; either experience or investigation has not yet determined authenticity or trustworthiness

2. Content Validity

A. 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:

- **Confirmed-** the information has been corroborated by an investigator or another reliable independent source
- **Probable-** the information is consistent with past accounts
- **Doubtful-** the information is inconsistent with past accounts.
- **Cannot be judged-** the information cannot be judged. Its authenticity has not been determined by either experience or investigation.

3. Sensitivity

A. SIC personnel must adhere to two types of sensitivity classifications since the SIC is in contact with federal, state, and local documentation and data.
B. Sensitivity classifications are tied to the handling, dissemination, and release of materials and products.
C. Federal governments' and other states' classifications are different then what is required by Minnesota state laws.
D. SIC Personnel must adhere to federal classification guidelines when dealing with federal intelligence.

1. Federal Classifications

- **Classified (not public):** Documents are restricted to individuals who have a security clearance of secret or higher.

- **Unclassified/LES (not public):** Documents are viewable by law enforcement agencies only with the "right to know" and "need to know". It may contain information related to sources, methods, evidence, and active investigations.
- **Unclassified/FOUO (not public)**: Documents are viewable by anyone who is authorized to view documents under "Official Use Only" status. Usually falls under the "right to know" and "need to know" basis. Not for dissemination or view by the general public or media.

2. Minnesota Classifications

Minnesota Data Practice Act creates the presumption that unless otherwise provided by law, all government data are public. All data is controlled by the law at the time of the request, regardless of the law when the data were collected or created. The following are the Minnesota Data classifications

- **Private:** Data identifying an individual that are only available to the individual or with the individual's consent (Minn. Stat. § 13.02, subd.12)
- **Confidential:** Data identifying an individual that are not available to anyone outside the entity holding the data, including the individual (Minn. Stat. § 13.02, subd. 3). SIC personnel will share confidential data with the entities with the statutory authority to receive.
- **Nonpublic:** data on a business or other entity that is only available to the subject of the data or with the subject's informed consent (Minn. Stat. § 13.02, subd. 9).
- **Protected nonpublic:** Data on a business or other entity that are not available to the subject of the data or anyone else outside the entity holding the data (Minn. Stat. § 13.02, subd. 13)

Section 6 Dissemination

1. Dissemination Of Intelligence

A. Criminal intelligence shall not be released to the news media or general public without prior approval from the SIC Commander or his/her designee.
B. Primary responsibility for the dissemination of all SIC reports, assessments, and briefs shall rest with the SIC supervisors.
C. Criminal intelligence may only be shared with other law enforcement agencies with the approval of SIC supervisor or commander. The release of this information shall be based on a "need to know" and "right to know" basis.
D. Dissemination of criminal intelligence shall meet all federal, state and local laws.
E, SIC personnel shall not release any original intelligence documents. Information can be released verbally, request may be view onsite, or a copy of the document may be made for dissemination.
F. Release of intelligence in general and electronic surveillance information and photographic intelligence, in particular, to any authorized law enforcement agency shall be made only with the approval of the SIC supervisor and with the stipulation that such intelligence not be duplicated or otherwise disseminated without the approval of the SIC supervisor.

G. All files released under freedom of information provisions and through disclosure shall be carefully reviewed.
H. Informant files shall be maintained separately from intelligence files.
I. All request for information related to data practices shall be forwarded to the department Public Information Officer (PIO) office for approval and review of data practice policies.
J. All media request for information shall be forwarded to the SIC commander for referral to the department PIO.

Section 7 Audit and Purging Of Files

1. Audit & Purging

A. The SIC commander is responsible for ensuring that files are maintained in accordance to federal and state law.
B. Reviewing and purging of intelligence files will be done on an on-going basis, but at a minimum will be accomplished annually. The maximum retention period is five (5) years; if at that time the information has not been updated and/or revalidated it must be removed from the system. The department may update and/or revalidate the submission and extend the retention period at any time, based on reasonable suspicion of new criminal activity.
C. The decision to purge information should be guided by the following considerations:
    - The number of request for the file/individual
    - The validity of the information
    - The reliability of the information
    - Federal /State Law
    - Defined retention periods for permanent and temporary files
    - Public Safety and/or officer safety
    - Any information that is found to be inaccurate, misleading, obsolete, or otherwise unreliable will be purged.
D. A record of all purged file numbers without personally identifiable data shall be maintained.