Rahm Emanuel
Mayor

Department of Police · City of Chicago
3510 S. Michigan Avenue · Chicago, Illinois 60653

Garry F. McCarthy
Superintendent of Police

April 11, 2012

Brennan Center for Justice
Attn: Michael Price
161 Avenue of the Americas, 12th Floor
New York, NY 10013

Re: NOTICE OF RESPONSE TO FOIA REQUEST
REQUEST DATE: March 29, 2012
FOIA FILE NO.: 12-1086

Dear Mr. Brennan:

The Chicago Police Department is in receipt of your multi-part FOIA request which seeks information related to the Department's polices and procedures as they relate to counterterrorism investigations and operations, as well as community outreach activities, the Department's participation in community outreach activities with the "MASA" (Muslim, Arab, or South Asian) communities, and policies and procedures relating to any type of "community mapping" program.

Initially, it must be pointed out that the language used in your request is quite broad. As a result, the responsive records could potentially include a myriad of documents or other categories of records. In order to fully comply with your request, the Department would have to perform a virtually unlimited search of Department records. In an attempt to comply with your request, without undertaking a search that would unduly burden the operations of the Department, the Department has located the enclosed the records (First Amendment Worksheet; General Orders related to 1st Amendment Investigations, Chicago Alternative Policing Strategy (CAPS), Racial Profiling and other Bias Based Policing, and Video Surveillance; Department Special Orders related to 1st Amendment Investigations, CAPS, and Anti-Terrorism Preparations; Department Uniform and Property Order related to the Observation Van; Intelligence Section Special Orders related to investigations; and the Crime Prevention and Information Center (CPIC) Privacy Policy) which may be responsive to your request. If after reviewing the enclosed records you wish to make a more specific records request, please contact me. The Department's directives can be located and searched at following, http://directives.chicagopolice.org/directives/.

Next, the Department has located responsive records that can be released with certain information redacted. These records, which are emails between the Director of News Affairs for the Chicago Police Department and a representative of CAIR (Council on American-Islamic Relations), contain private information and other identifying information that is exempt from disclosure under the following exemption found in the Illinois Freedom of Information Act:

> 5 ILCS 140/7 (1)(b) Private information, unless disclosure is required by another provision of this Act, a State or federal law or a court order;

Finally, the Department has located responsive records that are exempt from disclosure under Section 5 ILCS 140/7(1)(f) of the Illinois Freedom of Information Act. Section 5 ILCS 140/7 (1)(f) states "preliminary drafts,

notes, recommendations, memoranda and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of a record shall not be exempt when the record is publicly cited and identified by the head of the public body."

To be clear, the exempt records are preliminary intra-agency drafts which contain the formulation of Department policies and actions as they relate to the gathering of intelligence. Additionally, in Harwood v. McDonough, 344 Ill. App. 3d 242 (1st Dist. 2003), the Illinois Appellate Court held that "as a matter of public policy, section 7(1)(f) exempts from disclosure predecisional materials used by a public body in its deliberative process." Id. at 247. The court further noted that "preliminary" does not refer to the "posture of the particular document sought to be disclosed" but rather to "predecisional intra-agency communications." Id. at 247-248. The documents CPD wishes to withhold have not been publicly cited and identified by the head of the public body.

In closing, as was agreed today, the Department will provide you with an updated First Amendment General Order once it is available.

If I can be of further assistance, you may contact me at (312)745-5308, or by mail at the below address:

Chicago Police Department
Attention: Freedom of Information Officer
Records Inquiry Section, Unit 163
3510 S. Michigan Ave., Rm. 1027SE
Chicago, IL 60653

Sincerely,

P.O. O'Brien #7818
Freedom of Information Officer
Department of Police

To the extent that you consider this a denial, you have a right of review by the Illinois Attorney General's Public Access Counselor (PAC). You can file a request for review by writing to:

Public Access Counselor
Office of the Attorney General
500 S. 2nd Street
Springfield, Illinois 62706
Phone: 312-814-5526 or 1-877-299-FOIA (1-877-299-3642)
Fax: 217-782-1396 E-mail: publicaccess@atg.state.il.us

If you choose to file a Request for Review with the PAC, you must do so within 60 calendar days of the date of this denial letter. 5ILCS 140/9.5(a). When filing a Request for Review, you must include a copy of the original FOIA request and this denial letter. You may also seek judicial review of a denial under 5 ILCS 140/11.

FIRST AMENDMENT WORKSHEET

Chicago Police Department

Date and Time of Request	
First Amendment Invest. Tracking No.	

To: **Superintendent of Police**
Attention: General Counsel

From: **District Commander/ Unit Commanding Officer of Exempt Rank:** _____
Name and star number

☐ Initial Authorization to Conduct
☐ Authorization to Continue
☐ **Order to Terminate/Disapproval Of**

} a First Amendment investigation relating to:

☐ Intelligence Gathering
☐ Public Gathering

Investigation Initiated: (Date) _____ (Time) _____ Date Authorization Expires: _____

FACTUAL BASIS FOR INVESTIGATION - For authorization to initiate or continue an investigation, indicate how the investigation will serve/ continue to serve a proper law enforcement purpose and source of information relied upon to justify the investigation; for termination of an investigation or disapproval of an initiation request, indicate rationale for that determination :

☐ See Attached Continuation Sheet

Indicate Investigative Techniques and Minimization Procedures to be used :

☐ See Attached Continuation Sheet

☐ Request authorization to use Level II Investigative Techniques (electronic surveillance, undercover methods) based on the following justification:

☐ See Attached Continuation Sheet

PERSONS OR GROUPS TO BE INVESTIGATED

Name	Address	Affiliation, if Any	I.R. No.

Signature of District Commander/Unit Commanding Officer of Exempt Rank	Signature of General Counsel	Date	General Counsel's Determination:
			Concur ☐ Do Not Concur ☐

CPD-11.440 (Rev. 10/03)

Chicago Police Department

General Order G02-01

HUMAN RIGHTS AND HUMAN RESOURCES

ISSUE DATE:	03 July 1992	**EFFECTIVE DATE:**	04 July 1992
RESCINDS:	G92-01		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. sets forth Department policy, procedures and guidelines governing the human rights of all individuals;

B. defines the responsibilities of Department members concerning applicable laws; and

C. provides information on City, State and Federal resources.

D. identifies select Federal and State law relative to human rights.

Department members will refer to the Special Order titled "**Human Rights and Human Resources**" for procedures and guidelines governing the human rights of all individuals.

II. GENERAL INFORMATION

A. As one of the world's largest cities, Chicago encompasses a variety of communities, each with its own distinctive cultures, lifestyles, customs and problems. The cosmopolitan nature of the City is further manifested by the diverse ethnic and sociological background of its people. However, all persons in each area of the City share the common need for protection and service through objective and impartial law enforcement.

B. The recognition of individual dignity is vital in a free society. Since all persons are subject to the law, all persons have the right to dignified treatment under the law. The protection of this right is a fundamental responsibility of the Department and its members. Every Department member is responsible for treating each person with respect, mindful that the person possesses human emotions and needs.

C. The daily interaction of Department members with citizens presents a unique opportunity to strengthen police-community relations. In all contacts with the public, members must inspire respect for themselves as individuals and as representatives of the Department by respecting the human rights of the members of the community.

III. POLICY

A. The Chicago Police Department is committed to observing, upholding and enforcing all laws relating to individual rights. Department members will respect and protect each person's human rights and comply with all laws relating to human rights.

B. In addition to respect for those human rights prescribed by law, Department members will treat all persons with the courtesy and dignity which is inherently due every person as a human being. Department members will act, speak and conduct themselves in a professional manner, recognizing their obligation to safeguard life and property, and maintain a courteous, professional attitude in all contacts with the public.

C. Members will not exhibit any bias or prejudice against an individual or group because of race, color, gender, age, religion, disability, national origin, ancestry, sexual orientation, marital status, parental status, military discharge status, or source of income. Members will not exhibit a condescending attitude or direct any derogatory terms toward any person in any manner.

D. The Chicago Police Department is committed to working with the communities of the City to serve and protect; to safeguard lives and property; to guarantee all persons fair and equal treatment under the law; and to ensure that all persons may enjoy their fundamental rights as human beings.

IV. INDIVIDUAL RIGHTS AND THE LAW

A. The Fourth Amendment to the Constitution of the United States guarantees protection from unlawful arrest and unreasonable search and seizure to all persons in this country.

B. Under the United States Code, it is unlawful for any person who is acting under color of any law, statute, ordinance, regulation or custom to willfully subject any inhabitant of any state, territory or district to the deprivation of any rights, privileges or immunities secured or protected by the Constitution or laws of the United States to different punishments, pains or penalties on account of such inhabitant being an alien or by reasons of his color or race. Violators can be subjected to a fine and/or imprisoned for a term of years or for life (Title 18, United States Code Annotated, Section 242).

C. Along with the criminal sanctions mentioned in Item II-B, violators can be liable to the party injured in civil proceedings (Title 42, Untied States Code Annotated, Section 1983).

D. The Americans with Disabilities Act provides a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities, and provides enforceable standards addressing discrimination against individuals with disabilities. (Public Law 101 - 336, Section 2 (b)).

E. The Illinois Human Rights Act secures for all individuals within Illinois the freedom from discrimination because of race, color, religion, sex, national origin, ancestry, age, marital status, physical or mental handicap, or unfavorable discharge from military service in connection with employments, real estate transactions, access to financial credit, and the availability of public accommodations; and prevents unlawful discrimination or sexual harassment in employment, discrimination in connection with real estate transaction based upon familial status, and sexual harassment in higher education. (Illinois Revised Statutes, Chapter 68-1-102).

V. RELEVANT ORDINANCE

A. "Declaration of city policy" (Municipal Code of Chicago, Section 2-160-010).

B. "Definitions" (Municipal Code of Chicago, Section 2-160-020).

C. "Unlawful discriminatory activities designated" (Municipal Code of Chicago, Section 2-160-030).

D. "Sexual harassment" (Municipal Code of Chicago, Section 2-160-040).

E. "Religious beliefs and practices" (Municipal Code of Chicago, Section 2-160-050).

F. "Discriminatory practices-Credit transactions" (Municipal Code of Chicago, Section 2-160-060).

G. "Discriminatory practices-Public accommodations" (Municipal Code of Chicago, Section 2-160-070).

H. "Exemptions for certain religious organizations" (Municipal Code of Chicago, Section 2-160-080).

I. "Violation-Investigation by Commission on Human Relations-Prosecution" (Municipal Code of Chicago, Section 2-160-090).

J. "Retaliation prohibited" (Municipal Code of Chicago, Section 2-160-100).

K. "Construction of chapter provisions" (Municipal Code of Chicago, Section 2-160-110).

L. "Violation-Penalty" (Municipal Code of Chicago, Section 2-160-120).

VI. LIMITED ENGLISH PROFICIENCY POLICY

A. The Chicago Police Department will provide professional and courteous police service to all persons, equally and without prejudice and will take reasonable steps to provide service to all individuals encountered regardless of their ability to speak, read, write, or understand English.

B. Individuals with Limited English Proficiency (LEP) requiring a Department/police service will be provided interpretation services by the Department free of charge to ensure proper communication

exists throughout the duration of the incident. Department members will refer to the Special Order entitled "**Limited English Proficiency**" for information regarding specific procedures.

Matt L. Rodriguez
Superintendent of Police

91-071 WHB, SAM, JVD, RM, JAB, MU (mmd)

GLOSSARY TERMS:

1. **Limited English Proficiency (LEP)**

   Designates an individual whose primary language is not English and who may have a limited ability to read, write, speak, or understand English. LEP designations are context specific and individuals may have sufficient English proficiency to function in certain types of communication (e.g., speaking, understanding) but lack the skills to function in other situations (e.g., reading, writing).

2. **Interpretation**

   The act of listening to or reading a communication in one language and orally converting it to another language while retaining the same meaning.

ADDENDA:

1. G02-01-01 - Criminal Investigations of Drug or Alcohol Abuse Patients
2. G02-01-02 - Testing for HIV Status, Disclosure of HIV Status, Discrimination Against Individuals Based on HIV Status

Chicago Police Department

General Order G02-02

THE FIRST AMENDMENT AND POLICE ACTIONS

ISSUE DATE:	11 October 2002	**EFFECTIVE DATE:**	25 October 2002
RESCINDS:	G02-10		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. states Department policy relating to citizens engaged in First Amendment conduct.

B. states Department policy relating to First Amendment-related investigations.

C. establishes responsibilities and procedures relative to all police action and investigations which may affect conduct protected by the First Amendment, including First Amendment-related intelligence.

D. informs members that the consent decree regarding First Amendment investigations entered into in 1982 by the City of Chicago has been wholly superseded by a modified consent decree [Alliance to End Repression v. City of Chicago, 237 F.3d 799 (7th Cir. 2001)] and is included in this directive as Attachment No. 1.

E. reestablishes the consent decree entered in case 76 C 1982 relating to attorney-client relationships. The text of this judgment order is included as Attachment No. 2.

F. reestablishes the consent decree entered in case 88 C 5434 relating to the protection of persons' First Amendment rights in the presence of a hostile audience. The text of this judgment order is included as Attachment No. 3.

Department members will refer to the Special Order titled "**The First Amendment and Police Actions**" for procedures relative to police actions and investigations.

II. POLICY

It is the policy of the Chicago Police Department to conduct all investigations for a proper law enforcement purpose. Each and every investigation must safeguard the constitutional liberties of all persons. Police conduct which may affect the exercise of First Amendment rights will be conducted in accordance with this directive and the modified consent decree which is included as Attachment No. 1. Pursuant to the modified consent decree, Department members may not investigate, prosecute, disrupt, interfere with, harass, or discriminate against any person engaged in First Amendment conduct for the purpose of punishing, retaliating, or preventing the person from exercising his or her First Amendment rights.

III. UNITED STATES CONSTITUTION

A. The First Amendment

1. "Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances."

2. First Amendment conduct means speech or activity related to the freedom of speech, free exercise of religion, freedom of the press, the right to assemble, and the right to petition the government. The First Amendment protects, but is not limited to, the following rights:

   a. The right to hold ideas or beliefs concerning public or social policy, or political, educational, cultural, economic, philosophical or religious matters;

b. The right to communicate or receive such ideas or beliefs, publicly or privately, orally, in writing or by symbolic means;

c. The right to associate and assemble publicly or privately with other persons concerning ideas or beliefs about public or social policy, or political, educational, cultural, economic, philosophical or religious matters (but not a right to associate or assemble for purposes unrelated to the right to hold and express such ideas or beliefs);

d. The right to advocate ideas or beliefs, including the right to advocate an alternative system of government and to advocate "the use of force or of law violation, except where such advocacy is directed to inciting or producing imminent lawless conduct and is likely to incite or produce such action";

e. The right to petition the government or governmental officials for redress of grievances;

f. The right to associate for the purpose of seeking and giving legal advice as well as advancing litigation.

3. First Amendment rights exercised in public forums may be subject to content-neutral time, place, and manner regulations that support an appropriate governmental interest.

B. The Fourth Amendment

1. "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched and the persons or things to be seized."

2. What a person seeks to preserve as private, including oral communications, even in an area accessible to the public, may be constitutionally protected under the Fourth Amendment.

3. The Fourth Amendment protects against governmental intrusion not justified by an appropriate governmental interest.

IV. FIRST AMENDMENT RIGHTS UPON THE PUBLIC WAY

A. The public way generally includes public property held open to the public such as city parks, public streets, and sidewalks. The public way does not include privately-owned property, such as the United Center, and publicly-owned property not open to the public, such as the working area of a police facility.

B. Persons on the public way have a right to:

1. express their views through any form of communication, including distribution or sale of newspapers, magazines, handbills or other printed matter; and

2. solicit financial contributions.

C. The rights protected by the First Amendment and exercised on the public way are not absolute and are subject to time, place, and manner restrictions, as well as any and all other applicable laws.

For example: persons expressing views protected by the First Amendment on the public way are required to comply with laws prohibiting physical obstruction of the movement of persons and vehicles on the public way or place, and damage to public or private property.

D. Persons on the public way may freely distribute, without charge to others, material or messages containing First Amendment protected ideas.

NOTE: Generally, persons giving away items containing First Amendment protected messages are not considered peddlers or itinerant merchants and ordinances applicable to itinerant merchants and peddlers do not apply to persons freely distributing First Amendment protected messages. For example, campaign literature.

E. Speech Peddling: Persons Selling a Protected Message

1. Section 4-244-141 of the Municipal Code of Chicago (MCC) defines speech peddling as a licensed peddler who sells or exchanges for value anything containing words, printing, or pictures that predominantly communicate a non-commercial message. Generally, this means a message relating to political, religious, artistic, and/or other non-commercial ideas and the message is the primary purpose of the item being sold. For example, a person who sells or exchanges for value a T-shirt which reads "Legalize Marijuana", or bumper stickers reading "Stop the Death Penalty" are engaged in speech peddling.

2. Persons engaged in speech peddling are subject to geographic restrictions and permit requirements contained in the MCC. For example, no person shall be allowed to engage in speech peddling within the Central District without a speech peddling permit (4-244-141 (b) MCC).

V. ATTACHMENTS

A. Attachment No. 1

Alliance to End Repression v. City of Chicago, No. 74 C 3268
American Civil Liberties Union v. City of Chicago, No. 75 C 3295
MODIFIED CONSENT DECREE

B. Attachment No. 2

JUDGMENT ORDER CONCERNING ATTORNEY-CLIENT RELATIONSHIPS
CASE NO. 76 C 1982

C. Attachment No. 3

Nelson v. Streeter, et.al., No. 88 C 5434
JUDGMENT ORDER

Terry G. Hillard
Superintendent of Police

01-006 LMT(PMD)

ADDENDA:

1. G02-02-01 - Investigations Directed at First Amendment-Related Intelligence
2. G02-02-02 - Other Police Action which may Impact First Amendment Conduct

Attachment No. 1

Alliance to End Repression v. City of Chicago, No. 74 C 3268

American Civil Liberties Union v. City of Chicago, No. 75 C 3295

MODIFIED CONSENT DECREE

STATEMENT OF JURISDICTION

This court has jurisdiction over the parties to these consolidated cases and over the subject matter of these actions pursuant to 28 U.S.C. §1331 and 1343(3).

STATEMENT OF PRINCIPLES

1. The First Amendment of the United States Constitution protects the rights of every person to freedom of speech, press, assembly, petition, and religion, including, without limitation, the rights to hold, communicate and receive ideas and beliefs, to speak and dissent freely, to associate for the advancement of litigation, to write and publish, to advocate and organize concerning public policy and social issues and to associate publicly and privately with other persons concerning political and social issues. These rights are subject to reasonable time, place, and manner regulations supported by an appropriate governmental interest, and, with a few exceptions, conduct that is forbidden without reference to whether it is being used for expression may be forbidden even when used for the purpose of expression.

2. The Fourth Amendment of the United States Constitution protects the rights of every person to be secure in person, house, papers and effects against unreasonable searches and seizures, including the right to be secure in communications which are engaged in with a reasonable expectation of privacy. This Amendment protects the innocent and the guilty alike against government intrusion not justified by an appropriate governmental interest or function.

3. The Fourteenth Amendment guarantees to every person equal treatment under the law unless an appropriate governmental interest justifies a difference in treatment.

INJUNCTION

The City of Chicago, its officers, employees, and agents, and all persons in active concert or participation with them who receive actual notice of this Decree, are hereby enjoined as follows:

1. No agency or agent of the City of Chicago shall

a) investigate, prosecute, disrupt, interfere with, or harass any person for the purpose of punishing or retaliating against that person for engaging in conduct protected by the First Amendment, or for the purpose of preventing them from engaging in such conduct, although nothing in this Decree shall enjoin reasonable investigative or law enforcement activities that are permitted by the First Amendment;

b) discriminate against any person on the basis of their conduct protected by the First Amendment, except as may be permitted by law;

c) authorize, assist, or encourage any person to violate this Decree, or to commit an act that would violate this Decree if committed by a City agent.

2. All current employees of the City of Chicago, and all future employees at the time of their hiring, shall be served with a copy of this Decree.

3. In each of the next five years, the Superintendent of Police shall conduct a departmental audit of the Police Department's compliance with this Decree, and submit copies of the audit report to the Mayor, the Police Board, and this court for filing as a public record. The annual report shall include a summary of any internal disciplinary complaints concerning compliance with this Decree and the findings made and the actions taken on such complaints.

4. The Chicago Police Board shall review the Superintendent's audit annually, and may request such additional information as it deems necessary to monitor compliance with this Decree, and shall report to the Mayor, the Superintendent of Police, and the public concerning its findings.

5. The Chicago Police Board shall also cause an audit of the City's compliance with the terms of this Decree to be performed by a national independent public accounting firm within five years of the entry of the order adopting this modified Decree. The audit report shall contain a description and evaluation of any conduct believed by the auditors to constitute a probable violation of the Decree. The Police Board may require further investigation of any such possible violations. The audit report, together with any additional findings or recommendations made by the Board, the Superintendent of Police, or the Mayor shall be made public. For the purpose of these audits, or for any other investigation that the Board may wish to conduct to investigate compliance with this Decree, the Board and the auditors engaged by the Board shall have access to all relevant data in the possession of the City except that the auditors shall not have access to information specifically identifying confidential informants or to current criminal investigations that the Superintendent of Police states might be compromised by disclosure to the auditors. The auditors shall not disclose any

information to anyone but the Board, the Superintendent of Police, or (upon his request) the Mayor. The Board shall not disclose in any manner details that specifically identify any investigations except as otherwise permitted by law, nor shall it disclose in any manner information that would reveal the identity of a confidential informant, compromise an ongoing criminal, regulatory, or employee disciplinary investigation, or constitute an invasion of a person's privacy.

6. If the Board, the Superintendent of Police, or the head of any other City Department learns of any probable substantial violation of this Decree, the matter shall be promptly referred to the Superintendent of Police (or, if the matter involves personnel of a City agency other than the Police Department, to the Inspector General). The Superintendent of Police or the Inspector General, as the case may be, shall cause an investigation to be made and shall report to the Board, the Superintendent, and the head of the agency who made the report the results of the investigation. Where the result of the investigation supports the finding of a violation, the Superintendent or other agency head shall in turn report to the Board what corrective action has been taken, including what disciplinary proceedings have been instituted or completed.

RETENTION OF JURISDICTION

The court expressly retains jurisdiction to enable the parties to the Decree to apply to this court for the enforcement of compliance with the provisions contained herein, and for the punishment of any violation of such provisions. Application to enforce the provisions or to impose punishment for any such violation may be presented to the court by any person affected by the conduct complained of. Prior written notice of all such applications shall be given to counsel for the named parties to this action. Except where emergency relief is sought, seven days written notice shall be given.

TERM OF DECREE

Upon completion of the independent audit called for in this order, and its submission to the court, the court will consider whether further modification or dissolution of this Decree is warranted at that time.

END OF TEXT OF MODIFIED CONSENT DECREE

Attachment No. 2

JUDGMENT ORDER CONCERNING ATTORNEY-CLIENT RELATIONSHIPS

CASE NO. 76 C 1982

The plaintiff having filed its complaint, and the plaintiff and the defendants having consented to the entry of this agreed order, judgment, and decree as to such parties without trial or adjudication of any factual allegation in the complaint or any issue of fact with respect to the alleged commission by said defendants of any unconstitutional, unlawful, or wrongful act, and without this Judgment constituting evidence of or an admission by any defendant with respect to any issue of fact herein or the commission of any unconstitutional, unlawful, or wrongful act;

Plaintiff in its complaint alleges in part:

1. surveillance at meetings of the attorneys and other individuals employed by, or working under the auspices of, the plaintiff, and the compilation of reports listing all persons in attendance at these meetings and detailing the statements made during these meetings;

2. use of secret informers and undercover agents to attend and report on private meetings and discussions during which attorneys employed by or working under auspices of the plaintiffs were engaged in private and privileged discussions related to pending and potential litigations;

3. maintenance by the Chicago Police Department of files reporting on the activities of the plaintiff and its employees, agents, and cooperating attorneys, including reports on meetings attended by officers, agents or employees of plaintiff, and further including detailed summaries of confidential or privileged conversations relating to the planning, investigation, prosecution of potential and pending lawsuits in state and federal courts;

4. disseminating and making available, both to other law enforcement agencies and to individuals not involved with the functions of law enforcement, the information collected and maintained in the files of the Chicago Police Department relating to and reporting on the activities of the plaintiff;

5. all done with the improper purpose of interfering with the attorney-client relationship and with the intent of obtaining confidential and privileged information relating to pending and potential lawsuits;

Defendants deny the above five allegations of plaintiff's complaint. The parties however agree

that the public interest requires the observance of and respect for the attorney-client privileges;

NOW, THEREFORE, this court having jurisdiction of the parties to this Agreed Order, Judgment and Decree and the subject matter of these actions under sections 1331 and 1343 (3) of Title 28 of the United States Code; and upon consent of the parties and approval of the court, it is hereby ORDERED, ADJUDGED AND DECREED as follow:

The City of Chicago, the individual defendants, their officers, employees, and agents, and all persons in active concert or participation with them [hereinafter referred to as defendants], are hereby permanently enjoined as follows:

I. PROHIBITED ACTIVITY.

A. Defendants shall not conduct surveillance at, gather information or compile reports on, or maintain files or records regarding, meetings or communications, if--

1. as to the meeting or communication, there is a reasonable expectation of privacy and that the attorney-client privilege will attach; and

2. the meeting or communication--

a. is between--

1) attorneys discussing the giving of legal advice or assistance in anticipated or pending litigation; or

2) an attorney and one seeking legal advice or assistance in anticipated or pending litigation; or

3) an attorney or attorneys and one or others engaged in assisting the attorney in the rendering of such advice or the giving of such assistance; and

b. involves--

1) the giving or seeking of legal advice; or

2) anticipated or pending litigation.

B. This prohibition shall not apply:

1. if the attorney, attorneys, or their assistants are, by such meetings or communications, participating in criminal activity; or

2. to a person who is a police officer, if such a person--

a. is know to the other participants in the meeting or conversation as a police officer; or

b. both--

1) is attending the meeting or participating in the conversation as a private individual; and

2) does not in his or her capacity as a police officer report on the meeting or conversation to any other defendant, except as allowed in I.B.1.

II. ENFORCEMENT.

A. Institutional.

1. **Training:**

Training with respect to the requirements of this Judgment shall be provided to new recruits as part of the Police Academy curriculum; and on a continuing, in-service basis to personnel of the Bureaus of Investigative, and Community Services, all district tactical units, and all other units likely to engage in investigative activity.

2. **Notice to defendants.**

All present employees of the Chicago Police Department, and, in the future, all new employees, before resuming or assuming their official duties, shall be given a copy of this Order. In addition, the summary attached hereto as "Exhibit A" shall be given, through enclosure in pay envelopes or by a similar method, to each Chicago Police Department employee no less frequently than once every five years.

3. **Internal reporting.**

At any point at which any defendant knows or, by the use of reasonable diligence, should know that any defendant is engaged in activity prohibited by Part I hereof, the defendant with such knowledge shall have the duty to report such activity in writing to his or her immediate superior. Such superior shall have the duty to forward a copy of this written report, along with the superior's report, if any, to the office of the Superintendent of Police.

B. Judicial.

1. **Continuing jurisdiction.**

This court shall retain jurisdiction of this cause for the enforcement of this Order and to punish violations thereof.

a. **Persons who may apply for sanctions.**

Application to enforce this Order or to punish violations thereof may be presented to this court by any person affected by the conduct complained of.

b. **Notice.**

Prior written notice of all such applications and other matters in this action shall be given to counsel for the named parties hereto. Except where emergency relief is sought, seven days notice shall be given.

2. **Private action for damages.**

Any person affected by the conduct complained of, independent of a request to this court for sanctions, may bring an action for damages if such cause of action apart from this order exists in state or federal court.

III. ANCILLARY MATTERS.

A. This judgment represents the agreed disposition of all substantive claims by plaintiff against defendants.

B. The court expressly finds, pursuant to Federal Rule of Civil Procedure 54(b), that there is not just reason for delay, and directs that this judgment be entered forthwith.

C. **Attorney's Fees.**

Plaintiff will petition the court to determine whether and in what amount fees and costs will be awarded with respect to the matters resolved by this Agreed Order, Judgment and Decree. Defendants will file objections. The parties have made no agreement with respect to these questions.

END OF TEXT OF JUDGMENT ORDER (76 C 1982)

Attachment No. 3

Nelson v. Streeter, et.al., No. 88 C 5434

JUDGMENT ORDER

PURPOSE

In the course of our daily activities, we may be confronted with situations in which an audience is hostile to the lawful expression of some individual or group of individuals. An angry crowd may gather around an individual making a speech in a public park, or people may assemble to protest an art exhibit they find offensive. All individuals have the right to express their opinions, but no one has the right to interfere with the expression of others.

In these types of hostile audience situations, we as police officers have important obligations. We have a general duty to maintain public order and to protect persons and property from harm; these are important governmental interests. But we have an equally important duty under the First Amendment to protect lawful expression from a hostile audience.

The purpose of this Department directive is to provide some guidance to Department members facing a hostile audience situation.

BACKGROUND

The First Amendment protects the rights of all persons to freedom of speech. In enforcing the protections of the First Amendment, we must approach our responsibilities with the neutrality of professionalism. We must protect the free speech rights of all persons, even if we as individuals do not personally like or agree with the particular message or position or philosophy espoused. Likewise, we must protect lawful expression even if other people are offended by it. These are fundamental principles embodied in the Department's mission statement and in the Law Enforcement Code of Ethics we have sworn to uphold.

Of course, not all speech is protected under all circumstances. For example, the government also has the right to impose reasonable time, place and manner restrictions on speech. Likewise, the expression of lawful speech does not excuse the commission of other, unlawful behavior. As police officers, we have an obligation to arrest individuals who are violating the law, even if they are also engaged in First Amendment activity. Except for specific circumstances such as these, however, we have a duty to enforce the broad protections of the First Amendment vigorously and impartially.

No person has a right to violate any applicable state law or municipal ordinance merely

because that person is engaging in expressive activities. Such persons may be cited or arrested, as appropriate, and any physical evidence relevant to the offense may be seized. When an individual has not violated any law, however, and the threat to public order arises solely from the reaction of a hostile audience, we must protect First Amendment rights.

The Department's responsibilities in hostile audience situations are not trivial or insignificant. The open expression of ideas is one of our nation's most cherished freedoms. It is a fundamental principle that sets us apart from so many other nations.

For police personnel, the First Amendment carries particular importance. As part of the community, all of us as individuals enjoy and frequently exercise our First Amendment rights. As police officers, we have a unique obligation to uphold and protect the free speech rights of all members of the community, regardless of how unpopular or controversial their ideas may be. This is a unique responsibility that we are uniquely qualified to carry out.

PROCEDURES

In a hostile audience situation, where there are threats to a speaker, artist, exhibitor or art work, or where there is a danger of harm to persons or property, police officers should endeavor to proceed as follows:

1. Where art work or other expressive material is involved, officers should try to establish who has possessory rights to the material, including ownership and the right of custody.

2. Assuming that the speaker, artist or exhibitor is lawfully present on the property, officers should advise them of their right to continue their expression at the original site, except under the circumstances identified below.

3. If the speaker, artist or exhibitor decides to continue its expression at the original site, officers should commence or continue police protection so as to allow the continued expression, except under the circumstances identified below.

4. Officers should summon a supervisor to the scene who will determine if the assignment of additional police personnel is necessary.

Where police officers determine that expression cannot continue at the original site due to the activities of persons hostile to the expression, police officers should endeavor to proceed as follows:

1. The highest ranking sworn member on the scene, or if reasonably possible, the Superintendent or a member acting in his stead will determine: (a)that all police

resources reasonably available have been deployed to maintain the peace and allow the expression to take place; (b) that police efforts to take direct action against those violating the law have not been successful; and (c) that there is a threat of imminent violence that police are unable to control.

2. If reasonably possible, officers should consult with Department or City of Chicago legal advisors.

3. The expression may be discontinued at the original site where the highest ranking sworn member on the scene, or if reasonably possible, the Superintendent or a member acting in his stead, determines that order can be restored only by taking the expressive material into protective custody, or otherwise discontinuing the expression, and that available alternatives of continuing private custody have been considered and cannot be employed.

4. Any seizure into protective custody of expressive material must be of the shortest possible duration. The material seized will be inventoried and shall be returned to its owner or custodian at the earliest opportunity, and police protection continued as required by the circumstances at the original site. The owner should be advised of his right to immediately reclaim the expressive material at the unit of inventory.

END OF TEXT OF JUDGMENT ORDER (88 C 5434)

Chicago Police Department

General Order G02-02-01

INVESTIGATIONS DIRECTED AT FIRST AMENDMENT-RELATED INTELLIGENCE

ISSUE DATE:	09 January 2006	**EFFECTIVE DATE:**	16 January 2006
RESCINDS:	G02-10-01B		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. identifies and explains types of investigations which implicate rights protected by the First Amendment to the Constitution, even though not undertaken for the purpose of effecting the exercise of First Amendment rights.

B. establishes responsibilities and procedures, including the need for special authorizations, relative to investigations which implicate First Amendment rights. Department members will refer to the Special Order entitled "**Investigations Directed at First Amendment-Related Intelligence**" for information regarding specific methods, approvals and authorizations, and retention of documents.

C. refers members to the modified consent decree governing investigations relating to First Amendment rights, which is included as Attachment No. 1 of the Department directive entitled "**The First Amendment and Police Actions**."

II. FIRST AMENDMENT POLICY

A. Proper and Permissible Police Action

1. All police action will be conducted in accordance with the Constitution of the United States, including the First Amendment of the Constitution, in accordance with the law, and with the modified consent decree.

2. All police action will be conducted for a proper law enforcement purpose.

   a. The First Amendment protects the right of free expression, including oral or written speech, broadcasts, or other communications. The First Amendment does not prohibit police personnel from initiating investigations of expression, provided that there is a reasonable law enforcement purpose for doing so.

   b. A reasonable law enforcement purpose means that the investigation is intended to address unlawful conduct, either past, present, or future, including whether a person has knowledge of such past, present, or future unlawful conduct, or to address public safety issues, whether they amount to criminal conduct or not. A reasonable law enforcement purpose would include acquiring information or intelligence which may be useful in allocating resources for public safety and acquiring information or intelligence which may be useful for future criminal investigations.

   c. An investigation implicating First Amendment rights which is undertaken for a reasonable law enforcement purpose must be reasonable in scope and must not be intended to punish, discriminate, or retaliate against any person on the basis of conduct protected by the First Amendment.

3. All permissible investigations will be conducted in a manner which is least likely to impact a person's First Amendment rights, so that less invasive methods will be used where possible.

B. Prohibited Action: Under no circumstances will any sworn member or other employee of the Chicago Police Department:

1. investigate, prosecute, disrupt, interfere with, or harass any person for the purpose of preventing that person from engaging in conduct protected by the First Amendment;

2. investigate, prosecute, disrupt, interfere with, or harass any person for the purpose of punishing or retaliating against that person for engaging in conduct protected by the First Amendment;

3. discriminate against any person on the basis of conduct protected by the First Amendment, except as may be permitted by law;

4. authorize, assist, or encourage any person to engage in conduct which violates Items II-B-1 through II-B-3.

III. IMPERMISSIBLE INVESTIGATIONS

A. It is not permissible to investigate someone solely because that person advocates a position in his or her speech or writings which is offensive or disagreeable. It is not permissible to investigate someone for the content of his or her speech if there is no reasonable law enforcement purpose, such as criminal conduct or public safety.

B. Examples of Investigations Which Violate the First Amendment

1. A police officer undertakes an investigation of a crime allegedly committed by a member of a race-based hate group. During the course of the investigation, the officer decides to interview the employer of an admitted member of the group, even though there is no indication that the employer has any knowledge of the crime. The officer conducts the interview because he feels that the employer should be aware that one of his employees is a member of this type of organization. Although the investigation into the crime is permissible, there is no appropriate law enforcement justification for the interview with the employer, and therefore, it violates the First Amendment.

2. A police officer hears a CD which contains numerous songs with lyrics derogatory towards law enforcement, but none of the songs threaten violence. The officer decides to investigate the musical group because the officer is offended by the lyrics. The officer talks to the group's producer, manager, and record label about why the group puts out music with such lyrics. There is no appropriate law enforcement justification for this investigation, and therefore, it violates the First Amendment and is impermissible.

IV. PERMISSIBLE INVESTIGATIONS WHICH REQUIRE NO SPECIAL AUTHORIZATION

A. Investigations not based on First Amendment activity are permissible and require no special authorization under this directive. If an investigation is begun based on an articulable suspicion of criminal activity, such as illegal drug dealing, the unlawful use of weapons, or other illegal activity, this directive does not require special authorization for that investigation even if at some point it involves examination of speech or other expression. However, such an investigation will still comply with the First Amendment policy as set forth in Item I of this directive.

B. Examples of Permissible Investigations Which Require No Special Authorization

1. An officer receives information that a suspect is selling marijuana at a particular location. The officer goes undercover to purchase marijuana from the suspect in order to gather evidence to prosecute the suspect criminally. During the drug transaction, the suspect mentions that he thinks marijuana should be legal in the United States. The investigation was undertaken due to the reasonable suspicion that the suspect was selling drugs, not as a result of his speech or opinion. Therefore, this directive does not require special authorization for the investigation

of the suspect's drug activity, even though the suspect engages in his First Amendment right to express his opinion that marijuana should be legal.

NOTE: If this investigation had been initiated based on the suspect advocating legalization of drugs, the investigation would have required special authorization as detailed in Item V of this directive.

2. An officer has arrested several members of a street gang for violent criminal conduct. The officer wants to identify regular associates of these gang members, including searching the Internet for evidence of the gang member's associates. This investigation is based upon reasonable suspicion that the associates of these gang members are engaging in illegal conduct and is not based upon speech or other expression. Therefore, this investigation does not require any special authorization under this directive.

3. A police officer begins an investigation in response to a report that music is being played too loudly at a tavern. In addition, the tavern is known for playing music whose lyrics offend some members of the population. This investigation requires no special authorization under this addendum, even though music is generally protected by the First Amendment, because the investigation is undertaken to determine if there has been a violation of an applicable anti-noise ordinance rather than based upon the musical lyrics.

4. An informant tells an officer that an anarchist group plans to deface the building of a large corporate headquarters located in downtown Chicago. Based upon this information, the officer begins an investigation of this group, including a review of the Internet sites and any writings of the group, to determine the credibility and any details of the alleged plot. This investigation is based upon a reasonable suspicion of criminal conduct, rather than the oral or written expressions of the group. Therefore, no special authorization is required.

NOTE: Had this investigation been initiated based on the writings of the anarchist group that "corporations are ruining the country and need to be stopped," rather than upon information of planned criminal conduct, the investigation would have required special authorization as detailed in Item IV of this directive.

C. Investigating Hate Crimes Within the Confines of the First Amendment

To the extent that review of expression is necessary for the prosecution of criminal conduct under a "hate crime" law, the investigation is initiated due to the crime, and the review of expression is permissible as having a reasonable purpose related to the elements of the crime. Therefore, such investigations require no special authorization as detailed in this directive.

V. PERMISSIBLE INVESTIGATIONS IF SPECIALLY AUTHORIZED UNDER THIS DIRECTIVE (FIRST AMENDMENT INTELLIGENCE GATHERING INVESTIGATIONS)

A. First Amendment Intelligence Gathering Investigation Defined

A First Amendment intelligence gathering investigation is the gathering and analysis of written or oral speech or other expression which is undertaken:

1. due to or on the basis of the content of the speech or other expression and;

2. for the purpose of preventing future crime or for the purpose of aiding likely future investigations, even in the absence of an articulable suspicion to believe that a violation of law has occurred.

B. First Amendment Intelligence Gathering Policy

1. Certain law enforcement investigations prompted by or based upon a person's speech or other expression, whether written or oral, are permitted provided that there is a reasonable law enforcement purpose, as detailed in Item II-A-2 of this directive, for doing so. If an investigation is prompted by or based upon a person's speech or other expression for a

reasonable law enforcement purpose, the investigation is permissible but requires special authorization as outlined in this directive.

2. It is permissible to gather intelligence consisting of speech or other expression that is expected to serve a reasonable law enforcement purpose in the future even if not based on an articulable suspicion that a violation of law has occurred, and even when the investigation is undertaken on the basis of speech or other conduct protected by the First Amendment. Intelligence gathering is a legitimate law enforcement function provided it is conducted for reasonable law enforcement purposes, such as preventing crimes or providing information that may constitute useful future investigative leads. Intelligence gathering investigations undertaken in whole or part because of speech or other activity protected by the First Amendment require a proper law enforcement purpose and special authorization as provided in Item II of the Special Order entitled "**Investigations Directed at First Amendment-Related Intelligence**."

3. Advocacy of violence or unlawful acts or expression of sympathy with violence or unlawful acts is protected by the First Amendment until such advocacy presents an imminent and credible threat. Nevertheless, law enforcement has a duty to gather information about groups and individuals who advocate law breaking or express sympathy with law breaking in order to determine whether these groups or individuals are engaged in or plan unlawful activities, as well as to obtain intelligence that may be useful in future investigations and preventing future crime.

4. Debriefing or questioning arrestees regarding their social, political, or religious views is not permitted unless specifically related to criminal conduct necessary for investigation of illegal conduct or pursuant to an authorized First Amendment intelligence gathering investigation. For instance, a demonstrator at a rally who is arrested for blocking traffic will not be interrogated as to his or her political views.

C. Examples of First Amendment Intelligence Gathering Investigations Permitted if Specially Authorized as Provided in this Directive

1. A person is standing on a street corner in the Loop, violating no laws, but is offering passers-by literature supporting the bombing of targets in the United States. A plainclothes officer accepts the literature. Based upon the literature, the officer initiates an investigation into the source of the literature, including all statements made by the source, to determine the source's intentions, capabilities, funding, and other information related to assessing future violence. This investigation was prompted by the expression contained in the literature but was undertaken for a proper law enforcement purpose and therefore constitutes proper gathering of First Amendment-related intelligence if special authorization is received.

2. A police officer discovers a site on the internet run by a hate group which espouses violence against government officials and lists the addresses and personal routines of certain government officials. The officer opens an investigation into the group and includes a request for undercover officers to attend meetings of the group. Although the investigation is not prompted by a reasonable suspicion of a specific crime, it is undertaken to determine the credibility of any threats and the future criminal plans of the hate group and is thereby permissible under this directive if special authorization is received. In this instance, placing an undercover officer in the meeting has a reasonable law enforcement purpose.

3. An officer learns that a radical cleric has opened a place of worship in Chicago. This cleric preaches destruction of Western values and has a history of drawing persons involved in terrorist activities to places of worship that he organizes. Surveillance undertaken to determine if the cleric is drawing known terrorists to his place of worship has a reasonable law enforcement purpose even though not based upon reasonable suspicion of a specific crime and is therefore permissible under this addendum if special authorization is received.

4. A public rally is planned. One of the groups urging its members to attend is also speaking about the need to target and destroy certain symbols of corporate America. Although the investigation is based upon the speech of the group, sending an undercover officer to the meeting of this group to determine if any and what criminal activity is planned for the rally is a

reasonable law enforcement purpose and therefore is permissible under this addendum if special authorization is received.

VI. METHODS OF FIRST AMENDMENT INTELLIGENCE GATHERING: USE OF INFORMANTS, UNDERCOVER OFFICERS, AND INFILTRATORS

General Policy on Undercover Investigative Methods

C. The use of informants, undercover officers, and infiltrators to investigate individuals, groups, or organizations involved in social or political activity have the potential to substantially impact protected First Amendment rights, with infiltrators posing the highest risk of such impact. The use of these investigative methods is not prohibited by the First Amendment, but these methods should be used only to the extent necessary and in a manner designed to have the least impact upon First Amendment rights and should be closely monitored to ensure that the method is used only when and to the extent reasonable under the circumstances and for proper purposes.

D. The use of informants, undercover officers, or infiltrators requires specific authorizations as described in Item VI of this directive.

VII. PUBLIC GATHERINGS AND FIRST AMENDMENT CONDUCT

A. Public Speech and Public Gatherings and First Amendment Conduct

An event or gathering in public may be held for the purpose of or concerning ideas or beliefs about public or social policy, or political, educational, cultural, economic, philosophical, or religious matters. However, the First Amendment does not necessarily apply to gatherings or public assemblies unrelated to the right to hold and express the ideas and beliefs. For example, a public fireworks display need not have any First Amendment significance.

B. Policy Regarding Public Speech and Public Gatherings

All Department members present at public gatherings will be courteous and respectful. Members will not harass, intimidate, or make comments about the views expressed by persons attending public gatherings. Members will not interrogate or otherwise question participants concerning their views unless essential to an investigation of an apparent violation of law or as part of an investigation directed toward First Amendment-related intelligence that has been authorized as provided below.

C. Any sworn Department member may initiate a preliminary investigation of a public gathering for public safety purposes without requiring authorization as outlined in this directive, as follows:

1. Members may gather publicly available information about public gatherings, including information available on internet sites. Members may investigate publicly available information on prior public gatherings when useful to determine what police resources will be necessary to adequately protect demonstrators, bystanders, the general public, and to enforce all applicable laws.

2. Members may communicate overtly with any person involved in a public gathering regarding the number of persons expected to participate and similar information regarding the time, place, route, and manner of a public gathering and may review documents submitted for such purpose, such as parade permit applications.

3. Members may attend public rallies and walk in public parades without disclosing their identity provided that their purpose is solely to monitor the rally or parade for public safety and criminal conduct issues and that they do not direct or influence the participants of the rally or

parade or do not affirmatively represent themselves to be members of a specific participating organization.

Philip J. Cline
Superintendent of Police

05-140 LMT(PMD)

Chicago Police Department

General Order G02-02-02

OTHER POLICE ACTION WHICH MAY IMPACT FIRST AMENDMENT CONDUCT

ISSUE DATE:	13 October 2010	**EFFECTIVE DATE:**	13 October 2010
RESCINDS:	G02-10-02		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. describes the prohibitions on police action when the attorney-client relationship is involved, as described in the judgment order entered in case 76 C 1982.

B. informs members of their obligations to protect the First Amendment rights of law-abiding individuals who encounter a hostile audience threatening to create public disorder, as described in the judgment order entered in Nelson v. Streeter, et.al., No. 88 C 5434.

C. provides members with the text of the judgment orders, as required by provisions of each order, as Attachments No. 2 and 3 of this directive.

II. FIRST AMENDMENT PROHIBITIONS CONCERNING ATTORNEY-CLIENT RELATIONSHIPS (CASE 76 C 1982)

A. Judgment Order 76 C 1982 prohibits certain actions by Department members in relation to the exercise of First Amendment rights by arrested persons. The entire text of the judgment order is included as Attachment No. 2.

B. Department members will not conduct surveillance at, gather information or compile reports on, or maintain files or records regarding meetings or communications if:

1. during the meeting or communication, there is a reasonable expectation of privacy and that the attorney-client privilege will attach; and
2. the meeting or communication is between:
    a. attorneys discussing the giving of legal advice or assistance in anticipated or pending litigation; or
    b. an attorney and an individual seeking legal advice or assistance in anticipated or pending litigation; or
    c. an attorney or attorneys and one or more individuals engaged in assisting the attorney in the rendering of such advice or the giving of such assistance and involves:
        (1) the giving or seeking of legal advice; or
        (2) anticipated or pending litigation.

C. This prohibition will not apply:

1. if the attorney, attorneys, or their assistants are, by such meetings or communications, participating in criminal activity; or
2. to a person who is a police officer, if such a person:
    a. is known to the other participants in the meeting or conversation as a police officer; OR

b. is both of the following:

(1) attending the meeting or participating in the conversation as a private individual AND

(2) will not be reporting in his or her capacity as a police officer on the meeting or conversation to any other defendant, unless such persons are participating in criminal activity.

III. PROTECTIONS OF FIRST AMENDMENT RIGHTS IN A HOSTILE AUDIENCE ENVIRONMENT (CASE 88C5434)

A. Judgment Order 88 C 5434, Nelson v. Streeter, et.al., relates to Department members' responsibilities at public exhibitions of ideas which may result in hostile reactions from those viewing or hearing the exhibition. The entire text of the judgment order is included as Attachment No. 3.

B. Department members will protect the free speech rights of all persons, no matter what the particular message, position, or philosophy espoused, and even if other people are offended by it, as long as the person expressing that message, position, or philosophy is not violating the law and has abided by any reasonable time, place, and manner restrictions placed on the expression of such ideas.

C. In an incident where a hostile audience threatens a speaker, artist, exhibitor or art work or where there is a danger of harm to persons or property, members will:

1. if art work or other expressive material is involved, attempt to ascertain who owns or has right of custody of the material;
2. advise the speaker, artist, or exhibitor, if present, of his or her right to continue their expression at the current site;
3. begin or continue police protection so as to allow the speaker, artist, or exhibitor to continue his or her expression of speech or art;
4. request that their supervisor respond to the scene.

D. A supervisor who responds to the scene where an expression of speech or art is threatened by a hostile audience will determine if the assignment of additional police personnel will allow for the continuation of the expression.

E. If members determine that the expression cannot continue at the original site due to the activities of persons hostile to the expression, the highest ranking sworn member on the scene will determine that:

1. all police resources reasonably available have been deployed to maintain the peace and allow the expression to take place;
2. police efforts to take direct action against those violating the law have not been successful, and;
3. there remains a threat of imminent violence that police personnel are unable to control.

NOTE: If reasonably possible, members should consult with Department or City of Chicago legal advisors prior to taking action to discontinue a public expression of speech or art.

F. The expression may be discontinued at the original site when the highest ranking member on the scene determines that:

1. order can be restored:

a. only by taking the expressive material into custody or

b. otherwise discontinuing the expression.

2. available alternatives of continuing private custody have been considered but cannot be deployed.

3. when expression is discontinued, it should be permitted to resume as soon as the highest ranking member on the scene determines that order has been restored and can be maintained if the expression resumes.

G. Any expressive material taken into protective custody will be inventoried according to general inventory procedures. The owner of the material will be advised of his or her right to immediately reclaim the material at the unit of inventory.

Terry G. Hillard
Superintendent of Police

01-006 LMT(PMD)

Chicago Police Department

Special Order S02-02-01

INVESTIGATIONS DIRECTED AT FIRST AMENDMENT-RELATED INTELLIGENCE

ISSUE DATE:	26 October 2011	**EFFECTIVE DATE:**	26 October 2011
RESCINDS:	16 January 2006 Version; G02-10-01B		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive delineates methods, approvals and authorizations, and retention of documents. Department members will refer to the General Order entitled "**Investigations Directed at First Amendment-Related Intelligence**" for information regarding the types of investigations that can and cannot be conducted and responsibilities relative to First Amendment rights.

II. METHODS OF FIRST AMENDMENT INTELLIGENCE GATHERING: USE OF INFORMANTS, UNDERCOVER OFFICERS, AND INFILTRATORS

A. Methods of First Amendment intelligence gathering include all investigative methods, including but not limited to interviews, gathering written documents, and undercover investigative methods.

B. Undercover investigative methods include the use of an informant, an undercover officer, or an infiltrator in the investigation.

1. Informant

An informant is a person, not a police officer, who is providing information not publicly available to the police about other individuals, groups of individuals, or organizations.

EXAMPLE: A member of an organization contacts the police and informs an officer that at a private meeting held at an organizer's home, the organization discussed the possible bombing of a government building. The member tells the officer that he receives updates of activities and notices of meetings by email. The officer asks the member to provide him with a copy of the email updates and notices. The member of the organization is an informant.

2. Undercover Officer

An undercover officer is an officer who attends meetings or activities of the group or organization under investigation without disclosing his or her identity for the purpose of gathering information, but who does not become a part of the group for the purpose of influencing, directing, or participating in the organization.

EXAMPLE: The informant provides the officer with email notices of an upcoming meeting open to the public. The officer plans to attend to learn the identity of and observe the organizers. The officer, dressed in casual street clothes, attends the meeting but does not disclose his real identity. The officer listens and expresses support for the group but does not suggest any specific activities. The officer is an undercover officer.

3. Infiltrator

An infiltrator is an officer who affirmatively identifies himself as a member or participant in the group or organization and who does not disclose his function as an agent of the police. An infiltrator becomes a member of the organization under investigation and acts in a manner which participates, influences, or directs the organization.

EXAMPLE: After attending several meetings undercover, the officer becomes friendly with the organizers and is invited to private meetings at organizers' homes. He attends and participates in group debates about how to be effective in the organization's goals. The officer is now an infiltrator.

III. APPROVALS AND AUTHORIZATIONS

A. Special Authorizations Required for Permissible First Amendment Intelligence Gathering Investigations

1. First Amendment Investigation Initiation Report

A member who seeks to conduct a First Amendment intelligence gathering investigation will submit to his or her unit command staff officer a To-From-Subject report, addressed to the Superintendent of Police, Attention: General Counsel, and containing an approval line for the member's district or unit commanding officer and the chief of the member's bureau. The report will contain the following information:

a. Date and time the investigation will be initiated;

b. Basis of initiating the investigation and the reasonable law enforcement purpose of the investigation;

c. Methods of investigation sought to be employed and why these methods are likely to be more effective than less invasive investigative methods;

d. Amount of time the investigation is expected to last.

2. Commander Approval and First Amendment Worksheet

a. The unit command staff member who receives a To-From-Subject report initiating a First Amendment intelligence gathering investigation will approve the request only if he or she determines that the investigation is in accordance with the policy expressed in this directive.

NOTE: In the absence of a member of the command staff, the command staff member of the next higher rank will assume this responsibility.

b. If the command staff member approves the investigation, the commanding officer will:

(1) complete a First Amendment Worksheet, assigning a proper First Amendment Investigation tracking number to the worksheet using the following formula:

(a) the requesting unit number will appear first, followed by a dash;

(b) the calendar year will appear second, followed by a dash;

(c) the last number in the series will be the sequential number of the First Amendment-related investigation for that unit, as evidenced by that unit's First Amendment Investigation Unit Log.

EXAMPLE: A number of 188-2005-03 will designate the third First Amendment-related investigation for Unit 188 in the year 2005. This number will be recorded on the First Amendment Worksheet in the upper right-hand corner.

(2) provide written authorization for the investigation to the initiating member in the form of a copy of the completed First Amendment Worksheet containing

the date on which the authorization will expire and any limits on the use of investigative methods.

(3) submit the approved To-From-Subject initiation report and the completed First Amendment Worksheet to the chief of his or her bureau.

3. Bureau Chief Approval

A bureau chief who receives an approved To-From-Subject report initiating a First Amendment intelligence gathering investigation will approve the request only if he or she determines that the investigation is in accordance with the policy expressed in this directive. If approved, the bureau chief will submit the To-From-Subject initiation report, the First Amendment Worksheet, and any other pertinent materials to the General Counsel to the Superintendent.

4. General Counsel Concurrence

The General Counsel will advise the chief as to whether the investigation is permitted by the First Amendment and this directive and also confer with chiefs to ensure that the investigation does not duplicate another ongoing, approved First Amendment investigation. The General Counsel will review the submitted materials and either:

a. sign a concurrence on the First Amendment Worksheet where indicated, based upon the information provided, and return the original To-From-Subject initiation report and First Amendment Worksheet to the submitting chief.

b. if not in concurrence with an authorization, contact the affected chief in an attempt to resolve any concerns. If such concerns cannot be resolved, the matter will be submitted to the Superintendent for a decision. If the Superintendent determines that the investigation shall be initiated, the Superintendent will sign the concurrence in place of the General Counsel.

5. Notwithstanding the requirement of special authorization, a member may initiate and conduct a First Amendment intelligence gathering investigation, without prior special authorization, provided:

a. it is impractical to submit the required paperwork prior to initiating the investigation;

b. a command staff member has verbally approved the investigation, but infiltration may be approved verbally only by the Superintendent, and;

c. all required paperwork is submitted as soon as practicable but in no event later than twenty-four hours after the initiation of the investigation.

B. Additional Authorization Necessary For Use of Infiltrator

Any use of an infiltrator requires the prior approval of the Superintendent. A request to use an infiltrator will be submitted in a separate To-From-Subject report in the form of a First Amendment investigation initiation report, in accordance with the requirements of such a report as indicated in Item III-A-1, with an additional approval line for the Superintendent.

C. Continued Monitoring

Members will continually assess the authorized use of undercover methods and determine whether the use of these methods remain warranted in light of the information generated by these methods. Members conducting the investigation will submit to their unit command staff officer To-From-Subject reports detailing the progress of the investigation at thirty-day intervals or at shorter intervals as directed by the commanding officer. A command staff member may revoke his or her approval at any time for good reason and will, upon such revocation, notify his or her chief. A chief may revoke his or her approval at any time for good reason. Upon the revocation of either approval, the investigation will be terminated.

D. Time Limits on Authorizations of Investigations

1. Authorization to conduct First Amendment-related intelligence gathering will be in effect for a period not to exceed 120 days and may be approved in increments not to exceed 120 days in order to ensure that the investigation remains in accordance with this directive and the First Amendment. Prior to the expiration of the initial or succeeding authorized periods, application may be made for an additional period of up to 120 days, beginning upon the expiration of the preceding period, in a To-From-Subject report to the chief of the bureau containing the investigative unit. If the authorized period expires without proper approval of an extension, the investigation is automatically terminated.

2. Authorization to employ undercover methods will be in effect for a period not to exceed thirty days and may be approved in shorter increments in order to ensure that the investigation remains in accordance with this directive and the First Amendment. Prior to the expiration of the initial or succeeding authorized periods, application may be made for an additional period of up to thirty days, beginning upon the expiration of the preceding period, in a To-From-Subject report to the chief of the bureau containing the investigative unit. If the authorized period expires without proper approval of an extension, the investigation is automatically terminated.

3. Continued use of an infiltrator after the expiration of the initial authorized period also requires application for an extension for up to thirty days, in the form of a separate To-From-Subject report to the chief, with an additional approval line for the Superintendent.

E. Terminations

Upon termination of the investigation, by expiration or otherwise, the commanding officer of the investigating unit will complete a First Amendment Worksheet detailing the basis for and the date of the termination of the investigation and submit that Worksheet to his or her chief for forwarding to the General Counsel. All members involved in the investigation will be notified of the termination, and all documents will be retained and/or forwarded as indicated in Item V of this directive.

IV. PUBLIC GATHERINGS AND FIRST AMENDMENT CONDUCT

A. Documenting Investigations of Public Gatherings

Information obtained during the course of such a preliminary investigation will be made the subject of an Information Report (CPD-11.461), in order to facilitate future assessments of resources and public safety. That report, along with pertinent attachments, will be forwarded through the chain of command to the chief of the bureau of the member, with a copy to the First Deputy Superintendent. The Information Report will be treated, maintained, and retained in accordance with Department policy for non-First Amendment-related investigations.

B. *Video Recording, Audio Recording, and Photographing Public Gatherings*

Video recording and photographing of events on the public way are generally appropriate and may be conducted for any proper law enforcement purpose, including documenting violations of law, monitoring police conduct, defending against allegations of police misconduct, aiding in the future coordination and deployment of police resources, and training. Furthermore, audio recording may be authorized at the discretion of an exempt commanding officer as circumstances warrant, including documenting the issuance of police orders, warnings, or notices.

1. If done for any of the above reasons, *video recording, audio recording,* or photographing a public gathering is not an investigation directed toward First Amendment-related intelligence within the meaning of this directive, and the retention and disposal of such *video recording, audio recording*, or photographs will follow the restrictions outlined in Item IV-B-4 of this directive.

2. If *video recording, audio recording*, or photographing is done as part of an intelligence gathering investigation, the retention and disposal of such video recordings or photographs will follow the restrictions outlined in Item IV of this directive. Each video recording or photograph will be identified by its own unique tracking number.

3. Approval for *Video Recording, Audio Recording,* or Photographing Public Gatherings

Video Recording, audio recording, and photographing public gatherings must be approved by an *exempt commanding officer*. The *exempt commanding officer* will determine, based upon operational needs, who or which unit will conduct the *video recording, audio recording,* or photographing. The officer in charge of the event will ensure that the *video recording, audio recording*, or photographing equipment is available and used appropriately.

4. Retention of *Video Recordings, Audio Recordings*, or Photographs Taken at Public Gatherings

a. As soon as practicable, the unit which conducted the recording or photographing will send a To-From-Subject report to the persons listed below, indicating the nature of the *video recording, audio recording*, or photographs, the fact that they will be held within the unit for sixty days, and requesting a written signature acknowledging that there is no known reason to retain them past the sixty-day time period. Reasons for retention of the *video recording, audio recording*, or photographs include future training or planning purposes or allegations of criminal conduct or officer misconduct arising out of the event for which the *video recording, audio recording*, or photographs may be useful.

(1) General Counsel to the Superintendent;

(2) Chief, Bureau of Detectives;

(3) Chief, Bureau of Internal Affairs;

(4) Deputy Chief, Education and Training Division;

(5) Commander, Special Events Unit;

(6) Chief Administrator, Independent Police Review Authority.

b. If the persons listed above all sign an acknowledgment that there is no known reason to retain the *video recording, audio recording*, or photographs, then the unit retaining the *video recording, audio recording*, or photographs will dispose of them but retain the signed acknowledgments in unit files. If any person listed in Item IV-B-4-a-(1) through (6) requests that the *video recording, audio recording*, or photographs be retained due to future training or planning purposes or due to allegations of criminal conduct or officer misconduct arising out of the event, then the person requesting retention will direct the unit where to send the *video recording, audio recording*, or photographs. The sending unit will document the transfer of the *video recording, audio recording*, or photographs in a To-From-Subject report, which will be signed by a member at the accepting unit to indicate receipt of the *video recording, audio recording*, or photographs. The To-From-Subject report will be retained in original unit files.

V. RETENTION OF DOCUMENTS RELATING TO FIRST AMENDMENT INTELLIGENCE INVESTIGATIONS

A. The command staff member of the investigating unit will retain the documents and any films or photographs related to a First Amendment intelligence gathering investigation until the latter of:

1. the time that the documents cease to serve a proper law enforcement purpose (for instance, the information becomes stale) OR

2. the investigation is closed.

B. Upon the later expiration of the two preceding events, the commanding officer will forward all documents, films, and photographs related to this investigation, including all copies, to his or her chief with a To-From-Subject report indicating the action taken and the reason for the action (i.e., that the information is no longer relevant or that the investigation closed on a date indicated in the report). A copy of this report will also be directed to the Commander, Inspections Division.

C. Upon receipt of documents, films, and photographs from the commanding officer, the chief of the bureau containing the investigative unit will retain them until the next internal First Amendment audit,

at which time the chief will turn over the materials to the Inspections Division. The chief will address a To-From-Subject report to the Commander, Inspections Division, indicating the date that the documents, films, and photographs are turned over. The report and the related materials will be hand-carried to the Inspections Division, where a member of that division will sign a copy of the To-From-Subject report to indicate receipt of the materials. The chief will retain that signed receipted copy of the To-From-Subject report through the next external First Amendment audit.

D. The Inspections Division will maintain and preserve the documents, films, and photographs from First Amendment investigations received from the chief of the investigating unit until the latter of:

1. the next external First Amendment audit after receipt of such documents OR
2. a period of three years from the close of the investigation.

NOTE: This retention schedule will ensure that the external auditors will have an opportunity to examine such documents and that the documents will be available to defend any First Amendment lawsuit (such lawsuit being required to be filed within two years of the incident). Upon learning of the filing of any such lawsuit, the Inspections Division will suspend any destruction of relevant documents without regard to the retention schedule described above.

E. The General Counsel will maintain a copy of all First Amendment Worksheets until the latter of:

1. the next external First Amendment audit after the worksheet is opened OR
2. a period of three years from the time that the investigation was closed.

F. Notwithstanding anything in this directive, the commanding officer of the investigating unit or the respective chief may forward a copy of a report detailing information gathered in an investigation governed by this directive to the Deployment Operations Center (DOC) if appropriate to serve a reasonable law enforcement purpose as determined by the commanding officer of the investigative unit, the Commander of the DOC, the respective chief, and upon the advice of the General Counsel. The commanding officer of the investigative unit will document the forwarding of the copy of such information to the DOC in a To-From-Subject report containing the action taken, the date of such action, and the reason for the action, to be addressed to his or her chief, and maintained as if one of the original documents of the investigation.

G. Notwithstanding anything in this directive, the commanding officer of the investigative unit or his or her chief may forward to the Commander, Special Events Unit copies of any information gathered in an investigation governed by this directive which relate to a threat to the physical safety of a dignitary or to a public gathering.

(Items indicated by *italic/double underline* were added or revised on 26 October 2011)

Authenticated by: RMJ

Garry F. McCarthy
Superintendent of Police

11-101 TRH

Chicago Police Department

General Order G02-03

CHICAGO ALTERNATIVE POLICING STRATEGY (CAPS)

ISSUE DATE:	08 January 2009	**EFFECTIVE DATE:**	09 January 2009
RESCINDS:	G09-01		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directives sets forth the Department's policy to identify and address emerging and chronic crime and disorder problems. Department members will refer to the Special Order titled "**Chicago Alternative Policing Strategy**" for a detailed description of the Chicago Alternative Policing Strategy (CAPS).

II. POLICY

A. The Department will employ a strategy to identify and address emerging and chronic crime and disorder problems that reflects its mission statement:

"The Chicago Police Department, as part of, and empowered by the community, is committed to protect the lives, property and rights of all people, to maintain order, and to enforce the law impartially. We will provide quality police service in partnership with other members of the community. To fulfill our mission, we will strive to attain the highest degree of ethical behavior and professional conduct at all times."

B. The Department will act in a unified manner to ensure the effective implementation of CAPS.

C. The Department's response to emerging and chronic crime and disorder will be comprehensive and consistent with all aspects of the mission statement.

III. CHICAGO ALTERNATIVE POLICING STRATEGY

A. The Chicago Alternative Policing Strategy (CAPS) is a comprehensive citywide plan of action intended to identify and address emerging and chronic crime and disorder problems. It results from a planning process that requires the involvement of the community, the Department's development of problem-specific district plans, and the cooperation of other City service agencies.

B. CAPS is characterized by:

1. an organizational model that promotes team work at all levels.
2. the Department working in partnership with the community and other City service agencies.
3. the use of beat, district, and area level problem-solving and planning processes.
4. impartial enforcement of the law.
5. prompt response to serious crime and life-threatening emergencies.
6. the Department engaging in proactive problem solving related to both emerging and chronic crime and neighborhood disorder.
7. time management techniques that support problem solving.
8. use of technology to collect and analyze data at the beat, district, and area level to support problem solving.
9. support of beat-level problem solving by district and other Department members.

10. receiving, analyzing, and addressing community concerns as brought forward by the community.

Jody P. Weis
Superintendent of Police

08-123 MWK/jkh

Chicago Police Department

General Order G02-04

PROHIBITION REGARDING RACIAL PROFILING AND OTHER BIAS BASED POLICING

ISSUE DATE:	22 February 2012	**EFFECTIVE DATE:**	22 February 2012
RESCINDS:	Version dated 27 April 2001; G01-04		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. further defines Department policy regarding the proper treatment of all persons by Department members.

B. specifically prohibits "racial profiling" and other bias based policing.

II. POLICY

A. The Chicago Police Department expressly prohibits "racial profiling" and "other bias based policing."

B. The Chicago Police Department is committed to observing, upholding and enforcing all laws relating to the individual rights of all persons. Department members will respect and protect each person's human rights and comply with all laws relating to human rights.

C. In addition to respect for those human rights prescribed by law, Department members will treat all persons with the courtesy and dignity which is inherently due every person as a human being. Department members will act, speak and conduct themselves in a professional manner, and maintain a courteous, professional attitude in all contacts with the public.

D. It is a fundamental duty of every Chicago Police Officer to be vigilant in the investigation of unusual or suspicious occurrences; to detect violations of the law; to safeguard lives and property; to guarantee all persons fair and equal treatment under the law; and to ensure that the rights of all persons are protected. In meeting these duties the Department remains committed to working actively with all communities within the City.

III. INDIVIDUAL RESPONSIBILITIES

A. Members of the Chicago Police Department are expressly prohibited from engaging in "racial profiling" and "other bias based policing" activities.

B. Members will not use the actual or perceived race, ethnicity, color, national origin, ancestry, gender, religion, disability, sexual orientation, marital status, parental status, military discharge status, financial status or lawful source of income, of any person, as the sole basis for developing reasonable suspicion or grounds for a traffic or street stop, or in deciding upon the scope and substance of post-stop actions.

C. Members, when determining if reasonable suspicion for a traffic or street stop exists, or when developing probable cause for an arrest, may consider the factors listed in Item II-B of this directive when one or more of those factors are part of the description of a known or suspected offender wanted in connection with a specific criminal or quasi-criminal incident.

D. Members must be able to clearly articulate the specific police or public safety purpose of any traffic or street stop.

E. Members will immediately report any observed violations of the policies and procedures established under this directive to a Department supervisor.

IV. SUPERVISORY RESPONSIBILITIES

A. Supervisors will monitor the adherence to the policies and procedures established under this directive by all subordinates.

B. Supervisors will initiate an investigation, in accordance with the procedures established under the directive entitled, "**Complaint and Disciplinary Procedures**," into all:

1. violations of the policies and procedures established under this directive that are directly observed.

2. allegations of a violation of the policies and procedures established under this directive received from any person.

V. TRAINING

A. The *Deputy Chief*, Education and Training Division will ensure that the policies and procedures established under this directive are fully incorporated into:

1. the basic recruit training curriculum.

2. all in-service training regarding courtesy and demeanor, determining reasonable suspicion, establishing probable cause for arrest, the rights of the accused, search and seizure and related courses.

B. *Station supervisors* will ensure that all roll call training is fully consistent with the policies and procedures established under this directive.

(Items indicated by *Italic/double underline* were added or revised)

Authenticated by: RMJ

Garry F. McCarthy
Superintendent of Police

00-082/12-003 TJL(JAB)TRH

GLOSSARY TERMS:

1. **Racial Profiling**

Any arrest, detention, interdiction, or other law enforcement action that is based solely on the actual or perceived race, ethnicity, color, national origin or ancestry of the targeted person.

2. **Other Bias Based Policing**

Any arrest, detention, interdiction, or other law enforcement action that is based solely on the actual or perceived gender, religion, disability, sexual orientation, marital status, parental status, military discharge status, financial status or lawful source of income of the targeted person.

Chicago Police Department

General Order G03-05

VIDEO SURVEILLANCE TECHNOLOGY

ISSUE DATE:	22 February 2012	**EFFECTIVE DATE:**	22 February 2012
RESCINDS:	Version dated 14 April 2011; G11-03		
INDEX CATEGORY:	Field Operations		

I. GUIDING PRINCIPLES

A. The use of video surveillance technology can provide members with an invaluable instrument to increase their safety and enhance criminal prosecution by providing powerful evidence of criminal activity. Consistent with the mission of the Chicago Police Department, the Department will implement video surveillance technology as part of its anti-crime strategy to:

1. enhance public safety and security in public areas, while reducing the fear of crime.
2. prevent, deter, and identify criminal activity, identify suspects, and gather evidence.
3. target areas of gang and narcotics activity on the public way. Target areas are identified using information gathered from narcotics-related calls for service, public-violence incidents, community input and complaints, and Department analysis and intelligence. Taken together, this information provides a clear picture of the areas in greatest need of police video surveillance.
4. observe prescheduled public events for approved investigative purposes (e.g., Taste of Chicago, parades, protests).
5. assist districts, units, and tactical personnel in criminal investigations (e.g., narcotics, thefts, covert operations).
6. respond to major critical incidents.
7. document officer conduct during citizen interactions and police actions to safeguard the rights of the public and police officers, protect against unwarranted citizen complaints, and limit civil liabilities.
8. reduce the cost and impact of crime to a community.
9. improve the allocation and deployment of Department resources.

B. The use of video surveillance technology will be conducted in a professional and ethical manner, within accepted legal concepts regarding privacy. All information and recorded images obtained through the use of video surveillance technology will be used strictly for law enforcement purposes and will be preserved with utmost integrity and confidentiality consistent with Department policy and legal rules governing the handling of evidence and criminal justice records.

C. The design, implementation, and enhancement of any Department video surveillance technology will recognize legal parameters that both limit and expand the use of cameras in the public space.

II. GENERAL GUIDELINES

A. Department members will receive training concerning the First Amendment, the Fourth Amendment, consent-to-search issues, and the proper operation of the video surveillance equipment prior to being authorized to use any Department-authorized video surveillance technology.

B. When using any video surveillance technology, Department members will:

1. only use Department-approved equipment and have a proper law enforcement purpose. **No unauthorized recording, viewing, reproduction, retention, or distribution is permitted.**

2. conform to all laws applicable to the use of video surveillance technology, including viewing and recording images consistent with the First and Fourth Amendment.

3. only monitor public areas and public activities where no legally protected reasonable expectation of privacy exists (e.g., street, sidewalk, park).

4. except while investigating a crime committed by a person whose description is known, not base an investigation or the use of video enhancement or tracking capabilities on individual characteristics or classifications including, but not limited to, race, gender, sexual orientation, national origin, or disability.

NOTE: Department members will continue to adhere to the polices and guidelines outlined in the Department directives entitled "**Prohibition Regarding Racial Profiling and Other Bias-Base Policing**" and "**The First Amendment and Police Actions**."

5. follow the procedures outlined in the video surveillance technology training.

C. The appropriate bureau *chief* may authorize the use of additional video surveillance technology or deviations from this policy by specialized units under their command provided that the technology and/or deviations are in compliance with all laws applicable to the use of video surveillance technology, including viewing and recording images consistent with the First and Fourth Amendment.

1. This authorization will be in the form of a unit-level directive providing specific justifications and the recommended usage, retention, and auditing guidelines.

2. Copies of this authorization will be maintained in each bureau with copies forwarded to Public Safety Information Technology and the Office of Legal Affairs.

D. Supervisors commanding Department members assigned to use video surveillance technology will:

1. monitor subordinates to ensure the video surveillance technology is utilized according to all legal requirements, procedures set in this directive, and the training provided. Any discrepancies or conflicts will be brought to the attention of the *station supervisor or designated unit supervisor* for resolution.

2. appropriately document the monitoring of video surveillance technology usage including any instances of additional training, corrective measures, or disciplinary actions.

(Items indicated by *italic/double underline* were added or revised)

Authenticated by: RMJ

Garry F. McCarthy
Superintendent of Police

10-175/12-003 mwk/TRH

Chicago Police Department

Special Order S02-03

CHICAGO ALTERNATIVE POLICING STRATEGY (CAPS)

ISSUE DATE:	08 January 2009	**EFFECTIVE DATE:**	09 January 2009
RESCINDS:	G09-01		
INDEX CATEGORY:	Human Rights and Community Partnerships		

I. PURPOSE

This directive:

A. describes the Chicago Alternative Policing Strategy (CAPS). Department members will refer to the General Order titled "**Chicago Alternative Policing Strategy**" for the policy governing CAPS.

B. introduces the CAPS Manual.

II. CAPS MANUAL

A. This directive institutionalizes the CAPS Manual, which is available on the CAPS Implementation Office server on the Department Intranet.

B. The CAPS Manual is a supplement to the guidelines and policies set forth in this directive. It is comprised of two types of materials:

1. Resource documents designed to assist Department members to better fulfill their assigned CAPS duties.
2. CAPS Procedural Guidelines which promote a consistent and efficient implementation of CAPS.

C. In addition to the responsibilities established in this directive, Department members will adhere to the procedures delineated in the CAPS Manual.

D. The Director, CAPS Implementation Office, has the sole authority and responsibility to maintain the CAPS Manual, issue modifications to it, and revise the CAPS Procedural Guidelines as necessary.

Jody P. Weis
Superintendent of Police

08-123 MWK/jkh

ADDENDA:

1. S02-03-01 - Departmental Unit CAPS Responsibilities
2. S02-03-02 - District Plans
3. S02-03-03 - Building Partnerships with the Community
4. S02-03-04 - City Service Requests
5. S02-03-05 - Domestic Violence Liaison Officer (DVLO)
6. S02-03-06 - Court Advocacy Subcommittee

Chicago Police Department

Special Order S05-08

HOMELAND SECURITY AND ANTI-TERRORISM PREPARATIONS

ISSUE DATE:	06 December 2004	**EFFECTIVE DATE:**	06 December 2004
RESCINDS:	G04-04		
INDEX CATEGORY:	Extraordinary Responses		

I. PURPOSE

This directive:

A. informs Department members of the terrorism threat classifications provided under the Homeland Security Advisory System operated by the United States Department of Homeland Security.

B. outlines the Department's Homeland Security coordination procedures intended to enhance the Department's anti-terrorism preparations and response.

C. introduces the Department's Homeland Security Reference Manual (HSRM).

II. GENERAL INFORMATION

A. While the specific day-to-day duties of the Department's various units and personnel vary, each member shares in a collective responsibility for the effectiveness of the Department's response to potential terrorist threats and actual terrorism incidents. Ensuring an effective response requires the coordinated use of its administrative support, planning, training, patrol, investigative, and intelligence resources.

B. Overall command authority with respect to the Department's anti-terrorist response rests with the Superintendent of Police and, unless modified by the Superintendent, is delegated as follows:

1. Command authority over the Department's operational and field response to a potential terrorist threat or actual terrorist incident rests with the Assistant Superintendent, Operations. In the absence of the Assistant Superintendent, Operations, the ranking member of the Bureau of Patrol then assigned or supervising the incident shall be in command.

2. Command authority with respect to the coordination of the Department's anti-terrorism intelligence analysis and responsibility to coordinate the Department's overall anti-terrorism planning and preparation rests with the Deputy Superintendent, Bureau of Investigative Services.

C. Unless specifically modified by the provisions of this directive, the overall operational response to an actual terrorist incident by Department members will be consistent with the procedures established under the existing directives appropriate to the incident, including those relating to emergency or special response plans, preliminary investigations, hazardous materials, critical incidents, school violence, HBT incidents, crime scene processing, processing arrestees, First Amendment activities, eavesdropping, searches, and field and custodial interviews and interrogations.

D. Based upon the severity or scope of a potential terrorist threat or actual terrorist incident, the Superintendent of Police or Assistant Superintendent, Operations may direct temporary or emergency modifications to the Department's directives or procedures as necessary to ensure the effectiveness of the Department's response.

III. HOMELAND SECURITY REFERENCE MANUAL

The Department's **Homeland Security Reference Manual** is a confidential document approved by the Superintendent of Police and prepared and regularly updated under the coordination of the Deputy Superintendent, Bureau of Patrol. The Homeland Security Reference manual:

A. contains anti-terrorist response planning and precautionary procedures and delineates specific duties for various Department units and members consistent with the terrorist threat warnings established under the Homeland Security Advisory System (HSAS) operated by the United States Department of Homeland Security.

NOTE: For additional information on the HSAS, refer to the Department directive entitled "**Homeland Security Advisory System**."

B. will be utilized to prepare response plans specific to the then-current terrorist threat level in Chicago.

C. is distributed on a restricted basis by the Deputy Superintendent, Bureau of Patrol, to selected command and other personnel as designated by the Superintendent.

Philip J. Cline
Superintendent of Police

04-099 MWK/MES/TJL(PMD)

ADDENDA:

1. S05-08-01 - Homeland Security Advisory System
2. S05-08-02 - Anti-Terrorism Preparations
3. S05-08-03 - Terrorism Liaison Officer (TLO) Program

Chicago Police Department

Special Order S05-08-01

HOMELAND SECURITY ADVISORY SYSTEM

ISSUE DATE:	06 December 2004	**EFFECTIVE DATE:**	06 December 2004
RESCINDS:	G04-04-01		
INDEX CATEGORY:	Extraordinary Responses		

I. PURPOSE

This directive:

A. informs Department members of the terrorism threat classifications provided under the Homeland Security Advisory System operated by the United States Department of Homeland Security.

B. Delineates responsibilities of Department members relative to the various threat condition levels as designated by the HSAS.

II. GENERAL INFORMATION

The Homeland Security Advisory System (HSAS) operated by the United States Department of Homeland Security (USDHS) provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to federal, state, and local authorities and to the American people. The higher the Threat Condition Level, the greater the risk of a terrorist attack, including both the probability of an attack occurring and its potential gravity. Threat Condition Levels are assigned by the Secretary of the USDHS. From lowest to highest, the Threat Condition Levels are:

A. Low (Green)-Low risk of terrorist attacks;

B. Guarded (Blue)-General risk of terrorist attacks;

C. Elevated (Yellow)-Significant risk of terrorist attacks;

D. High (Orange)-High risk of terrorist attacks;

E. Severe (Red)-Severe risk of terrorist attacks.

III. RESPONSIBILITIES

The Assistant Superintendent, Operations or, in their absence, Deputy Superintendent, Bureau of Patrol, will notify Department members of the Department's response to a change in the Threat Condition Level for the Chicago area via an Administrative Message Facsimile Network (AMFN) message.

A. When the HSAS designates a **Threat Condition Level of Low (Green), Guarded (Blue), or Elevated (Yellow)** and unless otherwise directed by the Superintendent of Police or Assistant Superintendent, Operations:

1. Sworn members will be assigned to duties that are consistent with the Department's Homeland Security Reference Manual based upon the then-current threat level. Additionally those sworn members who:

   a. are specifically assigned anti-terrorism related duties will engage in activities that focus on enhancing the Department's general preparedness, intelligence, enforcement, and counter-terrorism capabilities.

      NOTE: This includes, but is not limited to, Special Weapons and Tactics (SWAT), Mobile Strike Force, or Targeted Response Unit, Special Functions Group, and the Bomb and Arson Section of the Detective Division, Bureau of Investigative Services.

   b. are **not** specifically assigned anti-terrorism related duties will report and carry out their duties consistent with the normal procedures relating to their assignments.

      NOTE: Refer to the parent order of this directive for additional information concerning the Department's Homeland Security Reference Manual.

2. Notifications regarding potential or actual terrorist threats will be made to Operations Command.

B. When the HSAS designates a **Threat Condition Level of High (Orange)**:

1. The Assistant Superintendent, Operations, will provide on-going recommendations to the Superintendent of Police as to the specific scope of field deployment needed relative to the "High" Threat Condition Level.

2. Sworn members:

   a. will be briefed by the watch commander regarding the general nature of the then-present threat and advised of those patrol areas or locations in need of special attention.

   b. will be assigned to duties that are consistent with the Department's Homeland Security Reference Manual.

3. Those sworn members who:

   a. are specifically assigned anti-terrorism-related duties will engage in activities that focus on enhancing the Department's specific preparedness, intelligence, and enforcement capabilities relative to the "High" Threat Condition Level.

   b. are **not** specifically assigned anti-terrorism-related duties, that are assigned to:

      (1) Bureau of Investigative Services (BIS) or field units of the Internal Affairs Division (IAD) must have their uniform, helmet, and other required equipment accessible such that they could be placed in uniform, equipped, and field deployed within one hour.

(2) all other units will be required to work in uniform and have readily available their helmets and any other required equipment as designated in the AMFN message relative to the "High" Threat Condition Level.

4. The Headquarters Command Post will be activated and manned at the direction of the Assistant Superintendent, Operations, or Deputy Superintendent, Bureau of Patrol.

5. Notifications regarding potential or actual terrorist threats will be made to the Headquarters Command Post on a twenty-four-hour basis and to the OEMC Command Center when the OEMC Command Center is in operation.

C. When the HSAS designates a **Threat Condition Level of Severe (Red)**:

1. The Assistant Superintendent, Operations, will provide on-going recommendations to the Superintendent of Police as to the specific scope of field deployment needed relative to the "Severe" Threat Condition Level. Consistent with the Department directive entitled "**Special Response Plans**," such deployment need may require the implementation of a:

   a. "Plan Red" relative to the special field deployment of on-duty personnel.

   b. "Plan Blue" relative to the recall and field deployment of off-duty personnel.

   NOTE: Only the Superintendent, Assistant Superintendent, Operations, or the Deputy Superintendent, Bureau of Patrol, may activate a Special Response Plan.

2. Sworn members:

   a. will be briefed regarding the general nature of the then-present threat and advised of those patrol areas or locations in need of special attention.

   b. will be assigned to duties that are consistent with the Department's Homeland Security Reference Manual.

3. Those sworn members who:

   a. are specifically assigned anti-terrorism-related duties will engage in activities that focus on enhancing the Department's specific preparedness, intelligence, enforcement, and counter terrorism capabilities relative to the "Severe" Threat Condition Level.

   b. are **not** specifically assigned anti-terrorism-related duties will be required to work in uniform and have readily available their helmets and any other required equipment as designated in the AMFN message relative to the "Severe" Threat Condition Level.

4. The Headquarters Command Post will be activated and manned at the direction of the Assistant Superintendent, Operations, Deputy Superintendent, Bureau of Patrol, or the Assistant Deputy Superintendent, Special Functions Group.

5. Notifications regarding potential or actual terrorist threats will be made to Headquarters Command Post on a twenty-four-hour basis and to the OEMC Command Center when the OEMC Command Center is in operation.

Philip J. Cline
Superintendent of Police

04-099 MWK/MES/TJL(PMD)

Chicago Police Department

Special Order S05-08-02

ANTI-TERRORISM PREPARATIONS

ISSUE DATE:	06 December 2004	**EFFECTIVE DATE:**	06 December 2004
RESCINDS:	G04-04-02		
INDEX CATEGORY:	Extraordinary Responses		

I. PURPOSE

This directive outlines the Department's Homeland Security coordination procedures intended to enhance the Department's anti-terrorism preparations and response.

II. GENERAL INFORMATION

The following teams under the command of the Deployment Operations Center have specific anti-terrorism responsibilities:

A. **Counter Terrorism Section (CTS)** - is an intelligence-gathering section within the Deployment Operations Center. Department members assigned to the CTS are responsible for:

1. gathering and disseminating intelligence relevant to both domestic and foreign terrorism in a timely manner.
2. cataloging and conducting analysis of all Department reports that contain information relevant to terrorist threats.
3. participating in vulnerability assessments of the key assets and critical infrastructure of the City of Chicago and maintaining the Department's database of these assessments.
4. functioning as Department liaison with federal, state, and local law enforcement agencies concerning the sharing of intelligence and information relevant to terrorist threats.
5. producing a daily briefing sheet containing information on incidents that have occurred within the previous twenty-four hours, information on topics of local and international homeland security interests, and future planned events.

B. **Joint Terrorist Task Force (JTTF)** - is a multi-agency investigative unit involving personnel/officers from the Chicago Police Department, Federal Bureau of Investigation, Department of Defense, Naval Intelligence, Immigration and Customs Enforcement, Secret Service, Illinois State Police, Army Criminal Investigative Unit, Coast Guard, United States Postal Service Postal Inspections, Cook County Sheriffs's Office, and other federal, state, and local law enforcement agencies. The JTTF members combine efforts and resources by working collectively on investigations concerning domestic and foreign terrorist threats in a unified defense of homeland security. Department members assigned to the JTTF are responsible for:

1. functioning as the lead investigative team for the Department on investigations concerning domestic and foreign terrorist threats.
2. receiving copies of all intelligence and information reports concerning domestic and foreign terrorist threats for investigation and analysis by the JTTF Field Intelligence Group.

III. HOMELAND SECURITY COMMITTEE

To promote the efficient use of Department resources and enhance the Department's anti-terrorism preparedness, the Homeland Security Committee shall:

A. consist of the following members:

1. Assistant Superintendent, Operations, who will serve as the committee chairperson.
2. Deputy Superintendent, Bureau of Patrol, who will serve as the committee vice-chairperson.
3. Deputy Superintendent, Bureau of Investigative Services.
4. Deputy Superintendent, Bureau of Administrative Services.
5. Chief, Counterterrorism and Intelligence Division.
6. Deputy Chief, Counterterrorism and Intelligence Division.
7. Commander, Intelligence Section.
8. Commander, Deployment Operations Center, who will serve as the committee secretary.

B. meet when necessary to review resource, funding, planning, and training proposals relating to anti-terrorism preparedness.

C. through the committee chairperson, make recommendations concerning anti-terrorism preparedness to the Superintendent of Police.

IV. ADDITIONAL RESPONSIBILITIES

A. The Deputy Superintendent, Bureau of Investigative Services, will:

1. serve as the Department's homeland security liaison to:

a. the Office of Emergency Management and Communications (OEMC).

NOTE: For all other matters the Department's OEMC liaison will be the Deputy Superintendent, Bureau of Administrative Services or such other command staff member as designated in the directive entitled "**Department Organization for Command**."

b. those federal and state agencies charged with homeland security responsibilities.

2. coordinate the preliminary review of all major Department homeland security requests, including but not limited to the following:

a. Organizing meetings concerning any planning, discussion, or coordination of any specific, major special event which may be impacted by an advanced terrorist threat level. The review of such requests will be in conjunction with the Assistant Superintendent, Operations, and the Deputy Superintendent, Bureau of Patrol.

b. Funding requests related to homeland security, including equipment and training. The review of such requests will be in conjunction with the Deputy Superintendent, Bureau of Administrative Services, command staff member of the Research and Development Division, and the Director, Finance Division.

c. Training under the scope of homeland security. The review of such requests will be in conjunction with the Assistant Deputy Superintendent, Education and Training Division.

3. set the agenda of the Homeland Security Committee to consist of those homeland security preparedness proposals meriting the committee's attention and potentially the approval of the Superintendent of Police.

4. oversee the preparation, regular update, submission to the Superintendent of Police for approval, and restricted distribution of the Department's Homeland Security Reference Manual.

NOTE: Refer to the Department directive entitled "**Homeland Security and Anti-Terrorism Preparations**" for additional information concerning the Homeland Security Reference Manual.

5. ensure the Department's anti-terrorism response plans are designed and implemented consistent with the United States Department of Homeland Security's National Incident Management System (NIMS).
6. oversee the anti-terrorism intelligence gathering and analysis capabilities of the Department.
7. designate a Weapons of Mass Destruction (WMD) Coordinator.

B. The Commander, Deployment Operations Center will assign and oversee the activities of personnel responsible for:

1. reviewing, analyzing, reporting, and disseminating, as appropriate, terrorism-related intelligence reports and information.
2. participating in the various anti-terrorism task forces, to include the JJTF, and assisting in anti-terrorism enforcement.
3. participating in the coordination conducted by the Office of Emergency Management and Communications with the management of critical facilities located in Chicago concerning specific terrorist threats and threat mitigation procedures.

C. The Weapons of Mass Destruction (WMD) Coordinator will:

1. coordinate security clearance concerns and WMD matters with the following Federal agencies:
   a. Federal Bureau of Investigations (FBI).
   b. Centers for Disease Control (CDC).
   c. Department of Defense (DOD).
   d. Department of Energy (DOE).
   e. Department of Health and Human Services (DHHS).
   f. Environmental Protection Agency (EPA).
   g. Federal Emergency Management Agency (FEMA).
   h. US Attorney's Office.
2. work directly with the Federal Bureau of Investigations, Chicago Division WMD Coordinator, and designated WMD representative from the US Attorney's Office for the Northern District of Illinois.
3. identify the needs and research appropriate requests for equipment and training of first responders.
4. attend and participate in terrorist threat intelligence conferences and disseminate, as appropriate, WMD-related materials and information.
5. brief the Deputy Superintendent, Bureau of Investigative Services on daily intelligence bulletins.
6. coordinate emergency preparedness and planning initiatives regarding WMD terrorism with the designated district Terrorism Liaison Officers, JTTF, CTS, and the CAPS Implementation Office.
7. coordinate such other WMD-related activities as assigned by the Deputy Superintendent, Bureau of Investigative Services.

D. District Terrorism Liaison Officers:

1. are recommended for selection by the Deputy Superintendent, Bureau of Patrol and appointed by the Deputy Superintendent, Bureau of Investigative Services.
2. participate in briefings and training sessions as directed.
3. serve as supplemental information and training resource for their assigned districts.

E. Department members will:

1. be alert and vigilant to suspicious activities and circumstances that suggest the presence of a potential terrorist threat.
2. immediately, upon the approval of their unit commanding officer or watch commander, fax a copy of all information reports in which the subject is terrorism or homeland security to the Deployment Operations Center.
3. perform such other duties as defined in the Department directive entitled "**Homeland Security Advisory System**."

Philip J. Cline
Superintendent of Police

04-099 MWK/MES/TJL

Chicago Police Department

Special Order S05-08-03

TERRORISM LIAISON OFFICER (TLO) PROGRAM

ISSUE DATE:	16 September 2009	**EFFECTIVE DATE:**	17 September 2009
RESCINDS:	S09-13		
INDEX CATEGORY:	Extraordinary Responses		

I. PURPOSE

This directive:

A. informs Department members of the Terrorism Liaison Officer (TLO) Program.

B. delineates the responsibilities of the:

1. Terrorism Liaison Officer.
2. District Watch Commanders.
3. supervisor assigned to the TLO program.

II. GENERAL INFORMATION

A. The Terrorism Liaison Officer (TLO) Program is under the direction of the Counter Terrorism Section (CTS) of the Deployment Operations Center (DOC) Section.

B. The TLO Program is established to afford an opportunity for the sharing of information pertaining to Homeland Security issues to all bureaus/units of the Chicago Police Department.

C. A member's rank has no bearing on their ability to be a TLO. Members with a military background and/or experience in intelligence gathering are preferred, but it is not required. However an interest in Homeland Security is required.

D. Terrorism Liaison Officers are chosen from each district and units with investigative or patrol functions. Districts and units may assign more than one member to be designated as a TLO.

III. RESPONSIBILITIES

A. Terrorism Liaison Officer

1. Sworn members assigned as a Terrorism Liaison Officer will:

a. act as liaison for their respective district / unit regarding Homeland Security issues.

b. establish and maintain an open line of communication with key personnel at critical facilities within their district / unit.

c. attend quarterly TLO meetings to discuss critical information concerning Homeland Security and the TLO program.

d. upon attending the TLO meeting, prepare a report for their watch commander / unit commanding officer regarding information from the TLO meeting.

e. attend CPD Area TLO Meetings to discuss critical information concerning Homeland Security pertaining to the districts within the Area.

f. upon attending the CPD Area TLO meeting, prepare a report for their watch commander / unit commanding officer regarding information from the CPD Area TLO meeting.

g. review reports from their units which pertain to Homeland Security and forward them to the CTS.

h. distribute literature to inform members of their unit relating to Homeland Security threats.

2. TLOs assigned to specialized units (e.g., Vice Control Section, Narcotics Section, and Gang Investigation Section) will assist the district TLOs when necessary.

B. Watch Commanders will ensure:

1. TLOs attend meetings or training.

NOTE: Watch commanders will allow TLOs to adjust their duty hours or days off to attend meetings or training, as long as such action does **NOT** adversely affect manpower needs.

2. a copy of the TLOs report from the quarterly TLO meeting is available for officers in their respective district/unit.

3. upon approval, the TLO report is forwarded to their district commander / unit commanding officer of command staff rank.

C. Unit commanding officers will ensure that the information from the TLO report is disseminated to the following for distribution to their respective personnel, including:

1. watch commanders.

2. tactical lieutenants.

3. area CAPS lieutenant.

D. The supervisor assigned to direct the TLO program will:

1. maintain a database of TLOs by district / unit.

2. coordinate and attend the Area TLO meetings.

3. prepare an agenda and take minutes for each TLO meeting.

4. forward pertinent information to TLOs between meetings (special bulletins, etc).

5. when possible, visit critical facilities with TLOs.

6. distribute information to officers and citizens to increase their awareness to Homeland Security issues with the assistance of TLOs.

7. ensure a quarterly meeting is held with citywide TLOs to discuss critical information concerning Homeland Security and the TLO program.

8. coordinate a TLO certification program with the Education and Training Division.

9. record and document all TLO specific training.

Jody P. Weis
Superintendent of Police

07-149 SEP

OBSERVATION VAN

ISSUE DATE:	14 April 2011	**EFFECTIVE DATE:**	14 April 2011
RESCINDS:	S11-06		
INDEX CATEGORY:	Department Vehicles		

I. PURPOSE

This directive:

A. continues the use of the Observation Van (OV) and provides certain definitions relative to its use.

B. provides procedures, duties, and responsibilities for deploying the OV and the storage and inventory of video images captured by the OV.

C. continues the:

1. Observation Van Deployment/Video Retrieval Request form (CPD-21.958).
2. Observation Van Worksheet Log (CPD-21.959).

II. GENERAL INFORMATION

A. The Observation Van is a specially modified vehicle, operated and managed by the Office of Emergency Management and Communications (OEMC), Public Safety Information Technology (PSIT), that can operate in all weather conditions to provide live video and recording capabilities, enabling Department members to view multiple feeds from:

1. a **mast camera** that is connected to the OV's mast mount. This camera can be used in all weather and lighting conditions and has the ability to be controlled from inside the OV with 360 degree pan, tilt, and zoom capabilities.
2. **remote satellite cameras** that have the same functionality as the mast camera and can be mounted within a half-mile distance of the OV.

B. All images recorded by the OV cameras are stored on individual digital video recorders (DVRs) connected to each camera. In the absence of a written request to save and inventory video images, all recordings from the DVRs, at the discretion of the Managing Deputy Director, Public Safety Information Technology (PSIT), may be deleted after 60 days.

C. The Observation Van has no audio recording capabilities.

D. All requests to deploy the OV, regardless of being granted or denied, will proceed through the chain of command and be forwarded to the Managing Deputy Director, PSIT.

III. PROCEDURES FOR REQUESTING THE DEPLOYMENT OF THE OV

A. Deployment of the OV During Major Critical Incidents

1. A unit commanding officer requesting the deployment of the OV during a major critical incident will request verbal approval from the appropriate Bureau of Patrol area deputy chief.
2. If approved, the appropriate Bureau of Patrol area deputy chief will immediately contact the Managing Deputy Director, PSIT, for van deployment.
3. All verbal requests approved by the appropriate area deputy chief must be followed by the completion of the Observation Van Deployment/Video Retrieval Request form which is to be forwarded within 24 hours of the incident consistent with the procedures set forth in this directive.

B. Concurrent Deployment with Command Van

1. If the Command Van is deployed to a critical incident consistent with Bureau of Patrol procedures, and with the approval of the appropriate area deputy chief, the OV will be deployed to the same incident.

2. The Operations Command Unit will notify the Managing Deputy Director, PSIT, who will deploy the Observation Van consistent with the procedures set forth in this directive, ensuring that the Observation Van Deployment/Video Retrieval Request form is completed.

C. If the Office of Legal Affairs, the Bureau of Professional Standards, or the Internal Affairs Division requests filming of a preplanned event, the Superintendent's approval is required.

IV. OTHER RESPONSIBILITIES

A. By agreement, the Managing Deputy Director, PSIT, will:

1. ensure that qualified personnel are trained to operate and deploy the OV.
2. be responsible for coordinating pre-event site surveys.
3. ensure the integrity of all recorded images.
4. review requests to hold and authorize video images to be copied after receiving a request.
5. maintain all completed Observation Van Deployment/Video Retrieval Request forms according to Department records-retention requirements.

B. By agreement, personnel assigned to PSIT will:

1. complete the Observation Van Worksheet Log and submit for approval to the Managing Deputy Director, Public Safety Information Technology.
2. when downloading images onto a recordable (e.g., CD or DVD) format and an RD number has been obtained, complete and submit a Supplementary Report (CPD-11.411-A) and include the following information in the report:
   a. the names of the officers who were operating the controls in the OV.
   b. the name of the officer that downloaded the images and the date and time the download was completed.
   c. a brief description of the images being recorded.
3. inventory one copy of the recording and retain one copy at PSIT.
4. if there is no RD number attached to the event, record the above information on a To-From-Subject report and forward it through the chain of command to the Managing Deputy Director, PSIT.

C. The General Counsel to the Superintendent will review each written request for the OV and determine if the request for the OV could potentially fall into the parameters of a First Amendment investigation consistent with the Department directive entitled "**The First Amendment and Police Actions**."

V. VIDEO RETRIEVAL REQUEST PROCESS

A. Requests for the retrieval of video images will be initiated by a command staff member, who will complete an Observation Van Deployment/Video Retrieval Request form and forward it through their chain of command to the Managing Deputy Director, PSIT. A copy of the request will be forwarded to the General Counsel to the Superintendent.

B. The Managing Deputy Director, PSIT, will complete and distribute appropriately all approved requests.

Terry G. Hillard
Interim Superintendent of Police

10-175 mwk

INTELLIGENCE SECTION **Special Order**	Date of Issue **8 September 2008**	Effective Date	No. 08-01
Subject Investigation Initiation Procedures		Amends	
Related Directives		Rescinds	

- If an Intelligence Section member wants to initiate an investigation on a subject or a location in which a significant amount of resources or time will be expended, he/she will submit a report in writing through his/her chain to the Intelligence Section commander

- The initiation report will be in the format as noted on the attached (INT SO #08-01 – Att. 1). If approved by the commander, the report will be given to the unit secretary to be assigned an "initiation number" ("I" number).

- The "I" number will be sequentially based and obtained from the "Initiation Number" log book for the unit. Format for the initiation number is as follows: four digit year – INT – three digit sequential number: Example: 2008-INT-001. The unit secretary will then note the "I" number in the log book. The log book entry will contain spaces for the following information: "I" number, requesting member's name, requesting member's sergeant's name, date assigned and date closed.

- The number will be noted on the initiation report bearing the commander's signature in the space provided and a copy of the report will be given to the requesting member's sergeant.

- A case file for the "I" number will be started at the time an "I" number is assigned. The file will be kept in a locked file cabinet in the unit secretary's office. Kept in this file will be any reports associated with the investigation with the "I" number referenced on each report. Originals of any reports, except for case/supplementary reports, will be kept in this file. Case/supplementary report originals will be processed in accordance with Department procedures and only copies of case/supplementary reports will be kept in the unit case files.

- If an investigation is of a confidential nature and a records division number is needed, a member will complete a General Offense Case or Vice Control Case Report. The address of occurrence will be 99 S. Confidential and the narrative will indicate that further information can be found in supplementary reports. In confidential investigations, supplementary report originals will be kept in the file until the time that the investigation is closed. At that time, supplementary report originals will be processed in accordance with Department procedures.

- Only the unit commanding officer or person specifically authorized by the commanding officer are allowed to remove paperwork from the unit case files.

INTELLIGENCE SECTION **Special Order**	Date of Issue **8 September 2008**	Effective Date	No. 08-01 Att. 1
Subject Investigation Initiation Procedures Attachment		Amends	
Related Directives INT SO 08-01 Investigation Initiation Procedures		Rescinds	

Bureau of Strategic Deployment (Date)
Counterterrorism and Intelligence Division
Intelligence Section

To: Commander
Intelligence Section

From: PO _____ Star #
Intelligence Section

Subject: REQUEST TO INITIATE AN INVESTIGATION I # ASSIGNED: _____

Target: (subject)
(First Name, LAST NAME) (IR#) (IDOC #) (FBI#)
(DOB)
(LKA) (District)
(Gang Affiliation)
(Primary geographic location(s) where he/she conducts criminal activity

(address)
(Address)
(District)

Criminal Activity: Examples: Gun Runner, Marijuana Dealer, Mortgage Fraud, etc.
Site of possible fencing operation

HIDTA Deconfliction: (#) (on date)

Assigned Case Officer(s):

Synopsis of Information:

_____
PO

APPROVED:

_____
Sergeant

_____
Lieutenant

_____
Commander

INTELLIGENCE SECTION **Special Order**	Date of Issue **8 September 2008**	Effective Date	No. 08-02
Subject Handling Electronic Evidence		Amends	
Related Directives		Rescinds	

- **DEFINITION OF ELECTRONIC EVIDENCE**
  Any information stored or transmitted in a digital format which can be of evidentiary value in a criminal or civil court proceeding.

- **PROCEDURES FOR HANDLING ELECTRONIC EVIDENCE**

  Members will ensure that any device they use to capture electronic evidence is set up to accurately reflect the correct date and time.

  Digital Photos
  Digital photos are captured on a camera's memory flash card. Never capture photos from separate investigations on the same memory flash card. Digital photos will be processed according to the following procedures:

- The camera containing a memory flash card used in the course of an investigation will be taken to the Organized Crime Division's (OCD) Technical Support Group offices.
- An OCD Tech will download ALL of the images to a CD. This CD will be considered the original and additional copies will be made. Images are numbered in sequential order when they are captured, therefore, ALL images will be downloaded and not deleted prior to downloading.
- Once the OCD Tech downloads the memory flash card, the memory card can be cleared and used again.
- The original CD will be placed in a plastic evidence envelope and sealed with the case officer's signature. The original CD and a copy will be kept in the unit case file until such time that a Records Division (RD) number is obtained. The original CD will then be inventoried using that RD number.
- An Observation/Surveillance Report or if applicable, a Supplementary Report will be completed to document the taking of the images contained on the CD.

  Video Recordings
  Video recordings will either be captured utilizing a surveillance van or a hand held video camera. In either instance, the media ((DVD, mini disc, mini cassette or any other video device used) will be processed under the following procedures:
- The video device containing the recording or the recording will be taken to the OCD Technical Support Group offices.
- An OCD Tech will download the video to a DVD. This DVD will be considered the original. Additional copies will be made.
- The case officer will pick up and sign for the original DVD and copies. The original will be placed in a plastic evidence envelope and sealed with the case officer's signature. The original DVD and a copy will be kept in the unit case file until such time that an RD number is obtained. The original DVD will then be inventoried under that RD number.
- An Observation/Surveillance Report, or if applicable, a Supplementary Report will be completed to document the taking of the video.

INTELLIGENCE SECTION Special Order	Date of Issue 30 September 2008	Effective Date 30 September 2008	No. 08-03
Subject Intelligence Section Duties and Responsibilities		Amends	
Related Directives		Rescinds	

THE DUTIES AND RESPONSIBILITIES OF THE INTELLIGENCE SECTION INCLUDE, BUT ARE NOT LIMITED TO THE FOLLOWING:

- **CRIMINAL ENTERPRISE GROUP**

  PRODUCE A DETAILED HEIRARCHY FOR THE THREE TO FIVE TOP "CREWS" FOR TRADITIONAL ORGANIZED CRIME IN CHICAGO TO INCLUDE THE MOST INFORMED OPINION ON WHO IS BELIEVED TO BE THE SUBJECT WITH THE MOST POWER IN THE CHICAGOLAND AREA. THE HEIRARCHY SHOULD BE UPDATED AS INFORMATION WARRANTS IT.

  PREPARE A REPORT ON MOTORCYCLE GANGS WITH A DIRECT IMPACT ON CHICAGO TO INCLUDE MEMBERS, CLUBHOUSE LOCATIONS AND CRIMINAL ACTIVITY IN WHICH THEY ARE SUSPECTED TO BE ENGAGED. THIS REPORT SHOULD BE IN A FORMAT THAT WILL ASSIST INVESTIGATIVE UNITS IN THE EVENT A CRIME SHOULD OCCUR INVOLVING MOTORCYCLE GANG MEMBERS. THIS REPORT SHOULD BE CONTINUALLY KEPT CURRENT.

  CONDUCT INVESTIGATIONS TO MAKE ARRESTS AND DEVELOP ADDITIONAL INFORMANTS IN THESE GROUPS.

  ANALYZE EXISTING DETECTIVE DIVISION CRIME PATTERNS TO ASCERTAIN IF THE MANNER AND METHOD OF OPERATION CAN BE ATTRIBUTED TO ANY ORGANIZED CRIME GROUP. THIS INFORMATION SHOULD THEN BE SHARED WITH A SUPERVISOR FROM THE AFFECTED AREA DETECTIVE DIVISION TO ASSIST AREA PERSONNEL IN THEIR INVESTIGATION.

- **JOINT TERRORISM TASK FORCE (JTTF) TEAMS**

  JTTF MEMBERS CONDUCT FOLLOW UP INVESTIGATIONS CONCERNING DOMESTIC AND INTERNATIONAL TERRORISM CONCERNS AS REPORTED BY DEPARTMENT MEMBERS AND VIA OTHER MEANS. CPD MEMBERS ON THE JTTF PARTICIPATE IN INVESTIGATIONS WITH OTHER MEMBERS OF THIS FEDERAL BUREAU OF INVESTIGATION TASK FORCE IN ACCORDANCE WITH A MEMORANDUM OF UNDERSTANDING.

- **FIELD INVESTIGATION TEAMS (FIT)**

  DEVELOP INFORMANTS AND CULTIVATE INFORMATION THAT WILL RESULT IN REAL TIME INTELLIGENCE BEING OBTAINED ON SUBJECTS INVOLVED IN CRIMINAL ACTIVITY. THE INVESTIGATION WILL THEN PROCEED VIA ONE OF THREE WAYS:

INTELLIGENCE SECTION Special Order	Date of Issue 30 September 2008	Effective Date 30 September 2008	No. 08-03
Subject Intelligence Section Duties and Responsibilities		Amends	
Related Directives		Rescinds	

- **FIELD INVESTIGATION TEAMS (FIT)** (cont.)

1) INFORMATION WILL BE GIVEN TO THE APPROPRIATE INVESTIGATIVE UNIT FOR THEIR PURPOSES, TO BE HANDLED INTERNALLY WITHIN THEIR UNIT.

2) CONTINUE THE INVESTIGATION UTILIZING INTELLIGENCE SECTION PERSONNEL AND RESOURCES AS NEEDED. EXPERTISE AS TO HOW THE CASE SHOULD PROCEED WILL BE PROVIDED BY THE APPROPRIATE INVESTIGATIVE UNIT PERSONNEL.

3) INTELLIGENCE SECTION PERSONNEL WILL CONDUCT THE INVESTIGATION AND MAKE THE ARREST.

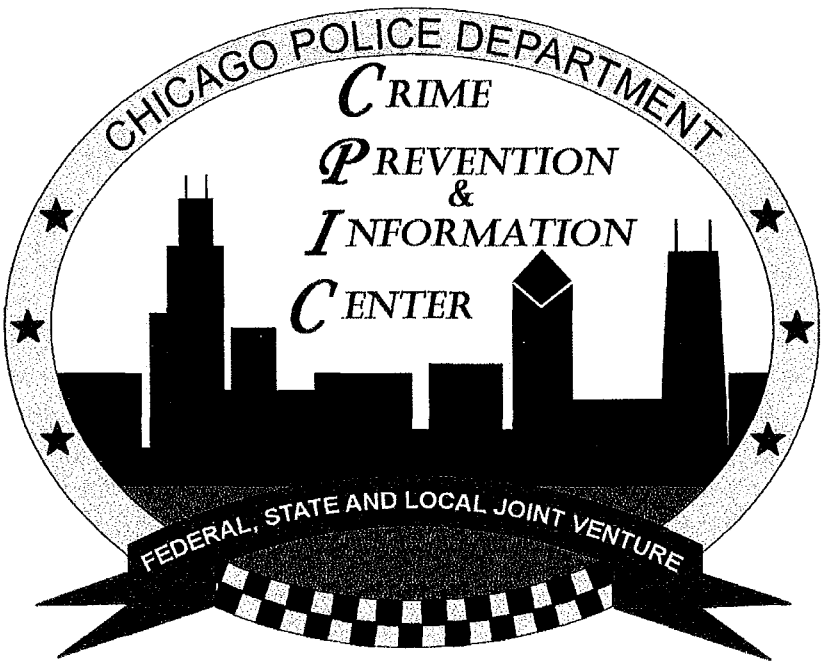
NOTE: THE DECISIONS AS TO HOW THE INFORMATION SHALL BE HANDLED WILL BE MADE BY INTELLIGENCE SECTION SUPERVISORS, AND THE APPROPRIATE INVESTIGATIVE UNIT SUPERVISORY PERSONNEL.

ASSIST JTTF TEAMS WITH PERSONNEL AND RESOURCES AS NEEDED TO SUPPLEMENT AND ENHANCE THEIR INVESTIGATIONS.

Authenticated:
SMS
18 Nov 08 - Revision

CHICAGO POLICE DEPARTMENT
DEPLOYMENT OPERATIONS CENTER

CRIME PREVENTION AND INFORMATION CENTER (CPIC) PRIVACY POLICY



MARCH 2011

Chicago Police Department's Crime Prevention Information Center

Privacy, Civil Rights, and Civil Liberties Protection Policy

A. Purpose Statement

1. The purpose of the Privacy, Civil Rights, and Civil Liberties Protection Policy (hereafter "Privacy Policy") is to promote **the Chicago Police Department's Crime Prevention Information Center** (hereafter "C.P.I.C."), source agency, and user agency (hereafter collectively referred to as "participating agencies" or "participants") conduct that complies with applicable federal, state, local, and tribal laws, regulations, and policies (see Appendix A – Terms and Definitions, of this policy) and assists participants in:
   - Ensuring individual privacy, civil rights, civil liberties, and other protected interests.
   - Increasing public safety and improving national security.
   - Protecting the integrity of criminal investigatory, criminal intelligence, and justice systems processes and information.
   - Minimizing the threat and risk of injury to specific individuals and damage to real or personal property.
   - Minimizing reluctance of individuals or groups to use or cooperate with the justice systems.
   - Encouraging individuals or community groups to trust and cooperate with the justice system.
   - Promoting governmental legitimacy and accountability.
   - Making the most effective use of public resources allocated to public safety agencies.

B. Policy Applicability and Legal Compliance

1. All participating CPIC personnel, participating agency personnel, personnel providing information technology services to the center, private contractors, and other authorized users will comply with the CPIC's privacy policy. This policy applies to information the center gathers or collects, receives, maintains, stores, accesses, discloses, or disseminates to center personnel, governmental agencies (including Information sharing Environment (ISE) participating centers and agencies), and participating justice and public safety agencies, as well as private contractors, private entities, and the general public.

2. The CPIC will provide a printed copy of its Privacy Policy to all CPIC personnel, non-agency personnel who provide services to the CPIC, and to each source agency and CPIC authorized user and will require both a written acknowledgement of receipt of this policy and a written agreement to comply with this policy and the applicable provisions it contains.

3. All CPIC personnel, participating agency personnel, personnel providing information technology services to the CPIC, private contractors, and other authorized users shall comply with applicable laws protecting privacy, civil rights, civil liberties, and other

protected interests, including, but not limited to, the U.S. Constitution, the Illinois Constitution, 28 Code of Federal Regulations (CFR) Part 23, Illinois Freedom of Information Act (5 ILCS 140/1, et seq.) and all other state, local, and federal privacy, civil rights, civil liberties, and legal requirements (refer to Appendix B) applicable to the CPIC and/or other participating agencies.

4. The CPIC has adopted internal operating policies that are in compliance with applicable laws protecting privacy, civil rights, and civil liberties, including, but not limited to, those listed in Appendix B.

C. Governance and Oversight

1. The Commander of the CPIC will have primary responsibility for operating the CPIC, system operations, and coordination of personnel; the receiving, seeking, retention, evaluation, information quality, analysis, destruction, sharing, disclosure, or dissemination of information; and enforcing the provisions of this policy.

2. A privacy committee of designees as determined by the Superintendent of Police will ensure that privacy and civil rights are protected as provided in this policy and by the Chicago Police Department's information-gathering and collection, retention, and dissemination processes and procedures. The committee will annually review and recommend updates to the policy to the Commander of the CPIC in response to changes in law, including the results of audits and inspections.

3. The CPIC's privacy committee is guided by a trained Privacy Officer who is selected by the CPIC Commander to assist in enforcing the provisions of this policy and who, in addition to other responsibilities, will receive reports regarding alleged errors and violations of the provisions of this policy, receives and coordinates complaint resolution under the CPIC's redress policy, and serves as the liaison for the Information Sharing Environment, ensuring that privacy protections are implemented throughout the process. The CPIC Privacy Officer can be reached at the below listed mailing or email address:

   Chicago Police Department – CPIC
   c/o Privacy Officer
   3510 S. Michigan, 4th Floor
   Chicago, IL 60653
   cpicpo@chicagopolice.org

4. The CPIC Privacy Officer ensures that enforcement procedures and sanctions outlined in this policy are adequate and enforced.

D. Terms and Definitions

1. The primary terms and definitions used in this privacy policy are set forth in Appendix A, Terms and Definitions.

E. Information

1. The CPIC will seek or retain information which a source agency (the CPIC or other agency) has determined that:
   - Is based on possible threat to public safety or the enforcement of criminal law, or
   - Is relevant to the investigation and prosecution of suspected criminal (including terrorist) incidents, the resulting justice system response, or the prevention of crime, or
   - Is based on reasonable suspicion that an identifiable individual or organization has committed a criminal offense or is involved in or planning criminal (including terrorist) conduct or activity that presents a threat to any individual, the community, or the nation and that the information is relevant to the criminal (including terrorist) conduct or activity, or
   - Is useful in crime analysis or in the administration of criminal justice and public safety, and
   - The source of the information is reliable and verifiable or limitations on the quality of the information are identified, and
   - The information was collected in a fair and lawful manner, with the knowledge and consent of the individual, if appropriate.

   The CPIC may retain information that is based on a level of suspicion that is less that "reasonable suspicion", such as tips and leads or suspicious activity report (SAR) information, subject to the policies and procedures specified within this policy.

2. Source agencies will agree not to submit information, and the CPIC will not seek or retain information about any individual or organization that was gathered solely on the basis of their religious, political, or social views or activities; their participation in a particular noncriminal organization or lawful event; or their races, ethnicities, citizenship, places of origin, ages, disabilities, genders, or sexual orientation.

3. The CPIC applies labels to center-originated information (or ensures that the originating agency has applied labels) to indicate to the accessing authorized user that:

   - The information is protected information as defined by the center to include personal information on any individual (see center's definitions of "protected information" and "personal information" in Appendix A of policy), and, to the extent expressly provided in this policy, to include organizational entities.
   - The information is subject to Illinois and federal law (Appendix B) restricting access, use, or disclosure.

4. The CPIC personnel will, upon receipt of information, assess the information to determine or review its nature, usability, and quality. Personnel will assign categories to the information (or ensure that the originating agency has assigned categories to the information) to reflect the assessment, such as:
   - Whether the information consists of tips and leads data, suspicious activity reports, criminal history, intelligence information, case records, conditions of supervision, case progress, or other information category.
   - The nature of the source as it affects veracity (for example, anonymous tip, trained interviewer or investigator, public record, private sector).
   - The reliability of the source (for example, reliable, usually reliable, unreliable, unknown).
   - The validity of the content (for example, confirmed, probable, doubtful, cannot be judged).

5. At the time a decision is made by the CPIC to retain information, it will be labeled (by record, data set, or system of records), to the maximum extent feasible, pursuant to applicable limitations on access and sensitivity of disclosure to:

   - Protect confidential sources and police undercover techniques and methods.
   - Not interfere with or compromise pending criminal investigations.
   - Protect an individual's right of privacy or their civil rights and civil liberties.
   - Provide legally required protections based on the individual's status as a child, sexual abuse victim, resident of a substance abuse treatment program, resident of a mental health treatment program, or resident of a domestic abuse shelter.

6. The labels assigned to existing information under Section E. 5. will be reevaluated whenever:

   - New information is added that has an impact on access limitations or the sensitivity of disclosure of the information.
   - There is a change in the use of the information affecting access or disclosure limitations; for example, the information becomes part of court proceedings for which there are different public access laws.

7. CPIC personnel are required to adhere to the following practices and procedures for the receipt, collection, assessment, storage, access, dissemination, retention, and security of tips and leads and suspicious activity report (SAR) information. Center personnel will:

   - Prior to allowing access to or dissemination of the information, ensure that attempts to validate or refute the information have taken place and that the information has been assessed for sensitivity and confidence by subjecting it to an evaluation or screening process to determine its credibility and value and categorize the information as unsubstantiated or uncorroborated if attempts to validate or determine the reliability of the information have been unsuccessful. The center will use a standard reporting format and data collection codes for SAR information.

- Store the information using the same storage method used for data that rises to the level of reasonable suspicion and which includes an audit and inspection process, supporting documentation, and labeling of the data to delineate it from other information.
- Allow access to or disseminate the information using the same (or a more restrictive) access or dissemination standard that is used for data that rises to the level of reasonable suspicion (for example, "need-to-know" and "right-to-know" access or dissemination for personally identifiable information).
- Regularly provide access to or disseminate the information in response to an interagency inquiry for law enforcement, homeland security, or public safety and analytical purposes or provide an assessment of the information to any agency, entity, individual, or the public when credible information indicates potential imminent danger to life or property.
- Retain SAR information for one (1) year to determine its credibility and value or assign a "disposition" label (for example, undetermined or unresolved, cleared or unfounded, verified, or under active investigation) so that a subsequently authorized user knows the status and purpose for the retention and will retain the information based on the retention period associated with the disposition label.
- Adhere to and follow the center's physical, administrative, and technical security measures to ensure the protection and security of tips, leads, and SAR information. Tips, leads, and SAR information will be secured in a system that is the same as or similar to the system that secures data that rises to the level of reasonable suspicion.

8. The CPIC incorporates the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents (SAR process) into existing processes and systems used to manage other crime-related information and criminal intelligence, thus leveraging existing policies and protocols utilized to protect the information, as well as information privacy, civil rights, and civil liberties.

9. The CPIC will identify and review protected information that may be accessed from or disseminated by the center prior to sharing that information through the Information Sharing Environment. Further, the center will provide notice mechanisms, including but not limited to metadata or data field labels that will enable ISE authorized users to determine the nature of the protected information and how to handle the information in accordance with applicable legal requirements.

10. The CPIC requires certain basic descriptive information (metadata tags or labels) to be entered and electronically associated with data (or content) for which there are special laws, rules, or policies regarding access, use, and disclosure, including terrorism-related information shared through the ISE. The types of information include:
    - The name of the originating center, department or agency, component, and subcomponent.
    - The name of the center's justice information system from which the information is disseminated.
    - The date the information was collected and, where feasible, the date its accuracy was last verified.

- The title and contact information for the person to whom questions regarding the information should be directed.

11. The CPIC will attach (or ensure that the originating agency has attached) specific labels and descriptive metadata to information that will be used, accessed, or disseminated to clearly indicate any legal restrictions on information sharing based on information sensitivity or classification.

12. The CPIC will keep a record of the source of all information sought and collected by the center.

F. Acquiring and Receiving Information

1. Information-gathering (acquisition) and access and investigative techniques used by the CPIC and source agencies must comply with and adhere to applicable laws, regulations and guidelines, including, but not limited to:
   - U.S. and Illinois state constitutional provisions (including those listed in Appendix B).
   - Applicable federal and state law provisions.
   - Chicago ordinances and regulations.
   - 28 CFR Part 23 regarding criminal intelligence information.
   - The OECD Fair Information Principles (under certain circumstances, there may be exceptions to the Fair Information Principles, based, for example, on authorities paralleling those provided in the federal Privacy Act; state, local, and tribal law; or center policy).
   - Criminal Intelligence guidelines established under the U.S. Department of Justice's National Criminal Intelligence Sharing Plan (NCISP).

2. The CPIC's SAR process provides for human review and vetting to ensure that information is both legally gathered and, where applicable, determined to have a potential terrorism nexus. Law enforcement officers and other personnel at source agencies who acquire SAR information that may be shared with the CPIC will be trained to recognize those behaviors and incidents that are indicative of criminal activity related to terrorism.

3. The CPIC's SAR process includes safeguards to ensure, to the greatest degree possible, that only information regarding individuals involved in activities that have been determined to be consistent with criminal activities associated with terrorism will be documented and shared through the ISE. These safeguards are intended to ensure that information that could violate civil rights (race, religion, national origin, ethnicity, etc.) and civil liberties (speech, assembly, religious exercise, etc.) will not be intentionally or inadvertently gathered, documented, processed, and shared.

4. Information-gathering and investigative techniques used by the CPIC, and those used by originating agencies, should be the least intrusive means necessary in the particular circumstances to gather information it is authorized to seek or retain.

5. External agencies that access the CPIC's information or share information with the center are governed by the laws and rules governing those individual agencies, including applicable federal and state laws.

6. The CPIC will contract only with commercial database entities that provide an assurance that their methods for gathering personally identifiable information comply with applicable local, state, tribal, territorial, and federal laws, statutes, and regulations and that these methods are not based on misleading information-gathering practices.

7. The CPIC will not directly or indirectly receive, seek, accept, or retain information from:
    - An individual who or nongovernmental entity that may or may not receive a fee or benefit for providing the information, except as expressly authorized by law or center policy.
    - An individual who or information provider that is legally prohibited from obtaining or disclosing the information.

G. Information Quality Assurance

1. The CPIC investigates, in a timely manner, alleged errors and deficiencies (or refers them to the originating agency) and corrects, deletes, or refrains from using protected information found to be erroneous or deficient.

2. The CPIC will ensure that source agencies assume primary responsibility for the quality and accuracy of their information collected by the CPIC. The CPIC will advise the appropriate contact person in the source agency in writing (this would include electronic notification) if information received from the source agency is alleged, suspected, or found to be erroneous or deficient.

3. The CPIC will make every reasonable effort to ensure that information sought or retained is derived from dependable and trustworthy sources; accurate; current; complete, including the relevant context in which it was sought or received and other related information; and merged with other related information about the same individual or organization only when the applicable standard (refer to Section I, Merging Records) has been met.

4. At the time of retention in the system, the information will be labeled regarding its level of quality (accuracy, completeness, currency, and confidence [verifiability and reliability]).

5. The labeling of retained information will be reevaluated by the CPIC or the originating agency when new information is gathered that has an impact on confidence (source reliability and content validity) in previously retained information.

6. The CPIC will conduct periodic data quality reviews of information it originates and make every reasonable effort to ensure that the information will be corrected, deleted from the system, or not used when the center identifies information that is erroneous, misleading, obsolete, or otherwise unreliable; the center did not have authority to gather the information or to provide the information to another agency; or the center used prohibited means to gather the information (except when the center's information source did not act as the agent of the center in gathering the information).

7. Originating agencies external to the CPIC are responsible for reviewing the quality and accuracy of the data provided to the center. The center will review the quality of information it has received from an originating agency and advise the appropriate contact person in the originating agency, in writing or electronically, if its data is alleged, suspected, or found to be inaccurate, incomplete, out of date, or unverifiable.

8. The CPIC will use written or electronic notification to inform recipient agencies when information previously provided to the recipient agency is deleted or changed by the center because the information is determined to be erroneous, includes incorrectly merged information, is out of date, cannot be verified, or lacks adequate context such that the rights of the individual may be affected.

H. Collation and Analysis

1. Information acquired or received by the CPIC or accessed for other sources will be analyzed only by qualified CPIC personnel who have successfully completed a background check and any applicable security clearance and have been selected, approved, and trained accordingly.

2. Information subject to collation and analysis is Information as defined and identified in Section E, Information of this policy.

3. Information acquired or received by the CPIC or accessed from other sources is analyzed according to priorities and needs and will be analyzed only to:
   - Further crime prevention (including terrorism), law enforcement, public safety, force deployment, or prosecution objectives and priorities established by the CPIC.
   - Provide tactical and/or strategic intelligence on the existence, identification, and capability of individuals and organizations suspected of having engaged in or engaging in criminal (including terrorist) activities.

The CPIC requires that all analytical products be reviewed by the Privacy Officer, or qualified designee as determined by the Commander of CPIC, to ensure that they provide appropriate privacy, civil rights, and civil liberties protections prior to dissemination or sharing by the center.

I. Merging Records

1. The set of identifying information sufficient to allow merging by the CPIC will utilize reasonable steps to identify the subject and may include the name (full or partial) and, in most cases, one or more of the following: date of birth; law enforcement or corrections system identification number; individual identifiers, such as fingerprints, photographs, physical description, height, weight, eye and hair color, race, ethnicity, tattoos, or scars; social security number; driver's license number; or other biometrics, such as DNA, retinal scan, or facial recognition. The identifiers or characteristics that, when combined, could clearly establish that the information from multiple records is about the same organization may include the name, federal or state tax ID number, office address, and telephone number.

2. If the matching requirements are not fully met but there is an identified partial match, the information may be associated by the CPIC if accompanied by a clear statement that it has not been adequately established that the information relates to the same individual or organization.

J. Sharing and Disclosure

1. Credentialed, role-based access criteria will be used by the CPIC, as appropriate, to control:
    A. The information to which a particular group or class of users can have access based on the group or class
    B. The information a class of users can add, change, delete, or print.
    C. To whom, individually, the information can be disclosed and under what circumstances

2. The CPIC adheres to the current version of the ISE-SAR Functional Standard for its suspicious activity reporting (SAR) process, including the use of a standard reporting format and commonly accepted data collection codes and a sharing process that complies with the ISE-SAR Functional Standard for suspicious activity potentially related to terrorism.

3. Access to or disclosure of records retained by the CPIC will be provided only to persons within the center or in other governmental agencies who are authorized to have access and only for legitimate law enforcement, public protection, public prosecution, public health, or justice purposes and only for the performance of official duties in accordance with law and procedures applicable to the agency for which the person is working. An audit trail sufficient to allow the identification of each individual who accessed information retained by the center and the nature of the information accessed will be kept by the CPIC.

4. Agencies external to the CPIC may not disseminate information accessed or disseminated from the center without approval from the center or other originator of the information.

5. Records retained by the CPIC may be accessed by or disseminated to those responsible for public protection, public safety, or public health only for public protection, public safety, or public health purposes and only in the performance of official duties in accordance with applicable laws and procedures. An audit trail sufficient to allow the identification of each individual who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

6. Information gathered or collected and records retained by the CPIC may be accessed or disseminated for specific purposes upon request by persons authorized by law to have such access and only for those uses and purposes specified in the law. An audit trail sufficient to allow the identification of each individual who requested, accessed, or received information retained by the center; the nature of the information requested, accessed, or received; and the specific purpose will be kept for a minimum of four (4) years by the CPIC.

7. Information gathered or collected and records retained by the CPIC may be accessed or disclosed to a member of the public only if the information is defined by law to be a public record or otherwise appropriate for release to further the center's mission and is not exempt from disclosure by law. Such information may be disclosed only in accordance with the law and procedures applicable to the center for this type of information. An audit trail sufficient to allow the identification of each individual member of the public who accessed or received information retained by the center and the nature of the information accessed will be kept by the center.

8. Information gathered or collected and records retained by the CPIC will not be:
   - Sold, published, exchanged, or disclosed for commercial purposes.
   - Disclosed or published without prior notice to the originating agency that such information is subject to disclosure or publication, unless disclosure is agreed to as part of the normal operations of the agency.
   - Disseminated to persons not authorized to access or use the information.

9. There are several categories of records that will not be ordinarily not be provided to the public:
   - Pursuant to Illinois Freedom of Information Act, 5 ILCS 140 *et al.,* the following records will not be provided to the public:
     1. Information specifically prohibited from disclosure by federal or state law or rules and regulations implementing federal or state law.
     2. Private information, unless disclosure is required by another provision of this Act, a state or Federal law or courts order.
     3. Personnel information contained within public records, the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,

unless disclosure is consented to in writing by the individual subjects of the information.

4. Records that relate to or affect the security of correctional institutions and detention facilities.
5. Preliminary drafts, notes, recommendations, memorandum and other records in which opinions are expressed, or policies or actions are formulated, except that a specific record or relevant portion of the record shall not be exempt when the record is publicly cited and identified by the head of the public body.
6. Trade secrets and commercial or financial information from a person or business where trade secrets or commercial or financial information are furnished under a claim of proprietary, privileged or confidential, and that disclosure would cause competitive harm to the person or business, and only insofar as the claim directly applies to the records requested.
7. Records relating to collective negotiating matters between public bodies and their employees or representatives, except that any final contract or agreement shall be subject to inspection and copying.
8. Records relating to a public body's adjudication of employee grievances or disciplinary cases; however, this exemption does not extend to the final outcome of cases in which discipline is imposed.
9. Information that would disclose or might lead to the disclosure of secret or confidential information, codes algorithms, programs, or private keys intended to be used to create electronic or digital signatures under the Electronic Commerce Security Act.
10. Vulnerability assessments, security measures, and response policies or plans that are designed to identify, prevent, or respond to potential attacks upon a community's population or systems, facilities, or installations, the destruction or contamination of which would constitute a clear and present danger to the health or safety of the community, but not to the extent that disclosure could reasonably be expected to jeopardize the effectiveness of the measures or the safety of the personnel who implement them or the public. Information exempt under this item may include such things as details pertaining to the mobilization or deployment of personnel or equipment, to the operation of communication systems or protocols, or to tactical operations.
11. Records in the possession of any body created in the course of administrative enforcement proceedings, and any law enforcement or correctional agency for law enforcement purposes, but only to the extent that disclosure would:
    1. interfere with pending or actually and reasonably contemplated law enforcement proceedings conducted by any law enforcement or correctional agency that is the recipient of the request;
    2. interfere with active administrative enforcement proceedings conducted by the public body that is the recipient of the request;
    3. create a substantial likelihood that a person will be deprived of a fair trial or an impartial hearing;

4. unavoidably disclose the identity of a confidential source, confidential information furnished only by the confidential source, or persons who file complaints with or provide information to administrative, investigative, law enforcement, or penal agencies; except that the identities of witnesses to traffic accidents, traffic accident reports, and rescue reports shall be provided by agencies of local government, except when disclosure would interfere with an active criminal investigation conducted by the agency that is the recipient of the request;
5. disclose unique or specialized investigative techniques other than those generally used and known or disclose internal documents or correctional agencies related to detection, observation or investigation of incidents of crime or misconduct, and disclosure would result in demonstrable harm to the agency or public body that is the recipient of the request;
6. endanger the life or physical safety of law enforcement personnel or any other person; or
7. obstruct an ongoing criminal investigation by the agency that is the recipient of the request.

- Information that meets the definition of "classified information" as the term is defined in the National Security Act, Public Law 235, Section 606, and in accord with Executive Order 13549, Classified National Security Information Program for State, Local, Tribal, and Private Sector Entities, August 18, 2010.
- Information determined to be confidential under Section 4002 of the Technology Advancement and Development Act.
- Information contained in local emergency plan submitted to a municipality in accordance with a local emergency plan ordinance that is adopted under Section 11-21.5-5 of the Illinois Municipal Code.
- Law enforcement officer identification information or driver information under Section 11-212 of the Illinois Vehicle Code.
- Information prohibited from being disclosed by the Personnel Records Review Act.
- Information prohibited from being disclosed by the Illinois School Student Records Act.
- Information that would violate an authorized nondisclosure agreement.
- Information of personally identifiable health information pursuant to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and any other confidentiality law.
- Protected federal, state, local, or tribal records, which may include records originated and controlled by another agency that cannot be shared without permission.
- Other authorized basis for denial.

10. The CPIC will not confirm the existence or nonexistence of information to any person, or agency that would not be entitled to receive the information unless otherwise required by law.

K. Redress

K.1 Disclosure:

1. Upon satisfactory verification (fingerprints, driver's license, or other specified identifying documentation) of his or her identity and subject to the conditions specified in item 2, below, an individual is entitled to know the existence of and to review the information about him or her that has been gathered and retained by the CPIC. The individual may obtain a copy, if appropriate or required, of the information for the purpose of challenging the accuracy or completeness of the information. The CPIC's response to the request for information will be made within a reasonable time and in a form that is readily intelligible to the individual. A record will be kept of all requests and of what information is disclosed to an individual. In Illinois, an individual's right to access and review criminal history record information is codified under Title 20, Part 1210 of the Illinois Administrative Code.

2. The existence, content, and source of the information will not be made available to an individual when:
   - Disclosure would interfere with, compromise, or delay an ongoing investigation or prosecution (5ILCS 140/7(1)(d)(i)).
   - Disclosure would endanger the health or safety of an individual, organization, or community (5ILCS 140/7(1)(d)(vi)).
   - The information is in a criminal intelligence information system subject to 28 CFR Part 23.
   - Other authorized basis for denial (refer to Section J, Sharing and Disclosure).

   If the information does not originate with the CPIC, the requestor will be referred to the originating agency, if appropriate or required, or the CPIC will notify the source agency of the request and its determination that disclosure by the CPIC or referral of the requestor to the source agency was neither required nor appropriate under applicable law.

K.2 Corrections

If an individual requests correction of information originating with the CPIC that has been disclosed, the CPIC's Privacy Officer or designee will inform the individual of the procedure for requesting and considering requested corrections, including appeal rights if requests are denied in whole or in part. A record will be kept of all requests for corrections and the resulting action, if any.

K.3 Appeals

The individual who has requested disclosure or to whom information has been disclosed will be given reasons if disclosure or requests for correction(s) are denied by the CPIC or the originating agency. The individual will also be informed of the procedure for appeal when the CPIC or originating agency has cited an exemption for the type of information requested or has declined to correct challenged information to the satisfaction of the individual to whom the information relates.

K.4 Complaints

1. If an individual has a complaint with regard to the accuracy or completeness of terrorism-related protected information that:

   A. Is exempt from disclosure,

   B. Has been or may be shared through the ISE,

      i) Is held by the CPIC and

      ii) Allegedly has resulted in demonstrable harm to the complainant,

   The center will inform the individual of the procedure for submitting (if needed) and resolving such complaints. Complaints will be received by the CPIC's Privacy Officer at the following e-mail address: cpicpo@chicagopolice.org or at that mailing address as found in Section N.1(2) of this policy. The Privacy Officer will acknowledge the complaint and state that it will be reviewed but will not confirm the existence or nonexistence of the information to the complainant unless otherwise required by law. If the information did not originate with the center, the Privacy Officer will notify the originating agency in writing or electronically within 10 days and, upon request, assist such agency to correct any identified data/record deficiencies, purge the information, or verify that the record is accurate. All information held by the CPIC that is the subject of a complaint will be reviewed within 30 days and confirmed or corrected/purged if determined to be inaccurate or incomplete, to include incorrectly merged information, or to be out of date. If there is no resolution within 30 days, the center will not share the information until such time as the complaint has been resolved. A record will be kept by the CPIC Privacy Officer of all complaints and the resulting action taken in response to the complaint.

2. To delineate protected information shared through the ISE from other data, the CPIC maintains records of agencies sharing terrorism-related information and employs system mechanisms to identify the originating agency when the information is shared.

L. Security Safeguards

1. The CPIC's Senior Watch Officer (SWO) is designated and trained to serve as the CPIC's security officer.

2. The CPIC will operate in a secure facility that is protected from external intrusion. The CPIC will utilize secure internal and external safeguards against network intrusions. Access to the CPIC's databases from outside the facility will be allowed only over secure networks.

3. The CPIC will secure tips, leads and SAR information in a separate repository system using security procedures and policies that are the same as or similar to those used for a system that secures data rising to the level of reasonable suspicion under 28 CFR Part 23.

4. The CPIC will store information in a manner that ensures it cannot be added to, modified, accessed, destroyed, or purged except by CPIC personnel authorized to take such actions.

5. Access to CPIC's information will be granted only to CPIC personnel whose positions and job duties require such access; who have successfully completed a background check and applicable security clearance; and who have been selected, approved, and trained accordingly.

6. Queries made to the CPIC's data applications will be logged into the data system identifying the user initiating the query.

7. The CPIC will utilize logs to maintain audit trails of requested and disseminated information (see Section N.2, Accountability, for more information on audit logs).

8. The CPIC will follow the data breach notification guidance set forth in the Illinois Personal Information Protection Act, 815 ILCS 530. The CPIC will:
    i. Notify an individual about whom personal information was or is reasonably believed to have been breached or obtained by an unauthorized person and access to which threatens physical, reputational, or financial harm to the person.
    ii. Make any necessary notice promptly and without unreasonable delay following discovery or notification of the access to the information, consistent with the legitimate needs of law enforcement to investigate the breach or any measures necessary to determine the scope of the breach and, if necessary, to restore the integrity of any information system affected by this release.

9. To prevent public records disclosure, risk and vulnerability assessments will not be stored with publicly available data.

M. Information Retention and Destruction

1. The CPIC's Privacy Officer will ensure that all information is reviewed for record retention (validation or purge) at least every two (2) years and in accordance with the Department's Form Retention Schedule and as provided by 28 CFR Part 23. For purposes of this Privacy Policy and for records retention and destruction purposes, suspicious activity reports will be treated as Chicago Police Department Information Reports which have a twelve (12) month retention.

2. When information has no further value or meets the CPIC's criteria for removal according to the Chicago Police Department's retention and destruction policy or according to the Illinois State Records Act, it will be purged, destroyed, and deleted or returned to the submitting agency.

3. The CPIC will delete information or return it to the originating agency once its retention period has expired as provided by this policy or as otherwise agreed upon with the originating agency.

4. The CPIC's Privacy Officer will complete a Department To-From Subject report through the chain of command accompanied by a Record Destruction Report per Department policies and procedures and in accordance with the Department's Form Retention Schedule for notification of appropriate parties before information is deleted or returned in accordance with this policy or as otherwise agreed upon with the originating agency.

5. Notification of proposed destruction or return of records may or may not be provided to the submitting agency by the CPIC depending on the relevance of the information and any agreement with the originating agency.

6. A record of information to be reviewed for retention will be maintained by the CPIC, and for appropriate system(s), notice will be given to the submitter at least 30 days prior to the required review and validation/purge date.

N. Transparency, Accountability, and Enforcement

N.1 Information System Transparency

1. The CPIC will be open with the public in regard to information and intelligence collection policies and practices. The CPIC will make the CPIC's Privacy Policy available upon request and posted on the Center's Web page at www.chicagopolice.org.

2. The CPIC's Privacy Officer will be responsible for receiving and responding to inquiries and complaints about privacy, civil rights, and civil liberties protections in the information system(s) maintained or accessed by the center. The CPIC Privacy Officer can be contacted at:

Chicago Police Department
c/o CPIC Privacy Officer
3510 S. Michigan, 4th Floor

Chicago, IL 60653
cpicpo@chicagopolice.org

N.2 Accountability

1. The audit log of queries made to the CPIC will identify the user initiating the query.

2. The CPIC will maintain an audit trail of accessed, requested, or disseminated information. An audit trail will be kept for a minimum of four (4) years of requests for access to information for specific purposes and of what information is disseminated to each person in response to the request.

3. The CPIC will adopt and follow procedures and practices by which it can ensure and evaluate the compliance of users with system requirements and with the provisions of this policy and applicable law. This will include logging access to these systems and periodic auditing of these systems, so as to not establish a pattern of the audits. These audits will be mandated at least semiannually and a record of the audits will be maintained by the CPIC Privacy Officer of the center.

4. CPIC's personnel or other authorized users shall report errors or suspected or confirmed violations of the CPIC's policies relating to protected information to the CPIC's Privacy Officer.

5. The CPIC will conduct an annual audit and inspection of the information and intelligence contained in its information system(s). The audit will be conducted by CPIC's Privacy Officer, or a designee as determined by the Superintendent of Police for the Chicago police Department. This person has the option of conducting a random audit at any time and without prior notice to the CPIC staff. This audit will be conducted in such a manner as to protect the confidentiality, sensitivity, and privacy of the CPIC's information and intelligence system(s).

6. The Department's Office of Compliance and/or CPIC's trained Privacy Officer will review and update the provisions protecting privacy, civil rights, and civil liberties contained in this policy annually and will make appropriate changes in response to changes in applicable laws, technology, the purpose and use of the information systems and public expectations.

N.3 Enforcement

1. If center personnel, a participating agency, or an authorized user is found to be in noncompliance with the provisions of this policy regarding the gathering, collection, use, retention, destruction, sharing, classification, or disclosure of information, the Director of the CPIC will:
   - Suspend or discontinue access to information by the center personnel, the participating agency, or the authorized user.

- Suspend, demote, transfer, or terminate center personnel, as permitted by applicable Department personnel policies.
- Apply administrative actions or sanctions as provided by Department General Order 93-03 entitled "Complaint and Disciplinary Procedures" and all addendum of General Order 93-03 in conjunction with the Rules and Regulations of the Chicago Police Department.
- If the authorized user is from an agency external to the agency/center, request that the relevant agency, organization, contractor, or service provider employing the user initiate proceedings to discipline the user or enforce the policy's provisions.
- Refer the matter to appropriate authorities for criminal prosecution, as necessary, to effectuate the purposes of the policy.

2. The CPIC reserves the right to restrict the qualifications and number of personnel having access to CPIC information and to suspend or withhold service and deny access to participating agency or participating agency personnel violating the CPIC's Privacy Policy.

O. Training

1. The CPIC will require the following individuals to participate in training programs regarding implementation of and adherence to this privacy, civil rights, and civil liberties policy:
   - All assigned personnel of the CPIC.
   - Personnel providing information technology services to the CPIC.
   - Staff in other public agencies or private contractors providing services to the CPIC.
   - User who are not employed by the CPIC or a contractor.

2. The CPIC's privacy policy training program will cover:

   - Purposes of the privacy, civil rights, and civil liberties protection policy.
   - Substance and intent of the provisions of the policy relating to collection, use, analysis, retention, destruction, sharing, and disclosure of information retained or submitted by the CPIC to the shared space.
   - Originating and participating agency responsibilities and obligations under applicable law and policy.
   - Department guidelines and procedures regarding the First Amendment and Police Actions, Modified Consent Decree regarding First Amendment investigations (Alliance to End Repression v. City of Chicago, 237 F.3d 799(7th Cir. 2001)), Judgment Order concerning First Amendment Rights and a hostile audience (Nelson v. Streeter, No. 88 C 5434), and Judgment Order concerning Attorney-Client Relationships (Case 76 C 1982).
   - How to implement the policy in the day-to-day work of the user, whether a paper or system user.
   - The impact of improper activities associated with infractions within or through the agency.

- Mechanisms for reporting violations of the CPIC's privacy protection policies and procedures.
- The nature and possible penalties for policy violations, including possible transfer, dismissal, and criminal liability, and immunity, if any.

3. The CPIC will provide special training regarding the center's requirements and policies for collection, use and disclosure of protected information to personnel authorized to share protected information through the Information Sharing Environment.

Appendix A—Terms and Definitions

The following is a list of primary terms and definitions used throughout this policy. These terms may also be useful in drafting the definitions section of the agency's/center's privacy policy.

Access—Data access is being able to get to (usually having permission to use) particular data on a computer. Web access means having a connection to the World Wide Web through an access provider or an online service provider. Data access is usually specified as read-only and read/write access.

With regard to the ISE, access refers to the business rules, means, and processes by and through which ISE participants obtain terrorism-related information, to include homeland security information, terrorism information, and law enforcement information acquired in the first instance by another ISE participant.

Access Control—The mechanisms for limiting access to certain information based on a user's identity and membership in various predefined groups. Access control can be mandatory, discretionary, or role-based.

Acquisition—The means by which an ISE participant obtains information through the exercise of its authorities, for example, through human intelligence collection or from a foreign partner. For the purposes of this definition, acquisition does not refer either to the obtaining of information widely available to other ISE participants through, for example, news reports or to the obtaining of information shared with them by another ISE participant who originally acquired the information.

Agency—The **CPIC** and all agencies that access, contribute, and share information in the **CPIC**'s justice information system.

Audit Trail—A generic term for recording (logging) a sequence of activities. In computer and network contexts, an audit trail tracks the sequence of activities on a system, such as user log-ins and log-outs. More expansive audit trail mechanisms would record each user's activity in detail—what commands were issued to the system, what records and files were accessed or modified, etc.

Audit trails are a fundamental part of computer security, used to trace (usually retrospectively) unauthorized users and uses. They can also be used to assist with information recovery in the event of a system failure.

Authentication—Authentication is the process of validating the credentials of a person, computer process, or device. Authentication requires that the person, process, or device making the request provide a credential that proves it is what or who it says it is. Common forms of credentials are digital certificates, digital signatures, smart cards, biometrics data, and a combination of user names and passwords. See Biometrics.

Authorization—The process of granting a person, computer process, or device with access to certain information, services, or functionality. Authorization is derived from the identity of the person, computer process, or device requesting access that is verified through authentication. See Authentication.

Biometrics—Biometrics methods can be divided into two categories: physiological and behavioral. Implementations of the former include face, eye (retina or iris), finger (fingertip, thumb, finger length or pattern), palm (print or topography), and hand geometry. The latter includes voiceprints and handwritten signatures.

Center—Center refers to the Chicago Police Department's **Crime Prevention & Information Center or CPIC.**

Civil Liberties—Fundamental individual rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. They are the freedoms that are guaranteed by the Bill of Rights, the first ten Amendments to the Constitution of the United States. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference. Generally, the term "civil rights" involves positive (or affirmative) government action, while the term "civil liberties" involves restrictions on government.

Civil Rights—The term "civil rights" refers to governments' role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, gender, or other characteristics unrelated to the worth of the individual. Civil rights are, therefore, obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress.

Computer Security—Protection of information assets through the use of technology, processes, and training.

Confidentiality—Confidentiality is closely related to privacy but is not identical. It refers to the obligations of individuals and institutions to use information under their control appropriately once it has been disclosed to them. One observes rules of confidentiality out of respect for and to protect and preserve the privacy of others. See Privacy.

Credentials—Information that includes identification and proof of identification that is utilized by CPIC members to gain access to local and network resources. Examples of credentials are user names, passwords, smart cards, and certificates. Credentialed security access will be utilized to control:

- What information a class of users can have access to;
- What information a class of users can add, change, delete, or print; and
- To whom the information can be disclosed and under what circumstances.

Criminal Intelligence Information or Data—Information deemed relevant to the identification of and the criminal activity engaged in by an individual who or organization that is reasonably suspected of involvement in criminal acts. The record is maintained in a criminal intelligence system per 28 CFR Part 23. Reasonable suspicion applies to the information. The record is maintained per 28 CFR Part 23.

Data—Inert symbols, signs, descriptions, or measures; elements of information.

Data Breach—The unintentional release of secure information to an untrusted environment. This may include incidents such as theft or loss of digital media—including computer tapes, hard drives, or laptop computers containing such media—upon which such information is stored unencrypted; posting such information on the World Wide Web or on a computer otherwise accessible from the Internet without proper information security precautions; transfer of such information to a system that is not completely open but is not appropriately or formally accredited for security at the approved level, such as unencrypted e-mail; or transfer of such information to the information systems of a possibly hostile agency or environment where it may be exposed to more intensive decryption techniques.

Data Protection—Encompasses the range of legal, regulatory, and institutional mechanisms that guide the collection, use, protection, and disclosure of information.

Disclosure—The release, transfer, provision of access to, sharing, publication, or divulging of personal information in any manner—electronic, verbal, or in writing—to an individual, agency, or organization outside the agency that collected it. Disclosure is an aspect of privacy, focusing on information which may be available only to certain people for certain purposes but which is not available to everyone.

Electronically Maintained—Information stored by a computer or on any electronic medium from which the information may be retrieved by a computer, such as electronic memory chips, magnetic tape, magnetic disk, or compact disk optical media.

Electronically Transmitted—Information exchanged with a computer using electronic media, such as the movement of information from one location to another by magnetic or optical media, transmission over the Internet, intranet, extranet, leased lines, dial-up lines, private networks, telephone voice response, and faxback systems. It does not include faxes, telephone calls, video

Fair Information Practices—The Fair Information Practices (FIPs) are contained within the Organization for Economic Co-operation and Development's (OECD) Guidelines on the Protection of Privacy and Transporter Flows of Personal Data. These were developed around commercial transactions and the transborder exchange of information; however, they do provide a straightforward description of underlying privacy and information exchange principles and provide a simple framework for the legal analysis that needs to be done with regard to privacy in integrated justice systems. Some of the individual principles may not apply in all instances of an integrated justice system. They are designed to:

1. Define agency purposes for information to help ensure agency uses of information are appropriate. ("Purpose Specification Principle")

2. Limit the collection of personal information to that required for the purposes intended. ("Collection Limitation Principle")

3. Ensure data accuracy. ("Data Quality Principle")

4. Ensure appropriate limits on agency use of personal information. ("Use Limitation Principle")

5. Maintain effective security over personal information. ("Security Safeguards Principle")

6. Promote a general policy of openness about agency practices and policies regarding personal information. ("Openness Principle")

7. Allow individuals reasonable access and opportunity to correct errors in their personal information held by the agency. ("Individual Participation Principle")

8. Identify, train, and hold agency personnel accountable for adhering to agency information quality and privacy policies. ("Accountability Principle")

Firewall—a security solution that segregates one portion of a network from another portion, allowing only authorized network traffic to pass through according to traffic-filtering rules.

Fusion Center—A collaborative effort of two or more agencies that provide resources, expertise, and information to a designated government agency or agency component with the goal of maximizing its ability to detect, prevent, investigate, and respond to criminal and terrorist activity.

General Information or Data—Information that could include records, documents, or files pertaining to law enforcement operations, such as Computer Aided Dispatch (CAD) data, incident data, and management information. Information that is maintained in a records management, CAD system, etc., for statistical/retrieval purposes. Information could be either resolved or unresolved. The record is maintained per statute, rule, or policy.

Homeland Security Information—As defined in Section 892(f)(1) of the Homeland Security Act of 2002 and codified at 6 U.S.C. § 482(f)(1), homeland security information means any information possessed by a federal, state, or local agency that (a) relates to a threat of terrorist activity; (b) relates to the ability to prevent, interdict, or disrupt terrorist activity; (c) would improve the identification or investigation of a suspected terrorist or terrorist organization; or (d) would improve the response to a terrorist act.

Information—Information includes any data about people, organizations, events, incidents, or objects, regardless of the medium in which it exists. Information received by law enforcement agencies can be categorized into four general areas: general data, tips and leads data, suspicious activity reports, and criminal intelligence information.

Information Quality—Information quality refers to various aspects of the information; the accuracy and validity of the actual values of the data, data structure, and database/data repository design. Traditionally, the basic elements of information quality have been identified as accuracy,

completeness, currency, reliability, and context/meaning. Today, information quality is being more fully described in multidimensional models, expanding conventional views of the topic to include considerations of accessibility, security, and privacy.

Information Sharing Environment (ISE) Suspicious Activity Report (SAR) (ISE-SAR)—A SAR that has been determined, pursuant to a two-part process established in the ISE_SAR Functional Standard, to have a potential terrorism nexus (i.e., to be reasonably indicative of criminal activity associated with terrorism).

Intelligence-Led Policing (ILP)—A process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions.

Invasion of Privacy—Intrusion on one's solitude or into one's private affairs, public disclosure of embarrassing private information, publicity that puts one in a false light to the public, or appropriation of one's name or picture for personal or commercial advantage. See also Right to Privacy.

Law—As used by this policy, law includes any local, state, or federal statute, ordinance, regulation, executive order, policy, or court rule, decision, or order as construed by appropriate local, state, or federal officials or agencies.

Law Enforcement Information—For purposes of the ISE, law enforcement information means any information obtained by or of interest to a law enforcement agency or official that is both (a) related to terrorism or the security of our homeland and (b) relevant to a law enforcement mission, including but not limited to information pertaining to an actual or potential criminal, civil, or administrative investigation or a foreign intelligence, counterintelligence, or counterterrorism investigation; assessment of or response to criminal threats and vulnerabilities; the existence, organization, capabilities, plans, intentions, vulnerabilities, means, methods, or activities of individuals or groups involved or suspected of involvement in criminal or unlawful conduct or assisting or associated with criminal or unlawful conduct; the existence, identification, detection, prevention, interdiction, or disruption of or response to criminal acts and violations of the law; identification, apprehension, prosecution, release, detention, adjudication, supervision, or rehabilitation of accused persons or criminal offenders; and victim/witness assistance.

Lawful Permanent Resident—A foreign national who has been granted the privilege of permanently living and working in the United States.

Least Privilege Administration—A recommended security practice in which every user is provided with only the minimum privileges needed to accomplish the tasks he or she is authorized to perform.

Logs—Logs are a necessary part of an adequate security system because they are needed to ensure that data is properly tracked and that only authorized individuals can access the system and the data.

Maintenance of Information—Applies to all forms of information storage. This includes electronic systems (for example, databases) and non-electronic storage systems (for example, filing cabinets). To meet access requirements, an organization is not required to create new systems to maintain information or to maintain information beyond a time when it no longer serves an organization's purpose.

Metadata—In its simplest form, metadata is information (data) about information, more specifically information about a particular aspect of the collected information. An item of metadata may describe an individual content item or a collection of content items. Metadata is used to facilitate the understanding, use, and management of information. The metadata required for this will vary based on the type of information and the context of use.

Need to Know— As a result of jurisdictional, organizational, or operational necessities, access to sensitive information or intelligence is necessary for the conduct of an individual's official duties as part of an organization that has a right to know the information in the performance of a law enforcement, homeland security, or counter-terrorism activity, such as to further an investigation or meet another law enforcement requirement.

Nonrepudiation—A technique used to ensure that someone performing an action on a computer cannot falsely deny that he or she performed that action. Nonrepudiation provides undeniable proof that a user took a specific action, such as transferring money, authorizing a purchase, or sending a message.

Originating Agency—The agency or organizational entity that documents information or data, including source agencies that document SAR (and, when authorized, ISE-SAR) information that is collected by a fusion center.

Participating Agencies—An organization entity that is authorized to access or receive and use center information and/or intelligence databases and resources for lawful purposes through its authorized individual users.

Permissions—Authorization to perform operations associated with a specific shared resource, such as a file, directory, or printer. Permissions must be granted by the system administrator to individual user accounts or administrative groups.

Personal Information—Information that can be used, either alone or in combination with other information, to identify individual subjects suspected of engaging in an activity or incident potentially related to terrorism.

Personally Identifiable Information—Personally identifiable information is one or more pieces of information that, when considered together or in the context of how the information is presented or gathered, are sufficient to specify a unique individual. The pieces of information can be:

- Personal characteristics (such as height, weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious

affiliation, place of birth, mother's maiden name, distinguishing features, and biometrics information, such as fingerprints, DNA, and retinal scans).

- A unique set of numbers or characters assigned to a specific individual (including name, address, phone number, social security number, e-mail address, driver's license number, financial account or credit card number and associated PIN number, Automated Integrated Fingerprint Identification System [AIFIS] identifier, or booking or detention system number).

- Descriptions of event(s) or points in time (for example, information in documents such as police reports, arrest reports, and medical records).

- Descriptions of location(s) or place(s) (including geographic information systems [GIS] locations, electronic bracelet monitoring information, etc.).

Persons—Executive Order 12333 defines "United States persons" as a United States citizen, an alien known by the intelligence agency concerned to be a permanent resident alien, an unincorporated association substantially composed of United States citizens or permanent resident aliens, or a corporation incorporated in the United States, except for a corporation directed and controlled by a foreign government or governments. For the intelligence community and for domestic law enforcement agencies, "persons" means United States citizens and lawful permanent residents.

Privacy—Refers to individuals' interests in preventing the inappropriate collection, use, and release of personal information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data. Other definitions of privacy include the right to be physically left alone (solitude); to be free from physical interference, threat, or unwanted touching (assault, battery); or to avoid being seen or overheard in particular contexts.

Privacy Policy—A printed, published statement that articulates the policy position of an organization on how it handles the personal information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, disclosure, and access. The purpose of the privacy policy is to articulate that the agency/center will adhere to those legal requirements and agency/center policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and -implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.

Privacy Protection—A process of maximizing the protection of privacy, civil rights, and civil liberties when collecting and sharing information in the process of protecting public safety and public health.

Private Information – Pursuant to Illinois Freedom of Information Act, 5 ILCS 140 *et al.*, Private Information means unique identifiers, including a person's social security number, driver's license number, employee identification number, biometric identifiers, personal financial information, passwords or other access codes, medical records, home or personal telephone

numbers, and personal email addresses. Private information also includes home address and personal license plates, except as otherwise provided by law or when compiled without possibility of attribution to any person.

Protected Information—Protected information includes personal data about individuals that is subject to information privacy or other legal protections by law, including the U.S. Constitution and the Illinois constitution; applicable federal statutes and regulations, such as civil rights laws and 28 CFR Part 23; applicable state and local laws and ordinances. Protection may also be extended to organizations by center policy or state or local law

For the (federal) intelligence community, protected information includes information about "United States persons" as defined in Executive Order 12333. Protected information may also include other information that the U.S. government expressly determines by Executive Order, international agreement, or other similar instrument should be covered.

Public—Public includes:

- Any person and any for-profit or nonprofit entity, organization, or association.
- Any governmental entity for which there is no existing specific law authorizing access to the agency's/center's information.
- Media organizations.
- Entities that seek, receive, or disseminate information for whatever reason, regardless of whether it is done with the intent of making a profit, and without distinction as to the nature or intent of those requesting information from the agency.

Public does not include:

- Employees of the agency.
- People or entities—private or governmental—who assist the agency/center in the operation of the justice information system.
- Public agencies whose authority to access information gathered and retained by the agency/center is specified in law.

Public Access—Public access relates to what information can be seen by the public, that is, information whose availability is not subject to privacy interests or rights.

Record—Any item, collection, or grouping of information that includes personally identifiable information and is maintained, collected, used, or disseminated by or for the collecting agency or organization.

Redress—internal procedures to address complaints from persons regarding protected information about them that is under the agency's control.

Repudiation—the ability of a user to deny having performed an action that other parties cannot prove otherwise. For example, a user who deleted a file can successfully deny doing so if no mechanism (such as audit files) can contradict that claim.

Retention—Refer to Storage.

Right to Know—Based on having legal authority or responsibility or pursuant to an authorized agreement, an agency or organization is authorized to access sensitive information and intelligence in the performance of a law enforcement, homeland security, or counterterrorism activity.

Right to Privacy—The right to be left alone, in the absence of some reasonable public interest in gathering, retaining, and sharing information about a person's activities. Invasion of the right to privacy can be the basis for a lawsuit for damages against the person or entity violating a person's privacy.

Role-Based Access—A type of access that uses roles to determine rights and privileges. A role is a symbolic category of users that share the same security privilege.

Security—Refers to the range of administrative, technical, and physical business practices and mechanisms that aim to preserve privacy and confidentiality by restricting information access to authorized users for authorized purposes. Computer and communications security efforts also have the goal of ensuring the accuracy and timely availability of data for the legitimate user set, as well as promoting failure resistance in the electronic systems overall.

Source Agency—Source agency refers to the agency or entity that originates SAR (and, when authorized, ISE-SAR) information.

Storage—In a computer, storage is the place where data is held in an electromagnetic or optical form for access by a computer processor. There are two general usages:

1. Storage is frequently used to mean the devices and data connected to the computer through input/output operations—that is, hard disk and tape systems and other forms of storage that do not include computer memory and other in-computer storage. This meaning is probably more common in the Information Technology industry than the second meaning.
2. In a more formal usage, storage has been divided into (1) primary storage, which holds data in memory (sometimes called random access memory or RAM) and other "built-in" devices such as the processor's L1 cache, and (2) secondary storage, which holds data on hard disks, tapes, and other devices requiring input/output operations.

Primary storage is much faster to access than secondary storage because of the proximity of the storage to the processor or because of the nature of the storage devices. On the other hand, secondary storage can hold much more data than primary storage.

With regard to the ISE, storage (or retention) refers to the storage and safeguarding of terrorism-related information, to include homeland security information, terrorism information, and law enforcement information relating to terrorism or the security of our homeland by both the originator of the information and any recipient of the information.

Suspicious Activity—Observed behavior reasonably indicative of preoperational planning related to terrorism or other criminal activity. Examples of suspicious activity include surveillance, photography of sensitive infrastructure facilities, site breach or physical intrusion, cyber attacks, testing of security, etc.

Suspicious Activity Reports (SARs)—Reports that record the observation and documentation of a suspicious activity. Suspicious Activity Report (SAR) information offers a standardized means for feeding information repositories or data analysis tool. Any patterns identified during SAR review and analysis may be investigated in coordination with the reporting agency and, if applicable, the state or regional fusion center. SAR information is not intended to be used to track or record ongoing enforcement, intelligence, or investigatory activities, nor are they designed to support interagency calls for service.

Terrorism Information—Consistent with Section 1016(a)(4) of the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), all information relating to (a) the existence, organization, capabilities, plans, intentions, vulnerabilities, means of finance or materials support, or activities of foreign or international terrorist groups or individuals or of domestic groups or individuals involved in transnational terrorism; (b) threats posed by such groups or individuals to the United States, United States persons, or United States interests or to those interests of other nations; (c) communications of or by such groups or individuals; or (d) other groups or individuals reasonably believed to be assisting or associated with such groups or individuals.

Terrorism-Related Information—In accordance with the IRTPA, as recently amended by the 9/11 Commission Act enacted on August 3, 2007 (P.L. 110-53), the ISE facilitates the sharing of terrorism and homeland security information, as defined in the IRTPA Section 1016(a)(5) and the Homeland Security Act 892(f)(1) (6 U.S.C. § 482(f)(1)). See also *Information Sharing Environment Implementation Plan* (November 2006) and Presidential Guidelines 2 and 3 (the ISE will facilitate the sharing of "terrorism information," as defined in IRTPA, as well as the following categories of information to the extent that they do not otherwise constitute "terrorism information": (1) homeland security information as defined in Section 892(f)(1) of the Homeland Security Act of 2002 (6 U.S.C. § 482(f)(1)) and (2) law enforcement information relating to terrorism or the security of our homeland). Such additional information includes intelligence information.

Weapons of Mass Destruction (WMD) information was defined and included in the definition of "terrorism information" by P.L. 110-53

Tips and Leads Information or Data—Generally uncorroborated reports or information generated from inside or outside the agency that allege or indicate some form of possible criminal activity. Tips and leads are sometimes referred to as suspicious incident report (SIR), suspicious activity report (SAR), and/or field interview reports (FIR). However, SAR information should be viewed, at most, as a subcategory of tip or lead data. Tips and leads information does not include incidents that do not have an criminal offense attached or indicated, criminal history records, or Computer Aided Dispatch (CAD) data. Tips and leads information

should be maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

A tip or lead can come from a variety of sources, including, but not limited to, the public, field interview reports, and anonymous or confidential sources. This information may be based on mere suspicion or on a level of suspicion that is less than "reasonable suspicion" and, without further inquiry or analysis, it is unknown whether the information is accurate or useful. Tips and leads information falls between being of no use to law enforcement and being extremely valuable depending on whether time and resources are available to determine its meaning.

Tips and leads information is maintained in a secure system, similar to data that rises to the level of reasonable suspicion.

User—An individual representing a participating agency who is authorized to access or receive and use a center's information and intelligence databases and resources for lawful purposes.

Appendix B –State and Federal Law Relevant to Seeking, Retaining, and Disseminating Justice Information

STATE LAW:

Constitution of the State of Illinois

Illinois Administrative Code, Title 20, **Corrections, Criminal Justice, and Law Enforcement**

Illinois Administrative Code, Title 20, Part 1210 **Individual's Right To Access and Review Criminal History Record Information**

Illinois Compiled Statutes (ILCS):

- **Civil Administrative Code of Illinois** (Department of State Police Law), Title 20, Part 2605/2605-45(4)
- **Illinois Freedom of Information Act**, 5 ILCS 140/1, et seq.
- **Illinois School Student Records Act**, Title 105, Part, Section 5
- **Illinois State Records Act**, 5 ILCS 160
- Municipalities, Title 65 Illinois Municipal Code, Part 5, Article 11, Division 21.5-5, "**Local Emergency Plans**"
- Personal Information Protection Act, Title 815, Part 530 and 815-530-10 "**Notice of Breach**"
- **Personnel Records Review Act**, Title 820, Part 40
- **Technology Advancement and Development Act**, Title 20, Part 700, Section 4002
- Vehicles, Title 65, Part 5, Chapter 11 **Illinois Vehicle Code**, 212 (law enforcement officer identification information or driver information)

FEDERAL LAW:

Brady Handgun Violence Prevention Act, 18 U.S.C. §§ 921, 922, 924, and 925A, United States Code, Title 18, Part I, Chapter 44, §§ 921, 922, 924, and 925A

Computer Matching and Privacy Act of 1988, 5 U.S.C. § 552a(a), United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a(a); see also Office of Management and Budget, Memorandum M-01-05, "Guidance on Interagency Sharing of Personal Data–Protecting Personal Privacy," December 20, 2000

Confidentiality of Identifiable Research and Statistical Information, 28 CFR Part 22, Code of Federal Regulations, Title 28, Chapter I, Part 22

Crime Identification Technology, 42 U.S.C. § 14601, United States Code, Title 42, Chapter 140, Subchapter I, § 14601

Criminal History Records Exchanged for Noncriminal Justice Purposes, 42 U.S.C. § 14611, United States Code, Title 42, Chapter 140, Subchapter II, § 14611

Criminal Intelligence Systems Operating Policies, 28 CFR Part 23, Code of Federal Regulations, Title 28, Chapter 1, Part 23

Criminal Justice Information Systems, 28 CFR Part 20, Code of Federal Regulations, Title 28, Chapter 1, Part 20

Disposal of Consumer Report Information and Records, 16 CFR Part 682, Code of Federal Regulations, Title 16, Chapter I, Part 682

Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522, 2701–2709, United States Code, Title 18, Part I, Chapter 119, §§ 2510–2522, 2701–2709, and 3121–3125, Public Law 99-508

Fair Credit Reporting Act, 15 U.S.C. § 1681, United States Code, Title 15, Chapter 41, Subchapter III, § 1681

Federal Civil Rights laws, 42 U.S.C. § 1983, United States Code, Title 42, Chapter 21, Subchapter I, § 1983

Federal Records Act, 44 U.S.C. § 3301, United States Code, Title 44, Chapter 33, § 3301

Freedom of Information Act (FOIA), 5 U.S.C. § 552, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552

HIPAA, Health Insurance Portability and Accountability Act of 1996, 42 U.S.C. § 201, United States Code, Title 42, Chapter 6A, Subchapter I, § 201; Public Law 104-191

HIPAA, Standards for Privacy of Individually Identifiable Health Information, 45 CFR Parts 160 and 164; Code of Federal Regulations, Title 45, Parts 160 and 164

Indian Civil Rights Act of 1968, 25 U.S.C. § 1301, United States Code, Title 25, Chapter 15, Subchapter I, § 1301

Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA), Section 1016, as amended by the 9/11 Commission Act

National Child Protection Act of 1993, Public Law 103-209 (December 20, 1993), 107 Stat. 2490

National Crime Prevention and Privacy Compact, 42 U.S.C. § 14616, United States Code, Title 42, Chapter 140, Subchapter II, § 14616

Privacy Act of 1974, 5 U.S.C. § 552a, United States Code, Title 5, Part I, Chapter 5, Subchapter II, § 552a

Privacy of Consumer Financial Information, 16 CFR Part 313, Code of Federal Regulations, Title 16, Chapter I, Part 313

Protection of Human Subjects, 28 CFR Part 46, Code of Federal Regulations, Title 28, Chapter 1, Volume 2, Part 46

Safeguarding Customer Information, 16 CFR Part 314, Code of Federal Regulations, Title 16, Chapter I, Part 314

Sarbanes-Oxley Act of 2002, 15 U.S.C., Chapter 98, § 7201, United States Code, Title 15, Chapter 98, § 7201

U.S. Constitution, First, Fourth, and Sixth Amendments

USA PATRIOT Act, Public Law 107-56 (October 26, 2001), 115 Stat.

Rahm Emanuel
Mayor

Department of Police – City of Chicago
3510 S. Michigan Avenue – Chicago, Illinois 60653

Garry F. McCarthy
Superintendent

Privacy Policy Agreement

I hereby agree that I have received a copy of the Crime Prevention and Information Center (hereinafter described as "CPIC") Privacy Policy and have read it and fully understand the CPIC Privacy Policy and the Privacy Principles contained therein. Additionally, I agree to abide by the Privacy Design Principles and guidelines contained within the CPIC Privacy Policy. Documents and information obtained in the CPIC may contain confidential or privileged information, by signing this agreement I agree to treat all communication obtained in the CPIC as Law Enforcement Sensitive for Official Use Only. I understand that any further distribution of these documents is restricted to law enforcement agencies unless otherwise approved by the Chicago Police Department. I understand and comply with the terms of the Privacy Policy Agreement and will adhere to the terms regarding distribution of information.

Member's Name _____

Member's Employee Number _____

Member's Signature _____

Date _____

Stratton, Melissa

From: [redacted]
Sent: Saturday, March 03, 2012 4:54 AM
To: Stratton, Melissa
Cc: [redacted]
Subject: Re: Follow Up

Thank you Melissa. We are all still at the office too! We have seats and dinners for both of u at our dignitaries table. You are our guests for the period u choose to stay.

Sent from my iPhone

On Mar 3, 2012, at 12:38 AM, "Stratton, Melissa" <Melissa.Stratton@chicagopolice.org> wrote:

[redacted]

Am so sorry to be getting back to you just now. I've been extremely short-staffed this week and am actually still at work at this hour.

In any event, I would like to thank you for the details you provided below. I'd also like to thank you for your kind offer of a table for our department.

Due to organizational changes and other initiatives rolling out this week, it'll just be me attending with the Superintendent. I don't need a seat or anything!

See you tomorrow.

Best,
Melissa

From: [redacted]
Sent: Thursday, March 01, 2012 4:30 PM
To: Stratton, Melissa
Subject: RE: Follow Up

Hi Melissa,

Hope all is well.

There is good news and bad news.

The bad news that there is a detailed document circulating in the media regarding the NYPD program in Newark specifically:
http://hosted.ap.org/specials/interactives/documents/nypd/nypd_newark.pdf

The good news is we have declined to comment on it despite several media requests and instead have stuck to simply saying that Superintendent McCarthy has stated that Newark's involvement was minimal and within the bounds of the law, and we are taking his word for it, and that our focus

is on Chicago where we envision a positive police/community relationship being formed due to both our willingness and the Superintendent's commitment to striking the right balance between security and civil liberties were the law is respected.

This is important as the NYPD controversy is blowing up harder in New York and at Yale where Jewish students and other are organizing against the spying that happened there against Muslims students.

Our WBEZ interview was in my judgment a positive piece for the Superintendent, as was the AP piece, which was circulated widely, where our leaders [redacted]) kept a consistent positive message of approval regarding the Superintendent (owing to the positive meeting of mutual understanding we had with him, and his positive outreach at our dinner this Saturday).

In regards to the dinner, reception is at 6, the program officially starts at 7. He does not have to be at the reception but he is welcome if he would like to interact. At the dinner he will speak briefly right after the awardees (see program) which is about 30 min into the program. He is welcome to remain for a short while thereafter or for the rest of the program.

Additionally, should you like it, we can offer the Chicago Police a complimentary table (of 10) at our event so that superintendents, staff, or others could also attend. It would have "Chicago Police" as the table name. I think this would be very good outreach. Tables are ordinary sold for $750.

Please advise me of who will be accompanying the Superintendent so we recognize them, and if you are interested in the table idea.

Let me know if you have any further questions.
202 870 0166

==========

[redacted]
CAIR-Chicago
www.cairchicago.org

<image001.jpg>

RSVP now for CAIR-Chicago's 8th Annual Banquet
A Future Without Bigotry – March 3rd 2012
Drury Lane, Oak Brook IL
http://www.cairchicago.org/rsvp2012

Stratton, Melissa

From: [redacted]
Sent: Tuesday, February 28, 2012 2:45 PM
To: Stratton, Melissa
Subject: communique

Hi Melissa,

As I said, there remains strong media interest in the NYPD fallout, with the White House weighing in to distance itself from the program, talks of investigations, law suits, etc. It's likely to go on for a while. This is a serious constitutional violation and many won't let it slide as they shouldn't. … We need to be in the driver's seat here if we are to distance Chicago from NY's problems and its aftermath and keep it positive and constructive here which is our vision for this great city's police/community relations and yours. I believe this does it:

CAIR, Chicago Police Superintendent Meet to Discuss NYPD Muslim Spying

Superintendent McCarthy to address Muslim community at CAIR-Chicago Banquet

(CHICAGO, 2/28/2012) Earlier today, CAIR-Chicago's Executive Director Ahmed Rehab and community partners met with Chicago Superintendent Gary F. McCarthy and members of his staff to discuss recent media reports about the NYPD community surveillance program which CAIR-Chicago, civil rights groups, elected officials, and university administrators have described as un-American and unconstitutional.

SEE:
http://www.salon.com/2012/02/28/the_nypd_spying_controversy_a_microcosm_for_the_911_era/singleton/

"We stand behind law enforcement in its mission to follow investigative criminal leads and probable cause, but that is not to be conflated with surveying entire communities and individuals based on no other fact except that they are Muslim," said Rehab. "Our system of justice works on individualized suspicion, not wholesale suspicion. Race, ethnicity, and religion do not constitute probable cause for criminal investigations; they never have and never will be".

Newark Mayor Cory A. Booker strongly condemned "blanket investigations" as "deeply offensive," while New Jersey Governor Chris Christie called them "disturbing."

SEE: http://articles.cnn.com/2012-02-23/us/us_new-jersey-nypd-surveillance_1_mayor-cory-booker-newark-mayor-nypd?_s=PM:US

Superintendent McCarthy was the Newark Police Superintendent when the NYPD was carrying out its program in New York and parts of New Jersey. CAIR-Chicago sent a letter to Superintendent McCarthy seeking a clarification of his position and a person-to-person meeting.

"We sent a letter outlining our concerns and requesting an in-person meeting; the fact that we heard back the same day with a date for a meeting was a strong indication that Superintendent McCarthy took this issue seriously," Rehab said.

Rehab was accompanied by CAIR-Chicago staff attorney Rabya Khan, and community partners Jane Ramsey (President of the Jewish Council on Urban Affairs) and Josh Hoyt (Chief Strategic Executive of the Illinois Coalition for Immigrant and Refugee Rights).

Rehab described the meeting as highly constructive.

The Newark police department was not an active part of the NYPD surveillance program. Superintendent McCarthy indicated that what limited interactions Newark had with the NYPD program were within the bounds of the law.

"We had an honest and open discussion about the issues that concern our community," Rehab said. "We sought and received reassurances that such a program would not be carried out in Chicago and that the Superintendent stood against community profiling and blanket investigations."

"We feel that Superintendent McCarthy has been doing a good job in Chicago. We left convinced that he harbors nothing but respect for Islam and the Muslim community as well as a deep personal commitment to upholding the law including the civil rights for all Chicagoans."

Rabya Khan added that "safety is a partnership between the police and the community, and positive relations between the two are essential in not only ensuring safety but in protecting our civil liberties. Both parties at the meeting understood this."

"Given the charged atmosphere regarding revelations about the NYPD program, we felt it would be helpful if Superintendent McCarthy would address the community directly and he has graciously agreed to do so at CAIR-Chicago's annual banquet this Saturday."

SEE: http://www.cairchicago.org/rsvp2012/

"This is a refreshing example of positive Police/Community outreach and cooperation, a model to be commended and followed in other cities," said Hoyt.

-END-

CAIR-Chicago is a chapter of America's largest Muslim civil liberties and advocacy organization. Its mission is to defend civil rights, fight bigotry, and promote tolerance.

CONTACT: [redacted]

Stratton, Melissa

From: Hernandez, Maribel
Sent: Friday, March 02, 2012 3:15 PM
To: Stratton, Melissa
Subject: Message - [redacted] - CARE Chicago

Melissa

Please ca[redacted]he is following up on the emails he sent you.

Maribel

City of Chicago
Department of Police
3510 South Michigan Avenue
Chicago, Illinois 60653

Brennan Center for Justice
ATTN: Michael Rance
161 Avenue of the Americas, 12th Floor
New York, NY 10013