

LOS ANGELES POLICE DEPARTMENT



CHARLIE BECK
Chief of Police

P. O. Box 30158
Los Angeles, California 90030
Telephone: (213) 978-2100
TDD: (877) 275-5273
Reference Number: 14,4

ANTONIO R. VILLARAIGOSA
Mayor

March 16, 2012

Mr. Michael Price
Mr. Emin Akopyan
Brennan Center For Justice
New York University School of Law
161 Avenue of the Americas, 12th Floor
New York, New York 10013

Dear Mr. Price and Mr. Akopyan:

I have received your request for:

Item No. 1

All documents, procedures, training materials, charts, statistics, reports, audits, Divisional Orders (including Divisional Orders of the Major Crimes Division), and portions of the Major Crimes Division confidential Procedural Manual relating to the conduct or regulation of:

- Investigations and preliminary inquiries of persons, groups or organizations engaged in First Amendment activities;
- Collection, dissemination, retention, database inclusion, purging and auditing of intelligence information relating to persons, groups or organizations engaged in First Amendment activities;
- Counterterrorism investigations and intelligence operations;
- Community mapping programs; and
- Interception of a wire or electronic communication

Item No. 2

All training materials shown, presented, displayed or provided, since September 11, 2001, by the Los Angeles Police Department or its agents, employees, consultants, representatives or independent contractors to LAPD personnel that refer or relate to the Muslim community, Islam, or jihad.

Department staff conducted a search and has located the following materials:

- Major Crimes Division (MCD) Standards and Procedures;
- Audit of Anti-Terrorist Intelligence Section (Phase I), Fiscal year 2006/2007;
- Anti-Terrorism Intelligence Section Audit, Fiscal year 2008/09;
- Anti-Terrorism Intelligence Section Audit, Fiscal Year 2009/2010;
- MCD Divisional Order No. 1, April 12, 2006, Intelligence Reporting Procedures for Anti-Terrorism Intelligence Section Function;
- MCD Divisional Order No. 2, April 12, 2006, Investigators Working Folder for the Anti-Terrorism Intelligence Section Function;
- MCD Divisional Order No. 3, April 12, 2006, Security of Intelligence Files for the Anti-Terrorism Intelligence Section Function;
- MCD Divisional Order No. 4, April 12, 2006, Surveillance Logs for the Anti-Terrorism Section Intelligence Function;
- MCD Divisional Order No. 5, April 12, 2006, Analysis Unit Information and Data Storage for the Anti-Terrorism Intelligence Section Function;
- MCD Divisional Order No. 6, April 12, 2006, Surveillance and Field Observations for Anti-Terrorism Intelligence Section Functions;
- MCD Divisional Order No. 7, April 12, 2006, Undercover Investigations for Anti-Terrorism Intelligence Section Functions;
- MCD Divisional Order No. 8, April 12, 2006, Dissemination of Intelligence Information;
- MCD Divisional Order No. 9, April 12, 2006, Use of LACLEAR for All Investigations;
- MCD Divisional Order No. 10, November 20, 2006, Initial Lead and Preliminary Investigation Time Limits;
- MCD Divisional Order No. 11, March 16, 2007, Investigator's Working Folder (Amendments);
- MCD Divisional Order No. 12, October 30, 2008, Surveillance Approval Procedure;
- MCD Divisional Order No. 13, February 18, 2009, Follow Up Intelligence Report;
- MCD Divisional Order No. 14, February 18, 2009, Investigator's Working Folder Audit Procedures;
- MCD Divisional Order No. 15, February 18, 2009, Integrated Case Briefing System;
- MCD Divisional Order No. 16, August 27, 2009, Privacy Guidelines for Evaluation Environment Initiative;
- MCD Divisional Order No. 17, March 16, 2010, Security Procedures for Major Crimes Division;
- Special Order No. 1, January 2, 2012, Reporting Incidents Potentially Related to Foreign or Domestic Terrorism – Revised and Renamed;
- Suspicious Activity Report, Form 3.24;
- Suspicious Activity Report Notebook Divider, Form 18.30.03;

Mr. Michael Price
Mr. Emin Akopyan
Page 5
14.4

The "Anti-Terrorism Intelligence Section Audit, Fiscal Year 2009/2010" is available in the Office of the Inspector General's public website, www.OIGLAPD.lacity.org. Click on the REPORTS link. If you prefer, I can provide you with a hardcopy of the audit upon receipt of the applicable duplicating fee. Please see the enclosed invoice.

The Department Manual is available, at no cost, in the Department's public website, www.LAPDOnline.org. If you prefer, I can provide you with a hardcopy of Department Manual Volume 3, Section 568, Radio and Electronic Investigation Equipment upon receipt of the applicable duplicating fee. Please see the enclosed invoice.

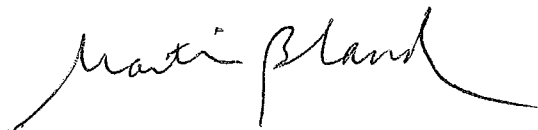
The following materials have also been located; however, these materials are exempt from public disclosure pursuant to Sections 6254(k), Section 6255 and/or Evidence Code Section 1040 as stated previously:

- Joint Regional Intelligence Center / LA-RTTAC Bulletin, October 29, 2008, (U) Identifying Suspicious Photography;
- Seven Signs of Terrorism; and
- PowerPoint – Sovereign Citizens

Any correspondence regarding this matter should include a copy of this letter and be directed to the Los Angeles Police Department - Discovery Section, 201 North Los Angeles Street, Space 301, Los Angeles, California 90012. If you have any questions regarding this correspondence, please contact Management Analyst David Lee of the Discovery Section at (213) 978-2152.

Very truly yours,

CHARLIE BECK
Chief of Police



MARTIN BLAND, Senior Management Analyst
Officer-in-Charge, Discovery Section
Risk Management Division

Enclosure

**LOS ANGELES POLICE DEPARTMENT
RISK MANAGEMENT DIVISION – DISCOVERY SECTION**

INVOICE FOR

**PUBLIC
RECORDS**

**BOR ADMINISTRATIVE
RECORD**

Requested By: Michael Price and Emin Akopyan **Date:** 03/16/12

Officer/Serial No.: Not applicable **Box File No.:** Not applicable

CPRA Reference No.: C12-1200018 **Analyst:** David Lee

Documents Provided	Pages	Fee*
Major Crimes Division (MCD) Standards and Procedures	38	Paid
Audit of Anti-Terrorist Intelligence Section (Phase I), Fiscal year 2006/2007	13	Paid
Anti-Terrorism Intelligence Section Audit, Fiscal year 2008/09	8	Paid
Anti-Terrorism Intelligence Section Audit, Fiscal Year 2009/2010	8	.80
MCD Divisional Order No. 1, April 12, 2006, Intelligence Reporting Procedures for Anti-Terrorism Intelligence Section Function	3	.30
MCD Divisional Order No. 2, April 12, 2006, Investigators Working Folder for the Anti-Terrorism Intelligence Section Function	2	.20
MCD Divisional Order No. 3, April 12, 2006, Security of Intelligence Files for the Anti-Terrorism Intelligence Section Function	2	.20
MCD Divisional Order No. 4, April 12, 2006, Surveillance Logs for the Anti-Terrorism Section Intelligence Function	1	.10
MCD Divisional Order No. 5, April 12, 2006, Analysis Unit Information and Data Storage for the Anti-Terrorism Intelligence Section Function	2	.20
MCD Divisional Order No. 6, April 12, 2006, Surveillance and Field Observations for Anti-Terrorism Intelligence Section Functions	2	.20
MCD Divisional Order No. 7, April 12, 2006, Undercover Investigations for Anti-Terrorism Intelligence Section Functions	1	.10
MCD Divisional Order No. 8, April 12, 2006, Dissemination of Intelligence Information	2	.20
MCD Divisional Order No. 9, April 12, 2006, Use of LACLEAR for All Investigations	2	.20
MCD Divisional Order No. 10, November 20, 2006, Initial Lead and Preliminary Investigation Time Limits	2	.20
MCD Divisional Order No. 11, March 16, 2007, Investigator's Working Folder (Amendments)	2	.20
MCD Divisional Order No. 12, October 30, 2008, Surveillance Approval Procedure	1	.10
MCD Divisional Order No. 13, February 18, 2009, Follow Up Intelligence Report	1	.10
MCD Divisional Order No. 14, February 18, 2009, Investigator's Working Folder Audit Procedures	1	.10
MCD Divisional Order No. 15, February 18, 2009, Integrated Case Briefing System	1	.10
MCD Divisional Order No. 16, August 27, 2009, Privacy Guidelines for Evaluation Environment Initiative	3	.30
MCD Divisional Order No. 17, March 16, 2010, Security Procedures for Major Crimes Division	2	.20
	Subtotal	3.80

* Admin Code, Div 12, Chapter 2, Art 4
Admin Code, Div 22, Chapter 11, Art 8

**LOS ANGELES POLICE DEPARTMENT
RISK MANAGEMENT DIVISION – DISCOVERY SECTION**

INVOICE FOR

**PUBLIC
RECORDS**

**BOR ADMINISTRATIVE
RECORD**

Requested By: Michael Price and Emin Akopyan **Date:** 03/16/12

Officer/Serial No.: Not applicable **Box File No.:** Not applicable

CPRA Reference No.: C12-1200018 **Analyst:** David Lee

Documents Provided	Pages	Fee*
Subtotal from Page 1		3.80
Subtotal from Page 2		14.70
TOTAL		18.50

* Admin Code, Div 12, Chapter 2, Art 4
Admin Code, Div 22, Chapter 11, Art 8

Make your check/money order payable to the LAPD. If you wish, you may obtain the documents at our public counter. Please ask to speak with the assigned analyst. Please note that only checks or money orders are accepted at the counter.

Pick-up Hours: 8:00 a.m. – 4:30 p.m.
Monday – Friday
excluding holidays

Location: LAPD – Discovery Section
201 N. Los Angeles St., Space 301
Los Angeles, CA 90012

Note: Please include “CPRA-DL” and the CPRA reference number on your check/money order. If you have any questions, please contact Management Analyst David Lee at (213) 978-2152.

LOS ANGELES POLICE COMMISSION

BOARD OF
POLICE COMMISSIONERS

JOHN W. MACK
PRESIDENT

VACANT
VICE PRESIDENT

ROBERT M. SALTZMAN
ALAN J. SKOBIN
DEBRA WONG YANG

MARIA SILVA
COMMISSION EXECUTIVE ASSISTANT I



ANTONIO R. VILLARAIGOSA
MAYOR

RICHARD M. TEFANK
EXECUTIVE DIRECTOR

DJANGO SIBLEY
ACTING INSPECTOR GENERAL

EXECUTIVE OFFICE
POLICE ADMINISTRATION BUILDING
100 WEST FIRST STREET, SUITE 134
LOS ANGELES, CA 90012-4112

(213) 236-1400 PHONE
(213) 236-1410 FAX
(213) 236-1440 TDD

March 23, 2010

BPC #10-0128

The Honorable Public Safety Committee
City of Los Angeles
c/o City Clerk's Office
City Hall, Room 395
Los Angeles, CA 90012

Attention John White:

RE: AMENDMENT TO MAJOR CRIMES DIVISION STANDARDS AND
PROCEDURES

At the regular meeting of the Board of Police Commissioners held Tuesday, March 23, 2010, the Board APPROVED the Department's report relative to the above matter.

This matter is being forwarded to you for approval.

Respectfully,

BOARD OF POLICE COMMISSIONERS

A handwritten signature in cursive script that reads "Maria Silva".

MARIA SILVA
Commission Executive Assistant I

Attachment

c: Chief of Police

BPC #10-0128 SE

INTRADEPARTMENTAL CORRESPONDENCE

March 17, 2010
1.15

RECEIVED

MAR 17 2010

TO: The Honorable Board of Police Commissioners

POLICE COMMISSION

FROM: Chief of Police

Adm J. Paul 3/18/10

SUBJECT: AMENDMENT TO MAJOR CRIMES DIVISION STANDARDS AND PROCEDURES

RECOMMENDED ACTIONS

- 1. That the Board of Police Commissioners (Board) REVIEW, APPROVE, and FORWARD to the Los Angeles City Council's Public Safety Committee the amended Major Crimes Division Standards and Procedures incorporating access of the Inspector General into the Secure Working Environment/Sensitive Compartmentalized Information Facility (SWE/SCIF).

DISCUSSION

The Los Angeles Police Department (LAPD) reached an agreement with the FBI to achieve a satisfactory level of civilian oversight relative to the LAPD SWE/SCIF as memorialized in the amended Major Crimes Division (MCD) Standards and Procedures. The amendments to the MCD Standards and Procedures include the following: Anti-Terrorism Division is now Major Crimes Division; The Board of Police Commissioners utilizes the Inspector General to conduct audits and ensure compliance with the standards and protocols; Section H (under Public Access to Information Standards and Procedures), page 33 and 34, and 35, has been added incorporating civilian oversight of the LAPD SWE/SCIF. Police Commission President John Mack and Police Commissioner Robert Saltzman have both reviewed this agreement and concur that it achieves a satisfactory level of civilian oversight. Additionally, the former LAPD Inspector General, Andre Birotte, who has since been appointed the United States Attorney for the Central District of California, has also reviewed and approved the agreement, believing it satisfies the Department and City's civilian oversight principle

This agreement has also been memorialized in the Standard Operating Procedures and Physical Security Requirements for the Sensitive Working Environment/Sensitive Compartmentalized Information Facility (SWE/SCIF), a confidential document not intended for public disclosure. The proposed amendments address City Council Motion #09-0021 made on November 4, 2009 relative to civilian oversight and the Police Commission's purview over the LAPD SWE/SCIF.

The LAPD SWE/SCIF will be utilized by the Joint Terrorism Task Force (JTTF), which consists of Los Angeles Police Department and Federal Bureau of Investigation (FBI) personnel. The Inspector General, working on behalf of the Police Commission, will have the appropriate security clearances to access the LAPD SWE/SCIF and will be entitled to inspect, audit, and review documents to ensure proper oversight.

The Honorable Board of Police Commissioners

Page 2

1.15

The development of this SWE/SCIF will greatly improve communication and coordination among federal, state, and local organizations toward the common goal of enhancing the information sharing environment in support of the National Strategy for Information Sharing.

Respectfully,



CHARLIE BECK
Chief of Police

BOARD OF
POLICE COMMISSIONERS
Approved *March 23, 2010*
Secretary *Maria Silva*

Attachments



**THE LOS ANGELES POLICE DEPARTMENT, MAJOR CRIMES
DIVISION STANDARDS AND PROCEDURES APPROVED BY THE
LOS ANGELES BOARD OF POLICE COMMISSIONERS ON:**

PREAMBLE

The Board of Police Commissioners (Board) recognizes terrorist activity as the existence in society of individuals and groups who plan, threaten, finance, aid/abet, attempt or perform unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.

The right of public expression through demonstration is expressly recognized and shall not, absent the reasonable suspicion to believe that there may be a potential for a "significant disruption of the public order," as defined in these Standards and Procedures, be subject to Major Crimes Division investigation that involves the maintenance of intelligence files.

Recognizing that terrorist-related intelligence information, properly gathered, analyzed, stored, maintained and disseminated, is essential to the performance of the Department's mandated duty to protect the public through crime prevention, the Board establishes these Standards and Procedures to provide for the legitimate needs of law enforcement while, at the same time, steadfastly respecting all constitutional and statutory rights guaranteed to every individual.

Generally, the focus of an intelligence investigation is strategy oriented. It focuses on the goals or potential of an individual, group or enterprise rather than on specific violations of law. The objective is not arrest and prosecution of suspects but rather the detection, collection, analysis and dissemination of information for the purpose of developing a strategy for crime prevention. Criminal investigations are case-oriented and focus on specific violators of law and specific violations for the purpose of arrest and prosecution after a crime has been committed.

These Standards and Procedures pertain only to Major Crimes Division's Intelligence function. They do not pertain to any Department function that is primarily responsible for conducting criminal investigations and does not maintain "Intelligence Files" as defined in these Standards and Procedures.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

I. DEFINITION OF TERMS

Agent Provocateur: An individual employed, directed, encouraged or allowed to associate with target members or groups in order to incite them to illegal action.

Attempt: An act done with intent to commit a crime and tending to, but falling short of, its commission.

Dissemination: The communication of any Major Crimes Division Intelligence File information to any person not assigned to Major Crimes Division's direct chain of command. All disseminations must be based upon a right to know and need to know.

File: A collection of information including, but not limited to, reports, photographs, documents, printed materials, tape recordings, videotape, computer information or other writings that are kept separately from Intelligence Files. A File may include Initial Lead, Preliminary Investigation, Intelligence Control Center, or Terrorist Threat Assessment Center information.

Informant: Generally, an informant is a person who provides information on a recurring basis and/or in exchange for consideration regarding specific criminal activity and who acts under the direction of an investigator.

Initial Lead Investigation: The lowest level of intelligence investigative activity which allows a limited follow-up of initial lead information, generally received from the public but may include Department and other law enforcement sources; of such a nature that some follow-up as to the possibility of terrorist activity is warranted. The Initial Lead Investigation threshold need not rise to the reasonable suspicion standard of a Preliminary Investigation and shall be concluded within a 60-day period. Initial lead information shall be stored separately from intelligence files. Only information that meets the reasonable suspicion standard, based on reliable information, may be placed in intelligence files.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Intelligence Control Center: A temporary function performed by Department personnel to gather and coordinate intelligence information during the course of a potential or actual unusual occurrence.

Intelligence File: An Intelligence File contains the investigative intelligence information gathered, received, developed, analyzed and maintained pursuant to an open Intelligence Investigation, for the purpose of identifying terrorist individuals, terrorists groups, and victims of terrorism.

Investigator's Working Folder: The Working Folder is retained by the assigned investigator and is specifically designated to contain the investigative materials gathered, received, and developed for the specific purpose of updating an approved ongoing Open Intelligence Investigation. However, the Working Folder shall not be part of the Open Intelligence File.

LAPD Sensitive Work Environment (SWE)/Sensitive Compartmented Information Facility (SCIF): A facility requiring a national security clearance for access, housed within the LAPD Police Administration Building, in which classified FBI Joint Terrorism Task Force (JTTF) directed intelligence investigations are processed and handled by JTTF members, assigned to CT 10.

Maintenance: The process of recording, collating, analyzing, evaluating, indexing, updating, securing, retaining, and purging Intelligence File information gathered pursuant to a Major Crimes Division Open Intelligence Investigation.

Monitoring: The short-term or preliminary act of observing or watching the activities of an individual or organization by Major Crimes Division Intelligence investigators for the purposes of gathering information relevant to an Initial Lead Investigation, Preliminary Intelligence Investigation or Open Intelligence Investigation. This short-term monitoring activity shall not rise to the level of "Surveillance" as defined in these Standards and Procedures.

Need to Know: A precondition for the communication of intelligence information to entities outside Major Crimes Division or its immediate chain of command.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Open Investigation: An intelligence investigation which has met the reasonable suspicion standard, is based on reliable information and has been approved by the Commanding Officer, Major Crimes Division.

Organizations: Any association or group of individuals.

Pending Activity: A future event possibly requiring operational planning for policing or police services.

Plan: Organized activity by individuals in preparation for the accomplishment of an illegal action involving possible terrorist activity.

Preliminary Investigation: A limited intelligence investigation approved by the Commanding Officer, Major Crimes Division, to develop existing information to the point of reliability in order to establish reasonable suspicion based on reliable information.

Reasonable Suspicion: An honest belief, based on known articulable circumstances, which would cause a reasonable and trained law enforcement officer to believe that some activity, relating to a definable criminal activity or enterprise, may be occurring or has a potential to occur. (This term is in accordance with Department of Justice definition: 28 CFR Part 23).

Reliable Information: Information that is trustworthy or worthy of confidence.

Right to Know: The authority or privilege to receive Major Crimes Division Intelligence information.

Significant Disruption of the Public Order: Pertains only to public demonstrations involving unlawful acts which can reasonably be expected to result in death, serious bodily injury or property damage and which are intended to have such results to further societal objectives, to influence societal action or to harass on the basis of race, religion, national origin, or sexual orientation. The mere fact of a potentially large demonstration shall not, by itself, constitute a significant disruption of the public order.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Storage/Storing: To provide a place in which any file is kept for the purpose of records retention and not for the purpose of updating. All stored information is kept separate from Open Intelligence Files.

Surveillance: The continuous or prolonged observation of a targeted individual or group by clandestine means for the purpose of collecting information material to an approved Preliminary Intelligence Investigation or Open Intelligence Investigation.

Target: The subject of an approved investigation.

Terrorist Activity: Individual(s) or group(s) who plan, threaten, finance, aid/abet, attempt or perform unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.

Note: Activity as it relates to individuals involved in public demonstrations must rise to the level of "Significant Disruption of the Public Order" standard, as defined in these Standards and Procedures.

Terrorist Threat Assessment Center: A permanent entity of the Department, staffed by Major Crimes Division personnel to receive, analyze, investigate and communicate terrorist related information.

Threaten: The advocacy of, or a statement of intention to commit a criminal act where such advocacy appears to be a viable threat.

Undercover Investigation: An approved intelligence investigation involving the use of an undercover officer who clandestinely obtains information about individuals or organizations through the development of ongoing relationships with such individuals or organizations

Undercover Officer: A Los Angeles Police Officer who, pursuant to an approved terrorist investigation, clandestinely obtains information about individuals or organizations through the development of ongoing relationships with such individuals or organizations.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Unusual Occurrence (UO): An event involving potential or actual personal injury and/or property damage arising from fire, flood, storm, earthquake, tidal wave, landslide, wreck, enemy action, civil disturbance, or other natural or man-caused incident necessitating the declaration of a Tactical Alert or Mobilization. (*Emergency Operations Policies & Procedures - Volume 1 of the LAPD Emergency Operations Guide 11*)

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

II. STATEMENT OF PRINCIPLE

- A. These Standards and Procedures govern the collection, maintenance, storage and dissemination of intelligence information by the Major Crimes Division intelligence function. These Guidelines also govern the collection, maintenance and dissemination of intelligence information by all other functions and personnel of LAPD when their primary responsibility is gathering intelligence information.

In establishing these Guidelines, the Board of Police Commissioners provides for the legitimate needs of law enforcement within limits created by constitutional and statutory protections which guarantee rights: (1) of privacy, (2) to receive, hold and express ideas, (3) to dissent freely, (4) to write and to publish, (5) to petition for the redress of grievances, (6) and to associate publicly and privately for any lawful purpose.

- B. In reaching the delicate balance of protecting the rights of individuals and providing for effective prevention of terrorist activity, community peace, and in recognizing that no other aspect of the Department's duties requires such detached and sensitive judgments on the part of individual peace officers and that nowhere else is reverence for the law more demanded, the Board affirms the following principles:
1. The Department has a policy of absolute prohibition against the use of illegal or unauthorized methods of collecting, maintaining or disseminating intelligence information; a policy which shall remain in full force and effect. The Commanding Officer, Major Crimes Division, shall report to the Chief of Police any intelligence activity reasonably believed to be contrary to the scrupulous observation of this principle.
 2. The Department considers it both unnecessary and wrong to maintain an intelligence file on any individual or organization unless the reasonable suspicion standard for an Open Intelligence Investigation according to these Standards and Procedures has been met.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

3. Major Crimes Division Intelligence Section personnel shall not collect, maintain or disseminate information about an individual's sexual, political or religious activities, beliefs or opinions unless such information is material to an approved investigation.
4. Major Crimes Division Intelligence Section personnel shall exercise due caution and discretion in the use of information, collected, maintained and disseminated so as not to interfere with the lawfully exercised rights of any person.

III. FUNCTIONS AND OBJECTIVES

- A. The primary objective of Major Crimes Division's Intelligence Operation is the prevention of terrorist activity in the City of Los Angeles and environs by:
 1. Identifying terrorist trends.
 2. Examining terrorist tactics, developing terrorist profiles, assessing terrorist threats, and developing information to protect potential targets.
 3. Investigating, identifying and monitoring individuals and groups that may be engaged in terrorist activity.
 4. Maintaining intelligence files on individuals and groups that may be engaged in terrorist activity.
 5. Assessing and analyzing the capabilities of terrorist individuals or groups, and providing concerned Department entities with sufficient information to thwart their terrorist goals.
 6. Assisting other subdivisions of the Department and other law enforcement agencies to prevent terrorist activities.
- B. A secondary objective of Major Crimes Division Intelligence Section is to advise the Chief of Police and other executive management personnel about pending events which may require operational awareness or planning for policing or police services.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

- C. The focus of Major Crimes Division activity is on the safety of persons and protection of property through the prevention of terrorism in the City of Los Angeles. The Board is aware, however, that terrorists do not respect municipal boundaries. It is therefore appropriate to gather intelligence on international terrorists and other persons and organizations whose conduct can reasonably be expected to affect the City of Los Angeles. Similarly, information may be gathered with respect to persons residing in Los Angeles who may commit acts of violence elsewhere and then return. In fulfilling these responsibilities, Major Crimes Division may work with other agencies and pursue investigations into other jurisdictions.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

IV. INTELLIGENCE INVESTIGATIVE ACTIVITY

Generally, the focus of an intelligence investigation, (usually of a long-term nature), is the group or individual enterprise, rather than just individual participants and specific unlawful acts. The immediate purpose of such an investigation is to obtain information concerning the nature and structure of a group or enterprise, including information relating to the group's membership, finances, geographical dimensions, past and future activities, and goals. This is done with a view toward detecting and preventing unlawful acts which are intended to have such results to further their societal objectives, to influence societal action or to harass on the basis of race, religion, national origin, or sexual orientation.

The objective of the Major Crimes Division intelligence investigation is not the arrest and prosecution of suspects, but rather the detection, collection, analysis and dissemination of information for the purpose of crime prevention.

A. LEVELS OF INTELLIGENCE INVESTIGATIVE ACTIVITY

The Standards and Procedures for Major Crimes Division provide for a graduated level of investigative activity and allow Major Crimes Division the necessary flexibility to act well in advance of the commission of a planned terrorist attack. The three levels of investigative activity are: (1) Initial Lead Investigations, (2) Preliminary Investigations, and (3) Open Investigations.

Whether it is appropriate to open an investigation immediately, or first to engage in a limited follow-up of lead information, depends on the circumstances presented. If the available information shows at the outset that the threshold standard for a Preliminary or Open Investigation is satisfied, then approval to conduct the appropriate investigative activity may be requested immediately, without progressing through the more limited investigative stage. However, if the reasonable suspicion standard has not been met, only an Initial Lead Investigation may go forward.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Major Crimes Division personnel shall operate the Terrorist Threat Assessment Center which is responsible for the follow-up of Initial Lead Investigations involving possible terrorist-related information.

INITIAL LEAD INVESTIGATIONS

The lowest level of investigative activity is the prompt and limited follow-up of initial leads, many of which are initiated by the public. Checking of leads should be undertaken whenever information is received of such a nature that some follow-up as to the possibility of terrorist activity is warranted. This limited activity should be conducted with an emphasis toward promptly determining whether further investigation, either a Preliminary Investigation or an Open Investigation, should be conducted.

Many initial investigative leads from the public and other sources are expected to be somewhat vague and may not meet the reasonable suspicion standard for a Preliminary or Open Investigation. However, public safety demands a limited but prompt follow-up investigation. The authority to conduct inquiries, short of a Preliminary or Open Investigation, allows Major Crimes Division to respond in a measured way to ambiguous or incomplete information.

INVESTIGATIVE TECHNIQUES FOR INITIAL LEAD INVESTIGATIONS

The following investigative techniques are authorized for Initial Lead Investigations:

- (a) Examination of records available to the public (open source);
- (b) Examination of LAPD records;
- (c) Examination of available federal, state, local government records, etc;
- (d) Interview of the person reporting;
- (e) Interview of the potential subject;
- (f) Interview of witnesses;
- (g) Monitoring.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

Initial Lead Investigations shall be completed within 60 days from the date of receipt of the specific lead. All materials collected during the Initial Lead Investigation shall be stored separately from Intelligence Files unless the initial investigation results in an approved Open Investigation.

PRELIMINARY INVESTIGATIONS

The next level of investigative activity, a Preliminary Investigation, should be undertaken when there is information or an allegation which indicates the possibility of terrorist activity. Preliminary Investigations are based on reasonable suspicion only and are for the purpose of determining whether or not the information or allegation can be developed to the point of reliability.

A Preliminary Investigation may be initiated when:

- Reasonable suspicion exists that an individual or organization may be planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts;
- The results of which are intended to further their societal objectives, influence societal action or harass on the basis of race, religion, national origin, or sexual orientation.

A Preliminary Investigation shall commence when the Commanding Officer, MCD, approves the request. The Preliminary Investigation shall not exceed 120 days.

INVESTIGATIVE TECHNIQUES FOR PRELIMINARY INVESTIGATIONS

A Preliminary Investigation shall not involve the use of electronic surveillance that requires a court order. All other approved investigative methods are authorized.

OPEN INVESTIGATIONS

The commencement of each Open Investigation shall be approved by the Commanding Officer, MCD, who shall ensure the reasons for initiating the investigation meet the required threshold as stated below.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

An Open Investigation may be initiated when there exists, a reasonable and articulated suspicion based upon reliable information that an individual or organization may be:

- Planning, threatening, attempting, performing, aiding/ abetting, or financing unlawful acts;
- The results of which are intended to further their societal objectives, influence societal action or harass on the basis of race, religion, national origin, or sexual orientation.

INVESTIGATIVE TECHNIQUES FOR OPEN INVESTIGATIONS

All lawful investigative technique may be used in an Open Investigation.

B. PENDING ACTIVITY REPORTS

1. Major Crimes Division Intelligence Section personnel may collect and disseminate information regarding events significant to the City of Los Angeles. Such events include, but are not limited to: parades, demonstrations, dignitary visitations, and VIP appearances, which require operational awareness or planning for policing or police services.
2. Pending Activity Reports are subject to the constraints delineated in the Preamble to these Standards and Procedures and shall be stored separately from Major Crimes Division's Intelligence Files.
3. Pending Activity Reports shall be transmitted to the appropriate Department operational entities immediately upon completion and approval. A copy shall be filed at the Department Command Post. Major Crimes Division shall maintain a log of such reports for audit purposes.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

C. INTELLIGENCE CONTROL CENTER FUNCTION

1. The Intelligence Control Center collects and disseminates intelligence information gathered during an unusual occurrence or a potential unusual occurrence.
2. Major Crimes Division Intelligence Section personnel may be temporarily assigned to the Intelligence Control Center.
3. While completing the work of the Intelligence Control Center, members of Major Crimes Division are not subject to these Standards and Procedures.
4. All materials gathered, organized and produced during an Intelligence Control Center activation shall be stored separately from Major Crimes Division's intelligence files. Information obtained during an Intelligence Control Center Activation that may be material to an intelligence investigation may only be accessed with approval of the Commanding Officer, Major Crimes Division.

D. TERRORIST THREAT ASSESSMENT CENTER FUNCTION

1. The Department has established the Terrorist Threat Assessment Center as the permanent clearinghouse for terrorist-related information specific to the City of Los Angeles or that may impact the City of Los Angeles.
2. The Terrorist Threat Assessment Center shall be responsible for receiving, analyzing, disseminating and conducting a limited intelligence investigation of terrorist-related threats and information.
3. In order to facilitate the dissemination of terrorist-related threats, the Terrorist Threat Assessment Center shall maintain special liaison with appropriate Department and City functions, as well as the Los Angeles County Terrorism Early Warning Group, the California Anti Terrorism Information Center,

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

The United States Department of Homeland Security and the Federal Bureau of Investigation.

4. The Terrorist Threat Assessment Center shall be staffed by Major Crimes Division Intelligence Section personnel. While completing the work of the Terrorist Threat Assessment Center, Major Crimes Division Intelligence Section personnel are subject to these Standards and Procedures. All materials gathered, organized and produced during a Terrorist Threat Assessment Center investigation shall be stored separately from Major Crimes Division Intelligence Files unless the Initial Lead Investigation develops into an approved Open Intelligence Investigation.

E. MULTI-AGENCY TASK FORCE

Members of Major Crimes Division, with the approval of the Chief of Police, may be assigned to a multi-agency task force. Major Crimes Division personnel that are members of a multi-agency task force, headed by another agency, may engage in the investigative methods legally authorized for use by that agency, as long as those methods do not violate current laws.

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

V. LIMITATIONS AND PROHIBITIONS

Major Crimes Division Intelligence Section personnel shall recognize and abide by legal and policy limitations placed upon their investigations. In addition to the parameters established by these Standards and Procedures, the following specific limitations and prohibitions apply to Major Crimes Division Intelligence Section personnel and investigations:

- A. No member of Major Crimes Division may engage in any unlawful activity in the collection, maintenance or dissemination of intelligence data or information.
- B. No member of Major Crimes Division may knowingly employ or direct any individual to illegally engage in the collection, maintenance or dissemination of intelligence data or information.
- C. No member of Major Crimes Division may act or knowingly engage another individual to act as an agent provocateur.
- D. No member of Major Crimes Division may employ the use of restricted electronic surveillance equipment without conforming to policy as stated in the Department Manual.
- E. Initial Lead Investigations shall not exceed 60 days.
- F. A Preliminary Investigation shall not exceed 120 days.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

VI. UNDERCOVER INVESTIGATIONS, SURVEILLANCE AND INFORMANTS

The Board of Police Commissioners recognizes its critical task in balancing the needs of law enforcement in its efforts to protect the broader society, versus the need to safeguard individual rights guaranteed by a democratic people. Necessarily involved in this process is the recognition that a few groups and individuals espouse, finance, aid or abet violence and/or the wanton destruction of property and that many such groups have attained a high level of criminal sophistication. It is that same criminal sophistication that causes law enforcement to resort to the use of undercover operations, surveillance and informants to counteract their progress. However, as serious as these concerns are, they do not outweigh the previously mentioned societal rights. It is imperative that constitutionally guaranteed rights remain the focal point when utilizing these investigative methods. The law enforcement intelligence community must therefore make optimum use of appropriate resources when available and maximize its capabilities while operating within legal and ethical constraints.

A. UNDERCOVER INVESTIGATIONS – SAFEGUARDS

An investigation involving the infiltration of an organization or the development of an ongoing relationship with an individual by an undercover officer is the most reliable tool for information gathering by law enforcement. The value of the information so obtained has been repeatedly demonstrated in the prevention of terrorist activity and other criminal acts.

The use of information gained in undercover operations is greatly diminished if the manner in which it is obtained casts aspersions upon the conduct of the undercover officer. The conduct of the officer and control of the investigation is therefore critical to minimize interference with lawfully exercised rights. The Chief of Police and the Board of Police Commissioners are charged with great responsibility in authorizing undercover investigations, and should do so only after all other reasonable investigative methods have been determined to be impractical or ineffective to accomplish the objectives of the investigation.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

It is most important that the selection, training, and oversight of undercover personnel receive the utmost attention. It is also imperative that undercover officers understand constitutional and statutory rights which govern their intelligence gathering limits.

The Chief of Police shall have the authority and responsibility to use all resources available to protect the identity and safety of an undercover officer and to protect the confidentiality of information obtained in an undercover investigation.

These Standards and Procedures establish the limits and guidelines by which the conduct of Major Crimes Division Intelligence Section personnel and undercover investigative techniques are controlled.

B. UNDERCOVER INVESTIGATION COMMITTEE

The President of the Board of Police Commissioners or another Commissioner designated by the President shall comprise the Undercover Investigation Committee. The Commissioner comprising that Committee shall serve a maximum of three consecutive years, and shall have the duties and assignments as prescribed by these Guidelines.

C. UNDERCOVER INVESTIGATION – AUTHORIZATION

1. Undercover investigations (i.e. use of an undercover officer) may be initiated subject to the following safeguards:

- a. The targeted individual(s) and/or organization have been approved for a Preliminary or Open Investigation.
- b. No undercover investigation shall be commenced without the written approval of the Chief of Police and the Committee. Prior to the actual commencement of any infiltration by an undercover officer, the requirements set forth below must be met:

Exception: In an emergency involving a life threatening situation where the Undercover Committee is unavailable, an undercover investigation may be commenced with the approval of

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

the Chief of Police. Telephonic notification to the Undercover Committee shall be made as soon as possible and written approval from the Undercover Committee shall be requested within 72 hours.

- 1) The undercover investigation application shall be signed by the Commanding Officer, Major Crimes Division, through the chain of command to the Chief of Police;
- 2) All supporting assertions of fact in the application shall be contained in affidavits (or declarations under oath); said affidavits or declarations may be based on hearsay evidence. The requirements for these affidavits shall meet the requirements of these Guidelines (and shall not be equated with the requirements for a search warrant).
- 3) The application shall include information which bears upon:
 - (a) Whether there is a reasonable suspicion to believe that the target individual or organization may be planning, threatening, financing, aiding/abetting, attempting or performing unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation;
 - (b) The expected results of the undercover operation in terms of prevention of terrorist activity;
 - (c) The anticipated manner in which the undercover operation will be conducted, including likely individuals and organizations who will be contacted;
 - (d) The authorized duration of the undercover investigation and the provision for periodic review;
 - (e) What other methods have been previously used and why Major Crimes Division believes that an undercover

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

investigation is the only practical means to accomplish the objectives of the investigation;

- (f) If the Department intends that the undercover officer shall infiltrate a non-target organization, then there shall be included additional information which clearly indicates the need to become a member of the non-target organization. No information on the non-target organization or its members will be reported in any intelligence file, unless there is reasonable suspicion to believe that the non-target organization, or members of the non-target organization, may be involved in terrorist activity or in cases of public demonstration, activities which may have the potential to significantly disrupt the public order.
- c. The Committee shall not issue written authorization initiating an undercover investigation of an individual or organization unless the Committee agrees that all of the following requirements have been met:
 - 1) The application has been signed by the officials listed in subparagraph C.1.b(1) above;
 - 2) All supporting assertions of fact are sworn to under oath; and
 - 3) The Committee has consulted with legal counsel for advice, as necessary.

The Committee shall maintain a written record of compliance with this subparagraph.

- 4) The Committee renders written findings that:
 - a. There is an approved Preliminary or Open Intelligence Investigation which meets the respective reasonable suspicion standard;

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

- b. That other means are unavailable or ineffective to achieve the investigative objectives of the Department; and
 - c. That the interests of privacy and free expression are outweighed by the nature and magnitude of the likely harm.
- 5) Where the Department seeks to infiltrate a non-target organization so that an undercover officer may infiltrate the target organization, the Committee shall render additional written findings that:
- a. All other means of obtaining sufficient information on the target organization either have been tried without success or are not practical; and
 - b. There is reasonable basis for believing that the presence of the undercover officer in the non-target organization will enable him/her to infiltrate the target organization as evidenced by the fact that:
 - c. Members of the target organization are also members of the non-target organization;
 - i. That the target organization recruits members from the active members of the non-target organization;
 - ii. That membership in the non-target organization is a condition of membership in the target organization; or
 - iii. There is a substantial link between the non-target organization and target organization, equal to those described in (i)-(iii) above, which otherwise justifies the undercover officer's infiltration of the non-target organization; provided, however, that this substantial link shall not be based solely on the evidence that:
 - I. The non-target organization espouses or holds the same political, social or economic

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

positions as the target organization (e.g. a non-violent organization which opposes nuclear power plants shall not be infiltrated in order to infiltrate a target organization which opposes nuclear plants by violent means unless there are other factors present);

- II. The non-target organization shares the same racial, religious or other status or concerns with the target organization.
- d. The interests in privacy and free expression of the non-target organization are outweighed by the nature and magnitude of the likely harm by the target organization. In this regard, the Committee shall consider, in part, former and other current infiltrations by undercover officers of the non-target organization.
 - e. Where the Committee finds that the application for an undercover investigation meets the requirements set forth in paragraph c.1-5 (Pages 16-17), it shall issue written authorization to conduct an undercover investigation under the following terms and conditions:
 - 1) Specifying the individual or organization that is the target of the undercover investigation;
 - 2) Setting forth limitations, if any, on the activities which can be engaged in by the undercover investigators with regard to the target individual or organization;
 - 3) Imposing a time limit on the undercover investigation, which, however, cannot exceed a period of one year with a semi-annual status review by the Undercover Committee;
 - 4) If the infiltration of a non-target organization also has been approved, the written confirmation shall include these additional terms and conditions:

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

- a) Specify the number of meetings of the non-target organization, which the undercover officer may attend without further approval of the Committee;
 - b) Set forth limitations, if any, on the activities which can be engaged in by the undercover officer in the non-target organization;
 - c) Require quarterly reports from Major Crimes Division regarding the steps taken by the undercover officer to infiltrate the target organization, estimates of the additional time necessary to infiltrate the target organization and an explanation of the reason why the target has not yet been infiltrated;
 - d) Require quarterly reviews by the Committee on whether the infiltration of the non-target organization still meets the requirements set forth in paragraph c. 1-5 (Pages 16-17), above.
- f. The Committee shall make its decision within 72 hours of receipt of the application of the Department. In the event that the Committee is unable to render a decision within this time frame, the Chief of Police may present the matter to the full Board for a determination. The Board's determination shall be made in accordance with the Undercover Standards and Responsibilities Section of these Standards and Procedures.
- g. If the Department seeks to continue an undercover investigation after the initial one-year period, the Department shall request that the investigation be reviewed by the Committee.
- 1) The request for review shall include all information previously submitted and, in addition, shall contain information on all activities of the undercover officer during the preceding investigation, including all

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

organizations and individuals which were contacted by him/her in that time period.

- 2) The Committee shall issue written authorization to continue an undercover investigation of a target organization or individual only where in the preceding one-year period:
 - a) The undercover officer has obtained some reliable information that the target may still be a viable threat in terms of planning, threatening, financing, aiding/abetting, attempting or performing unlawful acts, the results of which are intended to further their societal objectives, to influence societal action, or to harass on the basis of race, religion, national origin, or sexual orientation.
 - b) The undercover officer has taken all reasonable steps to develop the necessary contacts with the target organization or individual so as to ascertain whether said target is conducting activities described in paragraph 2.a. above, but the undercover officer has been unable to develop such contacts through no fault of his/her own.
- h. Except as permitted in paragraph VI.C, no undercover investigation shall be conducted absent compliance with the above-mentioned procedures.
- i. Unless already approved under VI.C.L.c(4) above, during a duly authorized undercover investigation, an undercover officer may be present on two occasions in organizations which are not the subject of a Major Crimes Division Intelligence investigation. Once the undercover officer has attended two such meetings, functions, demonstrations or other activities (whether public or private), the attendance of the undercover officer at these

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

activities shall be reported in writing to the Commanding Officer, Major Crimes Division, the Chief of Police and the Committee. The undercover officer shall not attend any further meetings, functions, demonstrations or other activities of the non-target organization except under either of the following circumstances:

- 1) The failure of the undercover officer to attend such activities will expose him/her to immediate danger to his/her physical safety or jeopardize the fictitious identity of the undercover officer. In this event, the undercover officer's attendance at these additional activities of the non-target organization shall be reported in writing to the Commanding Officer, Major Crimes Division, the Chief of Police and the Committee.
- 2) The Committee gives written authorization for the undercover officer to attend further activities of the non-target organization for the purpose of maintaining a cover, but only in accordance with the guidelines and findings set forth in Section VI.C.1c(4).
- 3) The events and writings pertaining to (1) and (2) above shall be audited by the Commission pursuant to Section IX, infra, to ensure compliance with these Guidelines.

D. REVIEW BY THE BOARD OF POLICE COMMISSIONERS

1. Each member of the Board of Police Commissioners shall have the right to request a review by the entire Board of any decision by the Committee and to have access to such information as may be necessary to make a determination as to whether such a request is appropriate. In addition, in the event that the Committee does not confirm the infiltration by the undercover officer, the Chief of Police may request in writing that the proposed undercover investigation be reviewed by the entire Board. The Board in making its review shall:

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

- a. Consider each and all of the findings made by the Committee (including such other information as the Board may seek from the Committee);
- b. Prepare written findings if the Board rejects the decision of the committee. The written findings shall expressly recite the basis for, and facts upon which, the decision to override the Committee was made;
- c. Not override the Committee unless at least three votes in favor of said override are obtained; and
- d. Report to the public on an annual basis the number of decisions reviewed and the number of times the decision of the Committee was changed.

E. UNDERCOVER STANDARDS AND RESPONSIBILITIES

1. UNDERCOVER OFFICER STANDARDS

- a. **PRESENCE AT RELIGIOUS EVENTS:** Undercover officers shall take all reasonable steps to minimize any intrusion of religious ceremonies, meetings or discussions. Undercover officers shall not report on those events unless they relate to the undercover investigation.
- b. **PARTICIPATION IN PRIVILEGED INFORMATION EVENT:** Undercover officers shall, when possible, avoid attendance at a meeting which would involve information covered by California Evidence Code Sections 954 (Lawyer-Client Privilege), 980 (Privilege for Confidential Marital Communications), 992 (Confidential Communication Between Patient and Physician), 1012 (Confidential Communication Between Patient and Psychotherapist), and 1033 (Privilege of Penitent). If an undercover officer attends a meeting where privileged information is shared, the undercover officer shall not report or divulge the content of said meeting.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

NOTE: Undercover officers are exempt from this restriction if the holder of the privilege waives same as defined under California Evidence Code Sections 912, 956, 981, 997 and 1018.

- c. **PRESENCE AT EDUCATIONAL INSTITUTION:** If attendance by an undercover officer in an educational institution is required as part of the investigation, the officer shall not report on any activity associated with the institution which is not directly related to the investigation. The undercover officer shall take all reasonable steps to minimize any intrusion which his/her conduct might have in connection with the academic freedoms associated with the institution.
- d. **WRITTEN REPORTS:** Undercover officers shall not make written reports of their operations and activities.
- e. **TRAINING OF UNDERCOVER OFFICERS:** The Officer-in-Charge, Special Assignment Unit, shall ensure each undercover officer is familiar with these sections and is trained regarding acceptable standards of conduct.

2. UNDERCOVER RESPONSIBILITY

- a. **OFFICER'S RESPONSIBILITY:** An undercover officer who attends a meeting as described in VI.E. 1.a and VI.E. 1.b shall report attendance to an investigative or Special Assignment Unit supervisor.
- b. **SUPERVISOR'S RESPONSIBILITY:** An investigative or Special Assignment Unit Supervisor who becomes aware that an undercover officer has attended a meeting as described in VI.E.1.a. shall report such attendance to the Commanding Officer, Major Crimes Division.
- c. **COMMANDING OFFICER'S RESPONSIBILITY:** The Commanding Officer, Major Crimes Division, when notified that an undercover officer has attended two meetings, functions, demonstrations or other activities of any organization not

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

approved for infiltration, shall report such activity to Major Crimes Division's immediate chain of command.

NOTE: In connection with religious ceremonies, no reporting beyond the Commanding Officer, Major Crimes Division, is required if the religious nature of the group was considered at the time the undercover operation was approved. The undercover officer shall be directed not to attend any further such meetings, functions, demonstrations or activities of any organization not approved for infiltration unless:

Failure of the undercover officer to attend such activities will pose an immediate danger to the physical safety of the officer or jeopardize his/her identity. In this event, the undercover officer's attendance at these additional activities shall be reported to the Commanding Officer, Major Crimes Division, and Major Crimes Division's immediate chain of command who shall authorize attendance at further activities for the purpose of maintaining cover.

3. APPROVAL OF THE BOARD

Any request to modify current restrictions on acceptable conduct by undercover officers as cited in the Major Crimes Division confidential Procedural Manual shall be considered during an Executive Session of the Board in compliance with the Ralph M. Brown Act.

F. SURVEILLANCE AND INFORMANT OPERATIONS

Surveillance and informant operations are discussed in Major Crimes Division's confidential Procedural Manual. Inclusion of those operations in these Guidelines would have a detrimental effect on operational effectiveness and could jeopardize the safety of officers and informants.

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

VII. CONTROL OF INTELLIGENCE FILES

- A. The Commanding Officer, Major Crimes Division, shall be responsible for the establishment of written procedures to ensure the security of intelligence files. These procedures shall be made available to the Commission's Audit Committee or designee at any time to monitor compliance with these Guidelines.
- B. The Commanding Officer, Major Crimes Division, shall review all intelligence reports and pending activity reports, prior to their storage.
- C. Information collected by Major Crimes Division Intelligence Section personnel shall not be maintained unless it is material to an investigation authorized under these Standards and Procedures. However, recognizing a determination of materiality is not always possible when information is originally received, an investigator may record information until such time as a determination can be made. Such information shall not become part of the files maintained by Major Crimes Division, and shall be destroyed in accordance with record keeping procedures when it is determined that the information is not material. Initial inquiries and contacts, the working investigation notes, drafts or other writings shall be maintained in the investigator's working folder.
- D. No member of Major Crimes Division Intelligence Section may disseminate information from Major Crimes Division files to any individual or agency that does not have both a need and a right to the information.
- E. No member of Major Crimes Division Intelligence Section may provide a copy of an intelligence report to anyone outside of Major Crimes Division Intelligence Section and Major Crimes Division's immediate chain of command without the prior approval of the Commanding Officer, Major Crimes Division, or the Major Crimes Division Custodian of Records.
- F. Any member of Major Crimes Division Intelligence Section who copies, permits inspection of, or disseminates intelligence information from intelligence files shall record the date, name of officer disseminating, name of the individual receiving, the reason for the dissemination, the information disseminated, and its reliability.

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

- G. In the case of a joint investigation by Major Crimes Division Intelligence Section and another law enforcement agency, the Commanding Officer, Major Crimes Division, may authorize a free flow of information on the particular individual(s) and organization(s) being investigated, consistent with the Standards and Procedures of Major Crimes Division.
- H. Members of Major Crimes Division Intelligence Section shall not maintain or utilize the Division's intelligence materials outside of their official work location without the written approval of the Commanding Officer, Major Crimes Division.
- I. Any writing prepared to summarize the status or activities of an investigation other than that placed on LAPD Form 1.89 (Intelligence Report), shall be recorded on a LAPD Form 15.7 (Employee's Report). The Employee's Report shall be retained and filed by the Commanding Officer, Major Crimes Division, for a period of one-year, after which time it shall be purged at the discretion of the Commanding Officer.

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

VIII. PERSONNEL ADMINISTRATION

- A. Recognizing the importance and sensitivity of the duties performed by Major Crimes Division, the Department will exercise special care and attention to the selection, development, training, and retention of all personnel assigned to Major Crimes Division.
- B. These Standards and Procedures shall be distributed to, and made the subject of training for, all Major Crimes Division Intelligence Section personnel.
- C. All Major Crimes Division Intelligence personnel shall be required to acknowledge, in writing, their receipt of a copy of these Standards and Procedures, and their willingness to abide by the purpose, procedures, and spirit of its content.
- D. As with any other Department guideline or regulation, any willful or negligent violation of or deviation from these Standards and Procedures will be viewed as misconduct and be subject to appropriate disciplinary action.

**PUBLIC ACCESS TO INFORMATION
STANDARDS AND PROCEDURES**

IX. AUDITING AND OVERSIGHT

A. At least annually, the President of the Board of Police Commissioners shall appoint two Board members (hereinafter the "audit committee") to audit the operations of Major Crimes Division for compliance with these Standards and Procedures. The audit committee may enlist the assistance of the Inspector General and such support staff who shall be subject to a background examination and possess the requisite auditing and management expertise to ensure compliance with the Standards and Procedures.

The audit shall consist of, but not be limited to, the following:

- a. A review of all Major Crimes Division Intelligence regulations, rules and policies.
 - b. A review of all Major Crimes Division Intelligence investigations conducted in the prior year.
 - c. A review of all materials gathered, received, developed or maintained by Major Crimes Division Intelligence Section for intelligence purposes.
 - d. An oral interview of Major Crimes Division Intelligence Section personnel assigned to task forces wherein another agency is the lead agency and is in possession of all work product, to ensure that Major Crimes Division personnel are in compliance with these Standards and Procedures. This oral interview is to include MCD Intelligence Section personnel assigned to the LAPD SWE/SCIF (CT-10).
 - e. A written report setting forth the nature of the audit and the findings on compliance with these Standards and Procedures.
- B. The audit committee or their designated administrative auditor(s) may, at any time, conduct surprise audits or inspections as deemed appropriate to monitor compliance with these Standards and Procedures.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

- C. Based upon the audit, the administrative auditor(s), under the supervision of the audit committee, shall prepare a confidential written report for the entire Board.
- D. From the above confidential report, the Police Commission shall prepare annually, a public report of the audit on the preceding year's activities of Major Crimes Division.
- E. Annually, the Commanding Officer, Major Crimes Division, shall provide written certification that all current Major Crimes Division intelligence investigations have been internally reviewed and that those Major Crimes Division investigations which are no longer viable have been closed.
- F. The written justification for the commencement of an intelligence investigation shall be retained and reviewed by the Commission during the audit described in Section IX.
- G. The Board shall have the right to review the Major Crimes Division confidential Procedural Manual and approve those portions which pertain to prohibitions on undercover officer conduct previously included in these Standards and Procedures. Any changes to those provisions shall receive prior approval of the full Board, upon recommendation of the Intelligence Committee. Discussion of the contents of the confidential Procedural Manual shall be held in Executive Session of the Board, and shall remain confidential.
- H. Oversight and Auditing of Major Crimes Division Intelligence Section personnel assigned to the LAPD SWE/SCIF (CT-10) (see also, Standard Operating Procedures and Physical Security Requirements - SCIF).
 - 1. Upon receipt of the necessary security clearance(s), the Inspector General for the Los Angeles Board of Police Commissioners will be provided access to the LAPD SWE/SCIF for the purpose of oversight directed at LAPD CT-10 personnel.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

2. In accordance with existing Joint Terrorism Task Force (JTTF) protocols, it is understood that certain LAPD investigations will be converted by the FBI into FBI JTTF investigations when the FBI determines that those investigations meet investigative thresholds under the United States Attorney General Guidelines and the FBI's Domestic Investigations and Operations Guide. These investigations and records pertaining thereto will be maintained within the LAPD SWE/SCIF and are subject to FBI and United States Department of Justice (DOJ) internal inspection and/or auditing processes.¹
3. In order to meet the objectives of ensuring adherence to federal law pertaining to the confidentiality of files under the control of the FBI, while also accomplishing oversight responsibilities vested in the LAPD Inspector General, the LAPD IG will, in conformance with federal laws and regulations (and with the necessary clearance[s]), have access to audits or inspections conducted by the federal government concerning LAPD CT-10 personnel.
4. Additionally, where the LAPD IG determines that an inspection or audit of a particular facet of LAPD CT-10 personnel is necessary, the Special Agent in Charge of the FBI's Counterterrorism Division (CT SAC), will audit or inspect the particular facet and create a written report for the LAPD IG.
5. Should the IG determine that it is necessary to review classified investigative records/information in order to

¹ Specifically, primary oversight for compliance with the United States Attorney General's Guidelines for Domestic FBI Operations (AGG-Dom) and the FBI's Domestic Investigations and Operations Guide (DIOG) lies with the United States Justice Department's National Security Division and the FBI's Inspection Division, Office of General Counsel, and Office of Integrity and Compliance. Congressional Oversight is conducted by various committees of the United States Congress, but primarily by the Judiciary and Intelligence Committees. The Intelligence Oversight Board (IOB), comprised of members from the President's Intelligence Advisory Board (PIAB), also conducts oversight of the FBI. Among its other responsibilities, the IOB reviews violations of the Constitution, national security law, Executive Orders and Presidential Decision Directives by the FBI and issues reports thereon to the President and the Attorney General.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

carry out the auditing/oversight of LAPD personnel assigned to CT-10, the IG shall coordinate access to such records and investigations with the CT SAC.

6. At the conclusion of the IG's review of any "classified" inspection/audit, the IG shall prepare a confidential declassified report to the Board of Police Commissioners in which the IG shall assess compliance by LAPD CT-10 personnel with applicable laws, rules, and standards and procedures. Any use of information from an FBI JTTF file, in either its original format or derived there from, must comply with federal laws and regulations. The IG may not reveal classified information in an LAPD IG report. If the information is vital to the report, the IG shall seek permission from the FBI to use that information in a declassified form. Only the FBI can determine whether classified information can be declassified. The IG will consult and gain the concurrence of the FBI's CT SAC prior to any dissemination of information derived from the FBI.

7. If the LAPD IG determines that there is a potential violation of federal law or regulation by an FBI or other federal employee, the IG will refer the matter to the FBI JTTF Assistant Special Agent in Charge for appropriate action.

PUBLIC ACCESS TO INFORMATION STANDARDS AND PROCEDURES

X. PUBLIC ACCESS TO INFORMATION

- A. Major Crimes Division Intelligence Section shall provide public access to all documents maintained or collected by Major Crimes Division Intelligence Section in accordance with the provisions of the Freedom of Information Ordinance (FOIO) of the City of Los Angeles, as interpreted in the opinion of the City Attorney, dated July 8, 1983, and in accordance with any state or local laws which may require or permit greater disclosure of information.
- B. In providing disclosure pursuant to requests made under this section, or other applicable laws, Major Crimes Division Intelligence Section shall evaluate each document within the scope of each such request on an individual document by document basis. Major Crimes Division Intelligence Section shall search documents within each category of documents maintained by Major Crimes Division Intelligence Section (and created after the effective date of these Guidelines) and shall, to the extent reasonably possible, maintain documents in a manner which enables their production in response to such requests.
- C. The Department shall apply the test set forth in subsection "o" of the FOIO to any requests and shall consult with the Office of the City Attorney, as necessary.



Public Version

LOS ANGELES POLICE COMMISSION

*Audit of Anti-Terrorist Intelligence
Section (Phase I)
Fiscal Year 2006/2007*



Conducted by

THE POLICE COMMISSION

ALAN J. SKOBIN
Commissioner

March 6, 2007

LOS ANGELES POLICE COMMISSION

BOARD OF POLICE COMMISSIONERS

JOHN W. MACK
PRESIDENT

ALAN J. SKOBIN
VICE PRESIDENT

SHELLEY FREEMAN
ANTHONY PACHECO
ANDREA SHERIDAN ORDIN



ANTONIO R. VILLARAIGOSA
MAYOR

REPLY TO:

RICHARD M. TEFANK
EXECUTIVE DIRECTOR

EXECUTIVE OFFICE
150 NORTH LOS ANGELES STREET
LOS ANGELES, CALIFORNIA 90012
(213) 485-3531 PHONE
(213) 485-8861 FAX

ANDRÉ BIROTTE, JR.
INSPECTOR GENERAL

OFFICE OF THE INSPECTOR GENERAL
201 NORTH FIGUEROA STREET, SUITE 610
LOS ANGELES, CALIFORNIA 90012
(213) 202-5868 PHONE
(213) 482-1247 FAX

March 6, 2007

TO: The Honorable Board of Police Commissioners

FROM: Alan J. Skobin, Commissioner

SUBJECT: AUDIT OF ANTI-TERRORIST INTELLIGENCE SECTION (PHASE I)
PUBLIC VERSION

RECOMMENDED ACTION

1. REVIEW and APPROVE the Police Commission's Audit of Anti-Terrorist Intelligence Section (Phase I).

DISCUSSION

One of the responsibilities of the liaison committee to the Anti-Terrorist Intelligence Section (ATIS), formerly known as Anti-Terrorist Division, is to ensure an audit is performed of ATIS. For quite some time, due to personnel resource constraints, the Police Commission has not been able to conduct a formal audit of ATIS, although there has been regular communication and updates. Because of the outstanding auditing skills at the Office of the Inspector General (OIG), I solicited the assistance of the Inspector General in this endeavor. Although the OIG has additional significant responsibilities as set forth in the Federal Consent Decree, the OIG was able to assist me in conducting and presenting the attached Audit.

Due to the sensitive nature of investigations conducted by ATIS, I worked closely with the Inspector General, an Assistant Inspector General, and one Special Investigator in conducting this Audit. Because of the Audit's broad scope, it was determined that it should be conducted in two phases. The Phase I portion of the Audit evaluated ATIS' handling of all open and preliminary intelligence investigations that were investigated anytime between January 2005 and June 2006. The Audit also evaluated the associated confidential informant packages and search warrants, if any. Finally, the Audit evaluated ATIS' handling of initial leads. I personally conducted interviews, reviewed investigative files and the OIG's Audit methodology, received frequent briefings on preliminary findings, and discussed the findings presented in the Audit report.

The Honorable Board of Police Commissioners

Page 2

1.0

The Audit contains information and suggestions, which I believe will improve ATIS' operations. The OIG played a key role in developing the information and suggestions and this Audit is but one example of the OIG's unique value and importance in providing oversight to the Department.

The diligent work performed by the OIG is much appreciated and I look forward to their assistance in conducting the Phase II portion of the Audit.

I am submitting two versions of the Audit report: the attached public version and through separate correspondence, a confidential version. The attached report has been revised to omit confidential and sensitive information, and the report may be discussed in open session.

The Inspector General and I are available to provide any additional information the Board may require.

Respectfully,


Alan J. Skobin
Commissioner

Attachment

c: Inspector General André Birotte, Jr.
Executive Director Richard M. Tefank
Chief of Police William J. Bratton
Police Administrator Gerald L. Chaleff, Consent Decree Bureau
Deputy Chief John M. Leap, Counter Terrorism and Intelligence Bureau
Captain Gary S. Williams, Major Crimes Division

TABLE OF CONTENTS

**POLICE COMMISSION
AUDIT OF ANTI-TERRORISM INTELLIGENCE SECTION (PHASE I)
FISCAL YEAR 2006/2007
PUBLIC VERSION**

	PAGE No.
<u>PURPOSE</u>	1
<u>BACKGROUND</u>	1
<u>RESULTS OF THE AUDIT</u>	3
INITIAL LEADS	3
PRELIMINARY INTELLIGENCE INVESTIGATIONS	3
OPEN INTELLIGENCE INVESTIGATIONS	4
Reasonableness of the Open Investigations	4
Support for Reasonable Suspicion	5
Documented Materiality	5
Documentation	5
CONFIDENTIAL INFORMANT PACKAGES	7
STANDARDS AND PROCEDURES	8
<u>OTHER RELATED MATTERS</u>	8
<u>CONCLUSION</u>	9

POLICE COMMISSION
AUDIT OF ANTI-TERRORISM INTELLIGENCE SECTION (PHASE I)
FISCAL YEAR 2006/2007
PUBLIC VERSION

PURPOSE

Pursuant to the Los Angeles Police Department's (LAPD or Department) Standards and Procedures for Anti-Terrorism Intelligence Section (ATIS), the Police Commission initiated a two-phased audit (Audit) of ATIS. The Phase I portion of the Audit evaluated ATIS' handling of all open and preliminary intelligence investigations that were investigated anytime from January 2005 to June 2006. The Audit also evaluated any associated confidential informant packages and search warrants.¹ Finally, the Audit evaluated ATIS' handling of initial leads. Per ATIS' Standards and Procedures, at least annually, the Police Commission must audit ATIS' operations. Due to limited resources, this Audit had not taken place for several years, but through the assistance of the Inspector General and his staff, the Police Commission was able to conduct the Audit.

The Phase II portion of the Audit, expected to be completed by the summer of 2007, will include an assessment of all materials gathered, developed, or maintained by ATIS for intelligence purposes. Additionally, oral interviews of ATIS personnel will be conducted to ensure personnel are adhering to the Standards and Procedures that were approved by the Police Commission.

Given ATIS deals with highly sensitive information, any reference to specific details of an investigation or ATIS operations were removed from the public version of this Audit Report.

BACKGROUND

The LAPD's mission is to serve and protect the citizens of Los Angeles. Along that vein, the ATIS is charged with preventing and investigating terrorist activity and illegal actions that could result in a significant disruption of public order. Generally, the focus of ATIS is strategy oriented. The section focuses on determining the ultimate goal of individuals and/or groups, rather than on specific violations of the law. The objective is not to arrest and prosecute suspects, but rather to detect, collect, analyze and disseminate information for the purpose of developing intelligence and preventing future terrorist activity. The possibility of future terrorist attacks is an unfortunate reality that law enforcement throughout the United States must attempt to address. Certain individuals and/or groups may attempt to further their own societal objectives by influencing and/or harassing on the basis of race, religion, national origin, or sexual orientation. Often, this is accomplished by individuals/organizations planning, financing, and/or aiding/abetting various criminal acts.

That being said, the Police Commission also recognizes the delicate balance between providing effective terrorist prevention activity and protecting the rights of citizens. Constitutional and statutory rights guarantee every citizen the right to privacy, to express ideas and dissension, and to associate publicly and privately for any lawful purpose. As such, the Police Commission has established a policy that strictly prohibits the use of illegal or unauthorized methods of

¹ All search warrants reported to have been served by ATIS were reviewed and no significant concerns related to the articulated reasonable suspicion were noted.

collecting, maintaining, or disseminating intelligence information. It is both unnecessary and wrong to maintain an intelligence file on any individual or organization unless the "reasonable suspicion" standard is met. Personnel are also prohibited from collecting, maintaining or disseminating information about an individual's sexual, political, or religious activities; beliefs; or opinions, unless such information is material to an approved investigation.

There are three types of investigations conducted by ATIS, as follows:

- **Initial Lead Assessment/Investigation.** Almost daily, ATIS receives initial leads on potential terrorist activity. The lead information may be received from other law enforcement agencies, Department employees, or private citizens. An ATIS supervisor reviews each lead and at that time, a decision is made to investigate the lead, refer the lead to another entity for investigation, or classify the lead as "for information only." If the lead is retained by ATIS for investigation, limited activity is performed to determine whether further investigation is warranted. As investigative leads from the public or other sources may be vague and not yet meet the "reasonable suspicion" standard, the investigator may access public and government records; interview the reporting person, potential subject, or witnesses; and/or monitor the potential subject. Initial lead investigations must be completed within 60 days from the date the lead was received.
- **Preliminary Intelligence Investigation.** A preliminary intelligence investigation may be initiated when reasonable and articulable suspicion exists to believe that an individual/organization may be: 1) planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts; and, 2) the results of which are intended to further their objectives by influencing societal action or harassing on the basis of race, religion, national origin, or sexual orientation. However, unlike initial leads, reasonable suspicion already exists but the information still needs to be developed to the point of reliability. Reasonable suspicion is defined as an honest belief based on known articulable circumstances which would cause a reasonable and trained law enforcement officer to believe that some activity relating to a significant disruption of the public order may be occurring or has the potential to occur. Reliable information is defined as information that can be depended on to be trustworthy or worthy of confidence. The Commanding Officer of Major Crimes Division (MCD) must approve the opening of each preliminary intelligence investigation and the investigation shall not exceed 120 days.
- **Open Intelligence Investigation.** An open intelligence investigation may be initiated when reasonable and articulable suspicion exists based upon reliable information that an individual or organization may be: 1) planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts; and, 2) the results of which are intended to further their societal objectives by influencing societal action or harassing on the basis of race, religion, national origin, or sexual orientation. The Commanding Officer of MCD must approve the opening of each open intelligence investigation and each year, the Commanding Officer reviews each investigation to ensure justification still exists for the case to remain open.

RESULTS OF THE AUDIT

Initial Leads

A random sample of initial leads, generated from January 2005 to June 2006, were identified and reviewed to determine whether the handling of these initial leads was appropriate.²

Based on our review, all the leads were properly classified and adequate steps were taken to investigate the leads retained and investigated by ATIS. Additionally, the initial leads investigated by ATIS were closed or converted into a preliminary or open intelligence investigation within the 60-day requirement. However, in our review of initial lead forms, it became apparent that greater care is needed with their completion. For example, on one form, there were inconsistencies with the marked check boxes on the form (the source reliability check box indicated "Fairly Reliable" and "Reliability Can't Be Judged," but the "Substantiated" check box was also marked).

Additionally, it appears that internal controls surrounding the initial lead classification process could be enhanced. When ATIS decides to retain and investigate a lead, a supervisor completes an Investigative Follow-Up Checklist. This checklist documents the supervisor's recommended investigative steps an assigned investigator should perform, and when the investigation is closed, the supervisor approves the closure on this checklist. However, the name of the supervisor is only typed in, making it impossible to verify that the supervisor actually approved the closure.³ Currently, initial leads are handled in a paperless fashion and all leads are handled electronically; however, we believe efforts should be made to ensure supervisor signatures are obtained. Additionally, one of the 14 lead investigations conducted by ATIS was closed without any indication of the approving supervisor. The date closed was also left blank. Per the Commanding Officer of MCD (ATIS is part of MCD), he recently issued a directive requiring the signature of an ATIS supervisor to close out all initial leads.

Preliminary Intelligence Investigations

This Audit assessed each investigation and any associated working files that were investigated from January 2005 through June 2006.⁴ Based on our assessment, ATIS is adhering to the 120-day requirement to complete preliminary investigations. Although the Audit identified five investigations that were closed after the 120-day limitation (by an average of 10 days), based on the dates documented in the investigations, the delay was due to the Commanding Officer of MCD being unable to give his final approval for the closure, not the investigators failing to adhere to the Department's Standards and Procedures.

² The initial leads were either referred to another entity, classified as information only, or investigated by ATIS.

³ Lead sheets that document the referrals to other law enforcement agencies and information classified as "for information only" also do not contain signatures of approving supervisors (the form only contains a supervisor's type name).

⁴ A working file contains information material to an investigation. The investigative file contains intelligence reports completed by ATIS staff that are approved by the Commanding Officer of MCD.

Additionally, the Audit included an assessment of the reasonable suspicion used to open the preliminary intelligence investigations. Although the information used to support reasonable suspicion may not yet be reliable, reasonable suspicion must exist to open a preliminary intelligence investigation. Based on this assessment, the reasonable suspicion to open two investigations appeared questionable. These concerns were discussed with the Commanding Officer of MCD and he indicated that reasonable suspicion was based on the investigators' training, experience, and knowledge about the subject, and information provided by another law enforcement agency. However, he agreed that more articulation regarding the reasonable suspicion should have been documented in the request to open the preliminary intelligence investigations. The Phase II portion of the Audit will follow-up on these two investigations and include a discussion with the investigators regarding the additional reasonable suspicion that was not originally articulated in the files.

Finally, it was noted that three preliminary intelligence investigations were opened based on information provided by another law enforcement entity. This law enforcement agency provided information on many potential terrorist suspects. However, the justification to open these particular investigations just referred to the initial lead and did not document the reasonable suspicion. This concern was discussed with the Commanding Officer of MCD and he indicated that at the time of his approval to open the investigations, he was aware of the information provided by the law enforcement agency. He further indicated that these details, that provide additional support for ATIS' reasonable suspicion, would be added to the investigations. The Phase II portion of the Audit will assess the information added to these investigations.

Open Intelligence Investigations

The Audit evaluated all open investigations, from January 2005 through June 2006, and focused on evaluating: 1) the reasonableness of keeping the investigations open; 2) the support for the reasonable suspicion; 3) the materiality of information maintained in associated working files for the investigations; and, 4) whether all material documents were included in the investigative and working files.

Reasonableness of the Open Investigations: All available information contained in the open investigative and working files was evaluated to determine whether the investigations should remain open. Based on this review, it appeared that two investigations should be closed due to the lack of any recent/additional evidence. Specifically, for one investigation, the reasonable suspicion used to open the investigation appeared supported, but given the lack of any recent/additional evidence, it appeared that the investigation should be closed. In fact, the last intelligence report, dated over a year and a half ago, justified keeping the investigation open due to the subject using "counter surveillance techniques" (no further description provided) in a prior surveillance conducted over a year before and the investigator still wanted to determine the subject's whereabouts. For another investigation, the initial reasonable suspicion was supported but given the lack of recent/additional evidence, it appeared that the investigation should be closed.⁵ There had been no additional information related to this subject for over two years.

⁵ This investigation was based on an initial lead, but the information to support the reasonable suspicion was not delineated in the working files.

These concerns were discussed with the Commanding Officer of MCD and he indicated that the investigations had been closed (after our initial review) when he performed his annual review of open investigations.

Support for Reasonable Suspicion: Four investigations (the subjects all knew each other) did not have enough information in the investigative or working files to support how the investigator obtained part of the information used to support the reasonable suspicion. The four investigations had the same intelligence report (copied and placed in each file) that indicated the four subjects were members of a radical group. However, the files do not document how the information was obtained to support that these individuals were actually members of the group. Therefore, the Audit was unable to determine how the information, used to support the reasonable suspicion, was obtained. This concern was discussed with the Commanding Officer of MCD and he indicated the information was obtained through another law enforcement agency but agreed that there needed to be some articulable statement indicating where this information came from.

Documented Materiality: All evidence gathered and retained in the investigative and working files was evaluated and for the most part, the information contained in the files appeared material. However, in five investigations, the Audit identified one or more documents in the working files in which it could not be determined whether the information was material to the investigation and there was no notation to indicate how the information was obtained or how the documents were material. The working files for three investigations contained photographs of individuals, vehicles, and/or residences/businesses; but the dates the photographs were taken and/or their materiality were not evident through a review of the file. Additionally, the working files for two investigations contained other documents that did not indicate how the information was obtained and/or their materiality.

In the past, ATIS personnel used a stamp, wherein personnel documented how and when the information (placed in the working folder) was obtained and material to the investigation. The stamp was not present on a majority of documents contained in the working files for the investigations reviewed. The current Standards and Procedures are unclear as to whether investigators need to document the materiality determination and how and when the information was obtained. The OIG believes the better practice would be to document this type of information and it is suggested that the Standards and Procedures be updated to clarify this area. On a positive note, the Commanding Officer of MCD reinstated this procedure in a directive provided to all ATIS personnel in April 2006.

Documentation: Investigative files contain intelligence reports completed by investigators which serve to update ATIS management and document any progress with the investigations. The investigations' associated working files contain all documentation to support material information referenced in the intelligence reports. For example, if an intelligence report indicates that an individual publicly posted "hate" messages and other incriminating information, the associated working folder should contain applicable copies of the public message. This ensures that the information in the intelligence reports is valid and supported. For the open investigations, the intelligence reports were evaluated along with any associated working files.

For 15 investigations, there was additional information that the OIG believes should have been maintained in the working files, as discussed below:

- For five investigations (four individual investigations and one organizational investigation), there was a photocopied intelligence report placed in each file that indicated the subject of one investigation was overheard stating he/she wanted to harm another person. However, the investigative and working files did not indicate who overheard this statement and the chronology log had no additional details. Additionally, the investigative files did not indicate whether there were any investigative steps to ensure this person was not in any danger. This concern was discussed with the Commanding Officer of MCD and he agreed that the working folder should have contained this information and stated how it was obtained. He stated that in this instance, the potential victim was notified by another agency.⁶
- For four investigations (the four subjects were related), the investigative file documented the number of people attending a radical group meeting along with information about what was discussed. However, it is unknown how this information was obtained and the working files did not provide any additional information.
- For one investigation, the intelligence report indicated that the subject purchased a violent and racist game but there was no indication of how this information was obtained. Additionally, the investigation did not have a chronology log or a working folder.
- For one investigation, the investigative file indicated that on two occasions the investigator either spoke with the subject or ran into him/her at a public event.⁷ However, there was no documentation on the details of these encounters, specifically what if any information was obtained.
- For one investigation, the investigative file referred to information that the subject produced that linked him/her to the main organization, but there were no copies of these documents in the investigative file and there was no working folder.
- For one investigation, the investigative file indicated that while serving a search warrant, the officers found a document with ingredients for explosives. However, it is unknown who saw this document and the return to the search warrant (that could help support that the document was seized) was not included in the file. Additionally, the initial lead information was not included in the investigative file.

⁶ Additionally, for one of these investigations, part of the reasonable suspicion is based on a crime committed by the subject; but the associated report was not included in the investigative or working folder.

⁷ The chronology log indicated the subject spoke at a public meeting and seemed to indicate that the investigator spoke with the subject about the organization. Another chronology log entry indicated that the investigator ran into the subject at a public event.

- For one investigation, the initial lead used to support reasonable suspicion was not included in the investigative file or working folder.
- For one investigation (an organization), the investigative file indicated that the investigator attended/surveilled a radical group meeting and the file indicated that numerous flyers produced by the organization were recovered in the City of Los Angeles. However, the investigative file did not document how this information was obtained or copies of the flyers. There was no working folder for this investigation.

These concerns were discussed with the Commanding Officer of MCD and he agreed that there should be more articulation as to how the information was obtained. He further indicated no undercover operations took place to obtain the information and that the information was either obtained during a public event or that citizens reported the information to their local police stations.

Overall, it appears that additional efforts should be taken to ensure that all information in intelligence reports is supported. Of the open intelligence investigations reviewed, ten (three individual and seven organizational investigations) did not have an associated working folder. This means there was no chronology log or other background information used to assist/support information in the main investigative file. Also, it appears that there needs to be a standard checklist, similar to the ones used for initial lead investigations, that requires the investigator to obtain relevant/applicable information for the subjects of the investigation. For example, a majority of the investigations did not contain the subject's driver license photograph, Department of Motor Vehicle information, criminal history, or Federal Bureau of Investigation information. Finally, 16 investigations that were open at the time of our evaluation did not have updates within the last six months (eight individual files and eight organization files). The Commanding Officer of MCD issued several directives in April 2006 to help supplement/clarify information provided in the Standards and Procedures manual. One directive required investigators to update open investigations at least twice a year to document the progress on the case, which would cause an investigator and the ATIS chain of command to evaluate whether the case should remain open. This requirement is not part of the current Standards and Procedures, but given its importance, it should be added.

Confidential Informant Packages

The Audit evaluated all informant packages for confidential informants used during 2005 and 2006. The review identified one informant package, which was deactivated on December 2005, with a concern regarding the authenticity of information in an update report. Specifically, the Exceptional Handling Report had the same verbiage as the Exceptional Handling Report (copying and pasting) from three years before. Additionally, one Exceptional Handling Report had a discrepancy on when it was approved. Finally, the Contact Forms did not consistently document the notification to a supervisor when meeting with the informant.

Standards and Procedures

According to the Standards and Procedures approved by the Police Commission, the Audit is required to review all of ATIS' regulations, rules and policies. Before commencing the Audit, this information was requested and ATIS provided the Standards and Procedures that have guided their operations throughout the years. The ATIS provided their Standards and Procedures dated March 18, 2003; October 16, 2001; December 10, 1996; and January 31, 1984. There have been slight revisions in all of these Standards and Procedures and as such, the Audit evaluated them to determine if there are any requirements that are now outdated or omitted from the current Standards and Procedures used by ATIS personnel.

Based on a review of the Standards and Procedures, the Audit identified the following concerns:

- Prior Standards and Procedures used to allow for extensions (for up to three months) of preliminary investigations by the Commanding Officer of MCD if justification was present. As preliminary investigations should be thorough, if 120 days is not enough time, the Commanding Officer of MCD should be able to exercise this discretion. The same is true for initial lead investigations. Therefore, it is suggested that the Standards and Procedures be updated to allow this type of flexibility.
- The Standards and Procedures used to require that, semi-annually, all ATIS personnel needed to be trained on intelligence policy and procedure and on Constitutional and statutory considerations by the Commanding Officer of MCD and the Deputy City Attorney. As anti-terrorism case law is constantly being updated, this type of training appears necessary. Therefore, it is suggested that the Standards and Procedures be updated to allow this type of training on an annual basis.

OTHER RELATED MATERS

While conducting the Audit, certain concerns came to the auditors' attention that did not necessarily fit into the Audit's original scope. Specifically, it was noted that the Standards and Procedures require the Commanding Officer of MCD to provide, annually, written certification to the Police Commission that all current intelligence investigations were internally reviewed and those investigations considered no longer viable were closed. While ATIS has been completing this type of assessment, there is no evidence that the certification was sent to the Police Commission. In the future, it is suggested that the Commanding Officer of MCD provide this certification to the Police Commission annually. Additionally, in the past, ATIS personnel submitted to a lie detector examination prior to being placed in the section. Due to limited resources within the Department and a need to transfer personnel into the section in a relatively short timeframe, this process was eliminated from the selection process. However, given the section deals with highly sensitive information, it is a good protocol. The Commanding Officer of MCD indicated that he was delayed in re-implementing the protocol due to employment and legal considerations, but for new personnel transferred to ATIS, the lie detector examination has now been added back to the selection process.

As indicated earlier, ATIS' objective is not to arrest and prosecute suspects, but rather to detect, collect, analyze and disseminate information for the purpose of developing intelligence and preventing future terrorist activity. However, when ATIS discovers possible criminal activity during an investigation, a referral is made to Major Crimes Division, Criminal Investigation Section, to investigate the criminal aspect of the case. As there could be a risk that terrorist investigations are being referred to the Criminal Investigation Section to circumvent the ATIS Standards and Procedure requirements, this Audit reviewed the criminal investigations referred by ATIS to the Criminal Investigation Section from 2003 through 2006. The Audit evaluated whether the referrals were appropriate and whether there was a legal basis for conducting the criminal investigations. Based on our review, no concerns were identified.

CONCLUSION

Overall, ATIS has done a good job adhering to the Standards and Procedures approved by the Police Commission. While the Audit identified a few areas where changes are needed, focused oversight should properly address these concerns going forward.



Public Version

Los Angeles Police Commission

Anti-Terrorism Intelligence Section Audit
Fiscal Year 2008/09



Conducted by the

**OFFICE OF THE INSPECTOR GENERAL
ON BEHALF OF THE BOARD OF POLICE COMMISSIONERS**

ANDRÉ BIROTTE, JR.
INSPECTOR GENERAL

April 9, 2009

**POLICE COMMISSION
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2008/2009**

PUBLIC VERSION

PURPOSE

On behalf of the Board of Police Commissioners (Police Commission) the Office of the Inspector General (OIG) initiated an audit (Audit) of the Anti-Terrorism Intelligence Section (ATIS), pursuant to the Los Angeles Police Department's (LAPD or Department) Standards and Procedures for ATIS. The Audit primarily evaluated ATIS' controls over Initial Lead, Preliminary and Open Intelligence investigations, as well as documents related to surveillances and confidential informants, to determine whether they were processed in compliance with Departmental policies and procedures.

According to ATIS' Standards and Procedures, at least annually, the Police Commission shall audit the operations of ATIS. For this Audit, in order to accomplish this objective, the Police Commission requested the assistance of the Inspector General and his audit staff. The last Audit, published on March 6, 2007, reviewed a random sample of Initial Leads and all Preliminary and Open Intelligence investigations that were investigated from January 2005 through June 2006.

SCOPE AND METHODOLOGY

The Audit scope included a review of Initial Lead, Preliminary, and Open Intelligence investigations *initiated* or *closed* from June 2007 through May 2008. A sample of Initial Lead investigations was randomly selected as well as all Preliminary investigations and all Open Intelligence investigations.¹ The Audit also included a review of documents related to each of the surveillances conducted during the scope period. Furthermore, confidential informant (CI) packages that were active during the period from June 2007 through May 2008 were tested.² Additionally, selected ATIS personnel were interviewed.

BACKGROUND

Anti-Terrorism Intelligence Section within the Major Crimes Division (MCD) has established that their primary objective is to prevent and investigate terrorist activity and illegal actions that could result in a significant disruption of public order. The intelligence investigations conducted are strategy oriented rather than case oriented as with criminal investigations. Intelligence investigations focus on the goals or potential of an individual whereas criminal investigations focus on specific violations of law after a crime has been committed. The objective is not to arrest and prosecute suspects, but rather to detect, collect, analyze and disseminate information for the purpose of developing intelligence and preventing future terrorist activity while steadfastly respecting all constitutional and statutory rights guaranteed to every individual.

¹ Working Folders, which are created by the investigator for each individual who is the subject of an approved Open Intelligence investigation, were also reviewed.

² Some of these CI packages reviewed were identified during our review of either Preliminary or Open Intelligence investigation files.

That being said, the Police Commission also recognizes the delicate balance between providing effective terrorist prevention activity and protecting the rights of citizens. Constitutional and statutory rights guarantee every citizen the right to privacy, to express ideas and dissension, and to associate publicly and privately for any lawful purpose. As such, the Police Commission has established a policy that strictly prohibits the use of illegal or unauthorized methods of collecting, maintaining, or disseminating intelligence information. It is not in keeping with Departmental standards to maintain an intelligence file on any individual unless the reasonable suspicion standard is met. Personnel are also prohibited from collecting, maintaining or disseminating information about an individual's sexual, political, or religious activities, beliefs, or opinions unless such information is material to an approved investigation.

The table below describes the three levels of intelligence investigations performed by ATIS, each one bound by strict guidelines with respect to the criteria and approval levels for opening an investigation, the available investigative techniques and the time limits for completing an investigation.

LEVELS OF INTELLIGENCE INVESTIGATION ACTIVITY			
	INITIAL LEAD	PRELIMINARY	OPEN INTELLIGENCE
Source of Information	Other law enforcement agencies, private citizen, departmental employees	Same as Initial Lead	Same as Initial Lead
Required Threshold for Opening Investigation	Prompt and limited follow-up of information received concerning the possibility that terrorist activity exists.	Articulate reasonable suspicion that an individual or organization may be planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts; and the results of which are intended to further their objectives by influencing societal action or harassing on the basis of race, religion, national origin, or sexual orientation.	Same as Preliminary except that the articulable reasonable suspicion must be based on reliable information.
Approval Level	Detective III	Commanding Officer, MCD	Commanding Officer, MCD
Investigative Techniques	Public records, LAPD records, interviewing potential subject, reporting person, witnesses, and monitoring.	Surveillance, use of confidential informants, and all other techniques utilized during Initial Lead investigations.	All lawful techniques may be used.
Time Limit for Completion	60 days	120 days	A Follow-Up Intelligence Report completed twice per year while the investigation remains open. It is reviewed and approved by the Officer-In-Charge, ATIS. Annually, the Commanding Officer, MCD reviews all ongoing Open Intelligence investigations.

SUMMARY OF RESULTS

The results of the Audit reflected substantial compliance with Police Commission guidelines applicable to ATIS operations. Additionally, ATIS has adopted these guidelines as evidenced in their written and published Directives and during the OIG's review of ATIS' investigation files. Specifically, each investigation was opened only after the appropriate threshold was met and closed only after it was evident to ATIS investigators that an individual no longer represented a threat of terrorist activity or the case was referred to another law enforcement agency or Department entity for appropriate investigation.³ Furthermore, the investigation files were well organized and the file documentation adequately supported the investigation, which appears to reflect improvement since the last audit.

However, the OIG identified compliance issues with certain ATIS Directives concerning supervisory oversight. In particular, these issues pertained to the ongoing review of Open Intelligence investigations, documentation and approval of surveillance for Preliminary and Open Intelligence investigations, review of Open Intelligence Working Folders, and contact of an active CI every 90 calendar days. MCD management generally concurred with the OIG's issues and has already implemented corrective action to the OIG's recommendations. The implementation of the corrective action will be reviewed during the next scheduled audit of ATIS.

DETAILED FINDINGS

A. Supervisory Oversight

1. Follow-Up Intelligence Reports

Background: A Follow-Up Intelligence Report is intended to communicate pertinent information regarding the Open Intelligence investigation including its status and its viability as an ongoing investigation. According to ATIS Divisional Order No. 1 dated April 12, 2006, a Follow-Up Intelligence Report shall be completed at least twice per year after the investigation has been approved by the Commanding Officer, MCD. After the Follow-Up Intelligence Report is completed by the investigator, it shall be reviewed and approved by the Officer-In-Charge, ATIS. For this audit, the OIG interpreted this requirement as completing two Follow-Up Intelligence Reports during the 12-month period following the date that the investigation was approved.

³ See Required Threshold for Opening Investigation in the Levels of Intelligence Investigation Activity table on page two of seven.

Issue: A Follow-Up Intelligence Report was not completed timely for thirty percent (30%) of the Open Intelligence investigations reviewed. Although Follow-Up Intelligence Reports were completed sporadically for all of the investigations following the date the investigation was approved, lapses in the semi-annual requirement ranged from either completing only one Follow-Up Intelligence Report or none in a particular 12-month period.

Risk: Open Intelligence investigations for which Follow-Up Intelligence Reports are not completed timely may not receive the essential ongoing review and feedback from supervisory staff to help ensure that the investigation is being conducted efficiently, effectively and in compliance with Departmental policies and procedures, with citizens' rights being adhered to.

Management's Response: MCD management has published Divisional Order Nos. 13 and 15, dated February 18, 2009, which require a Follow-Up Intelligence Report to be completed every six months following the date the Commanding Officer approves the opening of the investigation and formalized briefings to assess the viability of open investigations including the status of Follow-Up Intelligence Reports.

2. Operational Plans for Surveillance

Background: Surveillance is defined as the continuous or prolonged observation of a targeted individual or group by clandestine means for the purpose of collecting information material to an approved Preliminary or Open Intelligence investigation.⁴ ATIS investigators requesting surveillance resources are required to complete an Operational Plan which documents the name of the subject, the rationale for conducting the surveillance and the required signatures indicating the authorization to conduct the operation.

Issue: An Operational Plan for conducting surveillance operations was not evident during the audit as having been completed for forty-six percent (46%) of the surveillances reviewed and the required approvals were not noted on the Plan for twenty-three percent (23%) of the surveillances reviewed. The OIG noted during the Audit that a formalized process did not exist for completing the Operational Plan for surveillance, obtaining the required approvals, and the recordkeeping of the Operational Plan once completed.

Risk: If Operational Plans for surveillance are not completed and properly approved, there is a risk that the investigative steps taken may not be conducted efficiently and effectively and in compliance with Departmental standards.

⁴ According to the ATIS Standards and Procedures, Section I, page 3

Management's Response: Subsequent to the issuance of a draft version of this report, MCD management advised the OIG that five of the Operational Plans not previously provided to the auditors during the Audit were located. Additionally, two of the Operational Plans reviewed during the audit that lacked the required approvals were also located and provided to the OIG subsequent to the issuance of a draft version of this report. A formalized process did not exist to document the request, approval, and retention of the Operational Plans for surveillance. This is the primary reason why the aforementioned documentation could not be located during the Audit. MCD management has published Divisional Order No. 12, dated October 30, 2008, to standardize this process and to implement a recordkeeping system. Additionally, MCD management has determined that each current Open Intelligence investigation utilizing surveillance has an approved Operational Plan for surveillance on file.

3. Working Folders

Background: The Working Folder is a separate file from the investigation file and contains the investigative materials gathered, received, and developed for the specific purpose of updating an approved Open Intelligence investigation file. Supervisors shall ensure that a Working Folder is completed for each Open Intelligence investigation and that the required periodic reviews are conducted to ensure the Folder contains appropriate documents per Divisional Order No. 11 dated March 16, 2007. Additionally, Divisional Order No. 2, dated April 12, 2006, requires that supervisors shall audit the investigator's Working Folder at least three times a year and shall document those inspections on the investigator's Working Folder and initial, date and record his/her serial number.

Issue: For forty-four percent (44%) of the Open Intelligence investigative files reviewed, the Audit Control Sheet was not signed by a supervisor indicating that he/she performed the required periodic review of the investigator's Working Folder.

Risk: The lack of documented supervisory oversight of investigators' Working Folders creates a risk that Working Folders contain information that is not in compliance with the law and/or Departmental standards.

Management's Response: MCD management has published Divisional Order Nos. 14 and 15, dated February 18, 2009, which requires that each Working Folder contain a standardized Audit Control Form and that briefings be conducted to determine, among other matters, that the required supervisory review of the Working Folder is documented on the Audit Control Form.

4. Contact of Confidential Informants Every 90 Days

Background: The LAPD Informant Manual requires that the managing investigator, after acquiring supervisory approval, shall either in person or telephonically contact their confidential informant (CI) at least once every 90 calendars days. The CI contact shall be documented on an Informant Contact Sheet.

Issue: Forty-five percent (45%) of the CI packages reviewed lacked evidence that the CI was contacted by the investigator at least once every 90 calendar days. Specifically, a review of the CI Contact Sheets for CIs that were active from June 2007 through July 2008 indicated that there was a lapse in contacting the CI ranging from 17 to 94 days.

Risk: Scheduled follow-up contact is important to help ensure that the CI is still available and continues to remain motivated in providing information to the Department.

Management's Response: MCD management has provided the necessary training on the Department's requirement for contacting CIs. Additionally, a monthly self-assessment has been implemented to ensure that the 90-day requirement for contacting a CI is performed.

B. File Documentation

Preliminary Investigations

Background: Preliminary investigations are undertaken when there is information which indicates the possibility of terrorist activity. Preliminary investigations are based on reasonable suspicion only and are for the purpose of determining whether or not the information is reliable in order to support the rationale for initiating an Open Intelligence investigation.

Issue: Preliminary investigations opened on several individuals associated with the same group were initiated with sufficient reasonable suspicion that each of these individuals may have been planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts. However, it was necessary to review an Open Intelligence investigative file on another individual, the number which was referenced in all of these Preliminary investigative files, in order to fully make this determination that the reasonable suspicion standard had been met before the Preliminary investigation was initiated on each of these individuals.

Risk: As the policy of ATIS is to conduct Preliminary investigations on individuals not groups, it is important that the investigator sufficiently document that the reasonable suspicion threshold was met in each Preliminary investigation file before initiating an investigation to fully support that an individual's right to privacy was not violated.

Management's Response: MCD management has determined that the additional articulation has been added to all four Preliminary investigation files. Additionally, training has been provided to ATIS personnel so that they understand the importance that the documentation contained in each Preliminary investigation file to support reasonable suspicion should stand alone.

CONCLUSION

The results of the Audit reflected substantial compliance with Police Commission guidelines applicable to ATIS operations. Additionally, ATIS has adopted these guidelines as evidenced in their written and published Directives and during the OIG's review of ATIS' investigation files. Specifically, each investigation was opened only after the appropriate threshold was met and closed only after it was evident to ATIS investigators that an individual no longer represented a threat of terrorist activity or the case was referred to another law enforcement agency or Department entity for appropriate investigation. Furthermore, the investigation files were well organized and the file documentation supported the investigation, which appears to reflect improvement since the last audit.

However, as mentioned earlier, the OIG identified compliance issues with certain ATIS Directives concerning supervisory oversight. In particular, these issues pertained to the ongoing review of Open Intelligence investigations, documentation and approval of surveillance for Preliminary and Open Intelligence investigations, review of Open Intelligence Working Folders, and contact of an active CI every 90 calendar days. The OIG commends MCD management for the timely implementation of the corrective action to the issues reported herein. The OIG encourages MCD management to conduct periodic formal self-assessments to help ensure compliance with their Departmental standards. These self-assessments would also help to identify operational control strengths and weaknesses so that MCD management may take ongoing and timely corrective action as needed.

LOS ANGELES POLICE COMMISSION
ANTI-TERRORISM INTELLIGENCE
SECTION AUDIT,
FISCAL YEAR 2009/2010
(Public Version, Open Session)



Conducted by the

POLICE COMMISSION

ALAN J. SKOBIN,
DEBRA WONG YANG
Commissioners

January 19, 2012

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION

Page 1 of 7

PURPOSE

The primary purpose of the Anti-Terrorism Intelligence Section (ATIS) Audit (Audit) was to evaluate compliance with Police Commission (Commission) guidelines which, among other things, govern ATIS operations over initial lead investigations, preliminary investigations, open intelligence investigations, surveillance operations, analytical files, and use of confidential informants. Also, the Audit was intended to evaluate closed criminal investigations conducted by Major Crimes Division (MCD) to ensure that they indeed represent valid criminal investigations, *not* intelligence investigations conducted under the guise of criminal investigations.^{1,2}

BACKGROUND

According to Commission guidelines, ATIS operations shall be audited at least annually. Police Commissioners Alan Skobin and Debra Wong Yang constitute the Commission's Undercover Investigation Liaison and were tasked with assessing MCD's compliance with Commission guidelines. In order to accomplish this objective, Commissioners Skobin and Wong Yang requested the assistance of the Office of the Inspector General (OIG). The following members of the OIG assisted with the Audit: (Resigned) Inspector General Nicole Bershon, Assistant Inspector General Kevin Rogan, Assistant Inspector General Gary McCaskill, Police Performance Auditor IV John Grosdidier, and (Resigned) Special Investigator II Charles Gaither.

The ATIS, housed within MCD, has established that their primary objective is to prevent and investigate terrorist activity and illegal actions that could result in a significant disruption of public order. The intelligence investigations conducted by the ATIS are strategy oriented, rather than case oriented as with criminal investigations. Intelligence investigations focus on the goals or potential of an individual, whereas criminal investigations focus on specific violations of law after a crime has been committed. The primary objective of an intelligence investigation is not to arrest and prosecute suspects; rather, it is to detect, collect, analyze, and disseminate information for the purpose of developing intelligence and preventing future terrorist activity, while steadfastly respecting all constitutional and statutory rights guaranteed to every individual.

The Commission recognizes the delicate balance between providing effective terrorist prevention protocols and protecting the rights of all citizens. Constitutional and statutory rights guarantee every citizen the right to privacy, the expression of ideas and dissension, and the right to associate publicly and privately for any lawful purpose. As such, the Commission has established a policy that strictly prohibits the use of illegal or unauthorized methods of collecting, maintaining, or disseminating intelligence information.

¹ MCD is responsible for conducting certain criminal investigations, including those for which the criminal act could pose a threat to the City of Los Angeles.

² If an intelligence investigation was *disguised* as a criminal investigation, certain procedures and internal controls could possibly be circumvented.

**BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 2 of 7**

It is inconsistent with Los Angeles Police Department (Department) standards to maintain an intelligence file on any individual unless the standards underlying reasonable suspicion are met. Personnel are also prohibited from collecting, maintaining or disseminating information about an individual's sexual, political, or religious activities, beliefs, or opinions unless such information is germane to an approved investigation. The table, presented below, describes the three levels of intelligence investigations performed by the ATIS, each one bound by strict guidelines with respect to the criteria and approval levels for opening an investigation, the available investigative techniques, and the time limits for completing an investigation.

LEVELS OF INTELLIGENCE INVESTIGATION ACTIVITY			
	INITIAL LEAD	PRELIMINARY	OPEN INTELLIGENCE
Source of Information	Other law enforcement agencies, private citizen, Department employees	Same as Initial Lead	Same as Initial Lead
Required Threshold for Opening Investigation	Prompt and limited follow-up of information received concerning the possibility that terrorist activity exists.	Articulate reasonable suspicion that an individual or organization may be planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts; and the results of which are intended to further their objectives by influencing societal action or harassing on the basis of race, religion, national origin, or sexual orientation.	Same as Preliminary except that the articulable reasonable suspicion must be based on reliable information.
Approval Level	Detective III	Commanding Officer, MCD	Commanding Officer, MCD
Investigative Techniques	Public records, LAPD records, interviewing potential subject, reporting person, witnesses, and monitoring.	Surveillance, use of confidential informants, and all other techniques utilized during Initial Lead investigations.	All lawful techniques may be used.
Time Limit for Completion	60 days	120 days	A Follow-Up Intelligence Report completed every six months while the investigation remains open. The Officer-in-Charge, ATIS, shall ensure that the follow-up Intelligence Reports are completed every six months. The date the Commanding Officer, MCD, approved the initial Intelligence Report serves as the starting date for the six-month period.

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 3 of 7

SCOPE AND METHODOLOGY

The Audit scope period was the 12-month period of July 1, 2009, through June 30, 2010, and documentation evaluated included:

- A random sample of initial leads initiated or closed during the scope period.
- All preliminary investigation(s) initiated or closed during the scope period.
- All open intelligence investigation(s) initiated or closed during the scope period.³
- All confidential informant (CI) package(s) active during the scope period.⁴
- All intelligence-related surveillance operation(s) conducted during the scope period.
- All analytical file(s) active during the scope period.
- A random sample of criminal investigations closed during the scope period.

The sample sizes for the random samples of initial leads and criminal investigations were calculated based on a 95% one-tail confidence level, an expected error rate of 6%, and various plus precisions.^{5,6} The detailed audit work plan approved by Commissioners Skobin and Wong Yang delineates tests for each audit area (initial leads, CI packages, etc.).

The approximately 40 audit tests are not itemized in this report but are available upon request. Lastly, the methodology noted herein is consistent with the methodologies of prior audits conducted during the pendency of the Consent Decree and Transition Agreement.

SUMMARY OF RESULTS

The results of the Audit reflected substantial compliance with Commission guidelines, including that closed criminal investigations conducted by the ATIS, MCD, represents valid criminal investigations, *not* intelligence investigations. Moreover, in response to the prior year's Audit, the ATIS developed and implemented additional internal controls to assure compliance with Commission guidelines and to guard against risks inherent in obtaining and securing intelligence. Each investigation was opened only after the appropriate threshold was met, and closed when ATIS investigators determined that the individual suspected of terrorist activity no longer presented a threat to the City of Los Angeles or the actions required referral to another law enforcement agency or Department entity for appropriate investigation.⁷

³ Working folders, which are created by the investigator for each individual who is the subject of an approved open intelligence investigation, were also reviewed.

⁴ Some of the confidential informant packages reviewed were identified during our review of either preliminary or open intelligence investigation files.

⁵ Plus precisions of 7% for initial leads and 10% for criminal investigations.

⁶ This sample size calculation formula is a generally accepted auditing practice. A detailed explanation of each parameter is available from the OIG Audit Section.

⁷ See Required Threshold for Opening Investigation in the Levels of Intelligence Investigation Activity on Page 2.

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 4 of 7

Furthermore, the investigation files were well-organized and the documentation noted therein adequately supported the investigation, which suggests that the internal protocols implemented since the prior year's Audit have had a positive impact on the manner in which intelligence is gathered and maintained. Additionally, all MCD personnel contacted during the Audit were extremely cooperative, promptly provided all documents that were requested, and were responsive to all other requests.

Notwithstanding this substantial compliance, the Commission identified two issues that need further review and remediation: (1) documentation of supervisory oversight for criminal investigations and (2) articulation of reasonable suspicion to start open intelligence investigations.

DETAILED FINDINGS

Documentation of Supervisory Oversight for Criminal Investigations

Background: The Criminal Investigation Section (CIS) is housed within MCD, which enables MCD to quickly respond to incidents having a criminal predicate and to dedicate investigative resources concurrent with, but independent from, intelligence investigations. With respect to the dissemination and transfer of intelligence investigations to the CIS, a MCD Intradepartmental Correspondence, dated November 8, 2006, provides:

In order to properly track intelligence investigations referred to the CIS, a case referral form has been developed (see attachment). The concerned Intelligence Investigator shall complete the CIS Referral Form when referring an intelligence case to CIS for criminal investigation. This includes Initial Lead, Preliminary, or Open Intelligence Investigations. In addition, ATIS personnel that refer cases(s) containing information obtained from other official sources shall also complete a referral form. At the conclusion of the criminal investigation, the assigned CIS investigator shall complete the disposition portion of the form and store it in the respective CIS case package.

Issue: The purpose of this review of criminal investigation(s) was to ensure that each investigation had a nexus to criminal activity, that the probable cause standard was met, and that the protocols governing the transfer and dissemination of intelligence investigations were strictly adhered to. During the review, the Commission determined that there was no evidence that CIS investigators departed from procedures and controls governing the transfer or dissemination of intelligence investigations or initiated criminal investigations without probable cause. However, it was apparent that the CIS did not have a formalized documentation process by which CIS supervisors could assess whether CIS investigations conflicted with or involved intelligence investigations prior to the initiation of a criminal investigation.

Risk: Intelligence investigations are subject to extensive scrutiny to guard against constitutional violations involving freedom of association, free speech, and unlawful searches and seizures.

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 5 of 7

At issue, is the risk that the procedures and controls governing intelligence investigations could be circumvented by classifying them as criminal investigations for purposes of expediency or otherwise. Further, while the Commission is aware that CIS supervisors verbally discuss the merits of each case prior to the commencement of a criminal investigation, this method of supervisory oversight does not document the substance of supervisory review and may yield inconsistencies among supervisors tasked with approving criminal investigations.

Management's Response to Issue: Management of MCD expressed agreement with this issue. As a result, the ATIS changed the CIS Data Input Sheet and related checklist to initiate a criminal case so that it requires the signature of the approving supervisor and the substance of his or her review.

Articulation of Reasonable Suspicion to Start Open Intelligence Investigations

Background: An open intelligence investigation may be initiated when: (1) Reasonable suspicion, based upon reliable information, exists that an individual or organization may be planning, threatening, attempting, performing, aiding/abetting, or financing unlawful acts, and (2) The results of the unlawful acts are intended to further their societal objectives, influence societal action or harass on the basis of race, religion, natural origin, or sexual orientation.

According to Commission guidelines, reasonable suspicion is:

An honest belief, based on known articulable circumstances, which would cause a reasonable and trained⁸ law enforcement officer to believe that some activity, relating to a definable criminal activity or enterprise, may be occurring or has the potential to occur.

Issue: For 3 of the open intelligence investigations evaluated, the Commission concluded that the initial Intelligence Report itself did not adequately document reasonable suspicion before the investigation was started. However, after Commissioner Skobin conducted further discussion with ATIS personnel and a review of additional documentation, the Commission concluded that, apart from this initial Intelligence Report, there was documentation and information that adequately supported that reasonable suspicion existed *before* the investigation was started.

Risk: If the initial Intelligence Report approved by management does not "stand alone" in adequately articulating reasonable suspicion, an open intelligence investigation could possibly be started without the existence of reasonable suspicion.

Management's Response to Issue: Management of MCD expressed agreement with this issue. As a result, investigators and supervisory personnel within ATIS are being provided training to ensure that Initial Intelligence Reports are sufficiently detailed to demonstrate a reasonable suspicion in order to start an investigation. Additionally, as ATIS has changed the CIS Data

⁸ Trained specifically in terrorism intelligence.

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 6 of 7

Input Sheet and related checklist to initiate a criminal case so that it requires the signature of the approving supervisor and the substance of his or her review.

OTHER RELATED MATTERS

With the exception of the guidelines pertaining to the Department's Secret Working Environment, the Commission noted that the ATIS's policies and procedures governing the manner in which intelligence information is gathered and maintained has not been thoroughly reviewed and/or revised since 2003. In light of changes in the methods and modes of terrorist activity, technology, social media, open source information, and Department of Justice (DOJ) guidelines, the Commission requests that the Department thoroughly review its current standards and procedures to prevent and investigate terrorist activity and to report back to the Commission any recommended changes to policies and procedures that it believes the Commission should consider. The Department should also give special attention to DOJ guidelines to ensure that its methods to prevent and investigate terrorist activity are consistent with national standards and are consistently applied.

During discussions with MCD and ATIS personnel, the Commission determined that field and other personnel were not adequately supplied with equipment necessary to investigate and prevent terrorist activity. For example, it appears that the telephones used by field personnel are outdated and do not include the ability to send or receive photographic images or effectively communicate covertly during surveillance activities. Furthermore, in some instances the radio packages in the surveillance cars are not compatible from squad to squad. This is particularly problematic in larger multi-squad operations. While there are "fixes," such as combining officers from different squads on emergency call-outs, this is not a preferred practice for multiple reasons. Another example of an unmet equipment need is that MCD lacks "situation room technology" that would enable it to monitor field operations in real time or provide adequate oversight of field operations occurring at multiple locations. Moreover, this technology would help assure the "interoperability" of Department resources and enable MCD to keep abreast of counter-surveillance methods and technologies underlying their function. Finally, the Commission requests MCD to make it aware of equipment that may facilitate or enhance MCD's ability to prevent and investigate terrorist activity having a nexus to the City of Los Angeles.

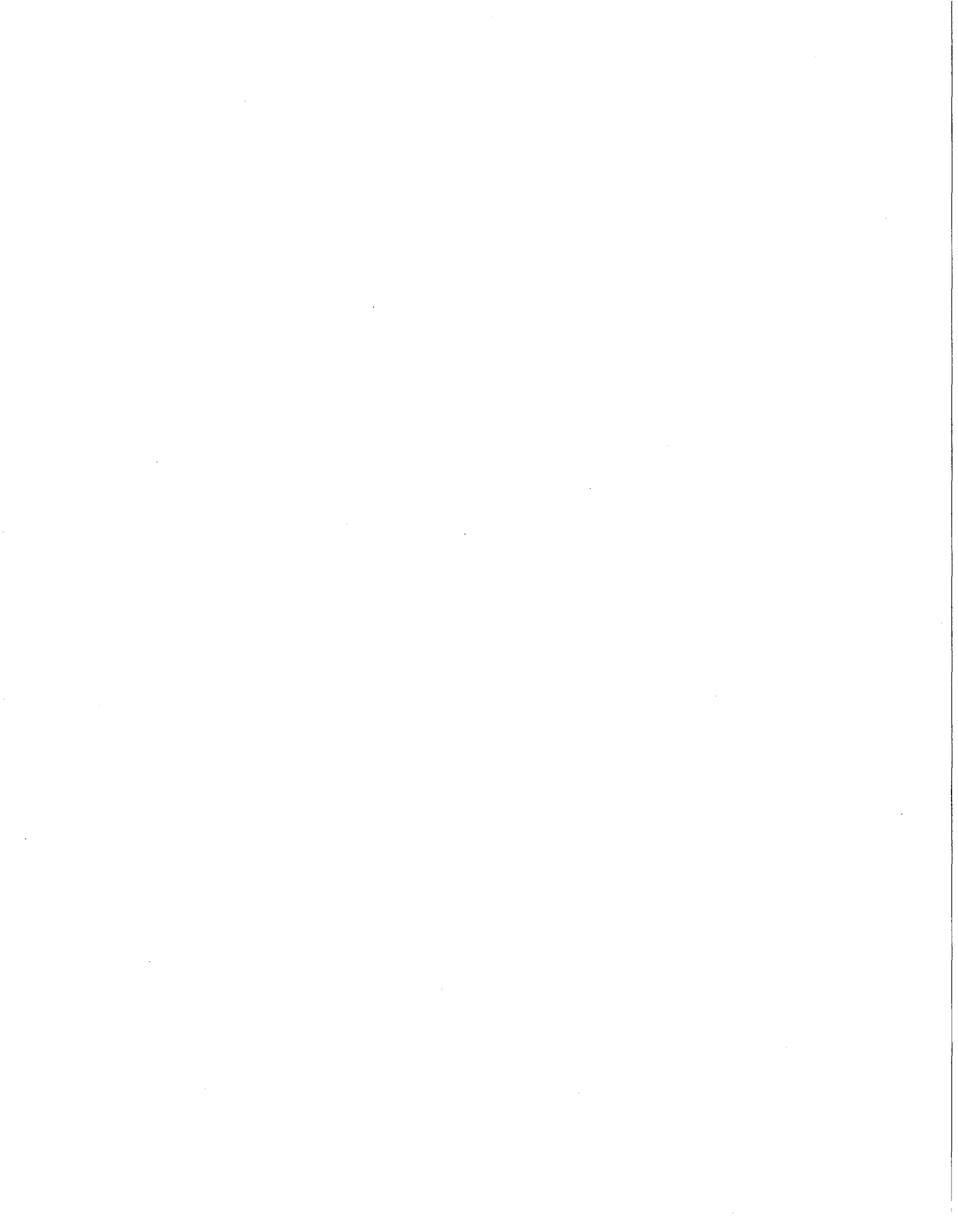
CONCLUSION

The results of the Audit reflected substantial compliance with Commission guidelines. Each investigation was opened only after the appropriate threshold was met and closed when ATIS investigators determined that the individual suspected of terrorist activity no longer presented a threat to the City of Los Angeles, or his/her actions required referral to another law enforcement agency or Department entity for appropriate investigation.

As noted above, all personnel contacted during the Audit were extremely cooperative, promptly provided all documents that were requested, and were responsive to all other requests.

BOARD OF POLICE COMMISSIONERS
ANTI-TERRORISM INTELLIGENCE SECTION AUDIT
FISCAL YEAR 2009/2010
PUBLIC VERSION
Page 7 of 7

These actions, the Audit findings, and improvements that were made by MCD both subsequent to the prior Commission audit and during the course of this Audit, demonstrated a commitment by MCD personnel to transparency and adherence to policies, guidelines and procedures. We particularly acknowledge the outstanding work of the MCD Compliance Officer.



MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 1
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: INTELLIGENCE REPORTING PROCEDURES FOR ANTI-TERRORISM INTERLLIGENCE SECTION FUNCTION

This directive will assist personnel in differentiating between and understanding the responsibilities associated with:

- Open Intelligence Investigations
- Preliminary Investigations
- Initial Lead Investigations
- Victim Files

Open Intelligence Investigations

Employee's Responsibility. The **initial** Open Intelligence investigation shall be reported on an Intelligence Report, Form 1.89. The report shall contain information compiled by the concerned Investigation and Analyst. All identifying information shall be entered into LACLEAR.

The assigned Analyst or Investigator may write the Intelligence Report. The writing of the Intelligence Report should be a collaborative effort between the Analyst and Investigator. In some instances, only the assigned Analyst or Investigator will write the report depending on the type of reporting required. The Section Officer in Charge shall make the final determination on who should write the concerned Intelligence Report.

A Follow Up Intelligence Report (Update) shall be completed at least twice per year thereafter. The narrative will be completed on white paper and contain the following headings:

- Individual: Name of subject(s)
- Organization: Name of Organization with which the subject is affiliated. If no affiliation can be determined, list as: No Affiliation
- Resume: A brief summary of the report

- Details of Report: The investigator shall keep a chronological log listing the actions accomplished on the case and a chronological narrative of the actions of the suspect(s) or organization. The assigned Investigator or Analyst will use the chronological narrative to update the investigation.

Mandatory Headings: When initiating an OPEN intelligence investigation on an individual or organization, the following headings are mandatory:

Reasonable Suspicion: Articulate the reasonable suspicion that the individual or organization may be involved in terrorist activity. This would include all known facts that support reasonable suspicion.

Reasonable suspicion is defined in the *Standards and Procedures for Anti-Terrorist Division, approved March 18, 2003*, as “an honest belief based on known articulable circumstances which would cause a reasonable and trained law enforcement office to believe that some activity relating to a definable criminal activity or enterprise may be occurring or has a potential to occur.”

Reliable Information: Articulate the source of the reliable information and how it is trustworthy of confidence. This information could come from personal observation, informant information or other law enforcement or official sources.

- Analysis: An analysis of the investigation compiled from information obtained from the investigator and all other sources, shall be completed by the assigned Analyst.
- Updated Information: this line may not always be used but may include, adding, deleting or changing indentifying information such as address, vehicles, etc.
- Concerned Investigator/Analyst Name and Serial No.
- Date Report Completed

Note: An ATIS Routing Slip shall accompany the report.

Follow Up Intelligence Report

The Follow Up Intelligence Report shall be used to report information concerning the investigation and completed on plain white paper after the initial Intelligence Report has been approved by the Commanding Officer. The above heading with the exception of Reasonable Suspicion and Reliable Information, shall be used in the Follow Up Report.

Preliminary Investigations

The Preliminary Investigation should be undertaken where there is information or an allegation, which indicates the possibility of terrorist activity. Preliminary Investigations are based on reasonable suspicion only and are for the purpose of determining whether or not the information or allegation can be developed to the point of reliability. The narrative shall contain information detailing the reasonable suspicion and how the information came to the Investigator's attention. The report shall contain the heading "**reasonable suspicion**" and a narrative clearly articulating the details of that reasonable suspicion.

The Preliminary Investigation (PI) shall be requested on an Employees Report, Form 15.7 to the Commanding Officer, Major Crimes Division. The investigation shall commence when the Commanding Officer approves the request. Verbal approval may be obtained prior to completion of the report and shall be documented in the 15.7. The PI shall not exceed 120 days.

Initial Lead Investigations

Initial Lead investigation shall be initiated on a Terrorism Lead Sheet. Subsequent investigative reporting shall be done on plain white paper. Initial Lead Investigations shall be completed within 60 days from the date of receipt of the specific lead from the reporting party.

Note: All Initial Lead and Preliminary Investigations shall be stored separately from intelligence files unless the investigation results in an approved Open Investigation

Employee's Responsibility. Employees are responsible for completing the initial lead investigation within 60 days. Supervisors shall be consulted in a timely fashion when circumstances arise that may preclude completion of the investigation within the required time period.

Supervisor's Responsibility. Supervisors shall ensure that Preliminary and Initial Lead Investigation are completed within the required time frame. Supervisors shall also utilize appropriate tracking controls to ensure timely completion of the respective investigation.

Victim Files

Victim files may be initiated when a person, not the official position or office, is a victim of a terrorist act related to an OPEN intelligence investigation. The information shall be reported on an Intelligence Form, form 1.89. A Follow Up Report is due at least twice a year from the date of the initial file being opened.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 2
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: INVESTIGATORS WORKING FOLDER FOR THE ANTI-TERRORISM INTERLLIGENCE SECTION FUNCTION

This directive will assist personnel in their responsibilities related to the Investigator's Working Folder

- Working folder defined
- Type of work product permitted for storage
- Identification of documents
- Removal of non material information

Investigator's Working Folder

The Investigator's Working Folder is retained by the assigned investigator and is specifically designated to contain the investigative materials gathered, received, and developed for the specific purpose of updating an approved ongoing Open Intelligence Investigation. The Working Folder shall not be part of the Open Intelligence File.

Type of Work Product Permitted for Storage

The Investigators Working Folder may contain a variety of documents, working notes, photographs, etc., which are either material to the investigation, or information which the materiality has not yet been determined.

Employee Responsibility. The documents, etc., contained in the Investigator's Working Folder shall be kept in a clearly marked folder/binder, etc., and stored in file cabinets designated for storage. The folder may be temporarily stored in a locked work place file cabinet or drawer when in use.

The employee shall make reasonable ongoing efforts to establish materiality on all documents contained in the Investigator's Working Folder.

Identification of Documents

Employee Responsibility. Each document in the Investigators Working Folder shall have an I/O Note Stamp completed by the concerned investigator that identifies the following:

- Nature of the document or item (DMV print out, photograph)
- How the information is material to investigation or materiality yet to be determined (Photo of subject, etc)
- Date the document or item was obtained.

Note: Multiple page documents can use one stamp on the first page indicating the number of pages such as: 1 of 20, etc.

Purge of Non-Material Information

One element of the intelligence process is the purging of information and/or documents that are no longer material to the investigation. Generally, the law requires that information in which materiality cannot be determined within five years, shall be removed. Non material information shall be removed from the concerned file and purged (destroyed).

Employee Responsibility. When information is determined to be not material to the investigation, it shall be immediately removed from the working folder and destroyed.

Supervisor Responsibility. Supervisors shall audit the Investigator's Working Folder **at least three times a year** to ensure that only appropriate information is stored and that the work folder is being appropriately maintained. The supervisor shall document those inspections on the Investigator's work folder and initial, date and record his/her serial number.

Note: When initiating an Open Intelligence Investigation on an individual or organization that was previously *closed*, the notes from the closed Investigator's Working Folder shall not necessarily become part of the new file. Information or documents from the previously closed folder may be incorporated into the new folder only if it is material to the newly initiated investigation.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 3
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: SECURITY OF INTELLIGENCE FILES FOR THE ANTI TERRORISM
INTELLIGENCE SECTION FUNCTION

This directive will assist personnel in properly conducting the following activities:

- Procedure for reviewing Open Intelligence Files
- Possessing intelligence information outside the workplace
- Procedure for reviewing Closed Files

Procedures for Reviewing Open Intelligence Files

Anti Terrorism Intelligence Section (ATIS) Intelligence Files are maintained and secured in the MCD Administrative Section under the control of the Custodian of Records.

Employee Responsibility. Personnel requesting to review Intelligence Files shall comply with the following procedures:

- Possess a need to know and a right to know the requested information
- Articulate the need and right to know to the Custodian of Records or his designee and complete the Sign Out Card within the file .
- Review the material within the confines of the Administrative/ATIS area
- Do not make a photocopy of any Intelligence File without the approval of the Commanding Officer MCD, or his designee.

Possessing Intelligence Information Outside of the Workplace

Personnel assigned to the Anti-Terrorism Intelligence Section (ATIS) shall comply with the *Standards and Procedures for Anti-Terrorist Division, approved March 18, 2003*, which mandates that section personnel not maintain or utilize the division's intelligence materials outside of their official work location without the written approval of the Commanding Officer. Employees shall only use intelligence materials for official business.

Note: Intelligence related work product materials other than intelligence files, such as surveillance work sheets and DMV printouts, including materials in **electronic format**, may be possessed outside the workplace for specific duty related activity after obtaining verbal approval from the employee's immediate supervisor.

Information contained in an electronic format shall be safeguarded in the same manner as any other ATIS work product paper document. Intelligence Files may not be possessed in any format outside the MCD office without the approval of the Commanding Officer, MCD. Personnel assigned to the Joint Terrorism Task Force shall comply with applicable federal guidelines regarding classified or non-classified United States Government information.

Supervisor's Responsibility: Supervisors shall ensure that employees have a need to possess work-related materials outside the workplace.

Procedures for Reviewing Closed (Not Purged) Intelligence Files

Closed intelligence files may be reviewed after completing the Request for Review of Closed Files form (see attachment) and obtaining approval from the Commanding Officer, Major Crimes Division. One of the following criteria shall be met prior to reviewing the closed files:

- Analytic Work Product (terrorist trend analysis, etc.)
- New reasonable suspicion is acquired to initiate a Preliminary or Open Investigation on an Individual/Organization listed in the closed intelligence files.
- Police Commission Directed (audit or review)
- Other justified reasons approved by the Commanding Officer, i.e. criminal case, etc.

Note: When initiating an Open Intelligence Investigation on an individual or organization that was previously *closed*, only the information from the closed file deemed material to the new investigation, shall be incorporated into the new 1.89.

Note: Closed files within the five year limit required by California State guidelines and 28 CFR, Part 23, may be stored at MCD. All closed files over the five-year limit shall be purged from MCD files per City Attorney guidelines and Los Angeles City records retention policies. They essentially, no longer exist.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 4
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: SURVEILLANCE LOGS FOR THE ANTI TERRORISM SECTION
INTELLIGENCE FUNCTION

This directive will assist personnel in the proper:

- Storage of Original Surveillance Logs
- Disposition of Surveillance Logs on a Closed Intelligence Investigation

Storage of Original Surveillance Logs

The Custodian of Records or his/her designee in the Administrative Section shall store original surveillance logs for an Open Intelligence Investigation. Surveillance Logs for a Preliminary Investigation (PI) shall be stored by the assigned investigator. All surveillance logs shall be categorized by the specific individual/investigation. The assigned analyst or investigator may keep a copy of the surveillance log(s) in the respective Investigator's Working Folder or Analysis Folder.

Note: Surveillance notes of a Joint Terrorism Task Force (JTTF) case shall be stored at the JTTF facility.

Disposition of Surveillance Logs on a Closed Intelligence Investigation

After the investigation is closed (Open or PI), the surveillance logs shall be forwarded to the Custodian of Records for appropriate storage (as would all materials in the Investigators Working Folder). Analysis personnel may maintain a copy of surveillance logs from a closed case only if it is material to another OPEN intelligence investigation or related to terrorist trends. Approval shall be granted by the ATIS Officer in Charge.

Note: The criteria for review of closed investigation surveillance logs once stored in the closed files shall be the same as those for review of closed intelligence files.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 5
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: ANALYSIS UNIT INFORMATION AND DATA STORAGE FOR THE ANTI
TERRORISM INTELLIGENCE SECTION FUNCTION

This directive will assist personnel in understanding the intelligence analysis function and the storage criteria of Analysis Unit materials:

- Analysis Unit Function
- Storage of Analysis Unit Information and Data

Analysis Unit Function

Intelligence analysis requires individuals to gather information collected from a variety of resources, process that information and produce actionable intelligence. This actionable intelligence can be in the form of reports or briefing. The broader content of the material collected by analysts is necessary to make significant connections "connecting the dots", identify trends, and ensure that terrorist activity is not being overlooked. In order to develop actionable intelligence, analysts need to identify trends in terrorist activity, including previous terrorist activities and attacks, and all other material information that may assist in the prevention of terrorist attacks. Actionable intelligence includes, but is not limited to, providing direction to investigative entities and personnel for the purpose of investigating groups and individuals that may be threatening, attempting, planning, or performing acts that may significantly disrupt the public order, or harass based on race, religion, national origin, or sexual orientation. Actionable intelligence also included providing intelligence assessments and recommendations to personnel at all levels of the Department.

Due to the fact that personnel assigned to analysis need to maintain a larger volume of information to carry out their mission, analyst material must be maintained separate from intelligence files and investigator notes. The intelligence files focus on specific individuals and groups whereas the analyst products and briefings focus on providing investigative insight, support and direction. This fact does not preclude analysts from being able to articulate the materiality of stored information, nor does it preclude analysts from properly storing the information.

Storage of Analysis Unit Information and Data

The following information shall be used as a guide for analysts assigned to Major Crimes Division, Anti-Terrorist Intelligence Section (MCD-ATIS), in order to properly store and secure information:

- 1.) Analysts are responsible for maintaining and storing information and documents in Department facilities. Facilities include any location that MCD personnel are assigned or required to work. This includes various task force offices.
- 2.) Analysts must be able to articulate the materiality of all stored information and documents under their control and explain the organizational method used to store information under their direct control.
- 3.) Analyst supervisors are responsible for articulating the materiality of all shared analytical information and documents stored by ATIS/Analysis Unit.
- 4.) Analysts must be able to transport information, documents and intelligence to and from meetings, briefings, study and research tasks, investigative assignments, etc. **The security of this information and the returning of the information to MCD is the responsibility of the individual analyst.** At times, Analysts may be required to travel and may be unable to return to MCD facilities at the end of watch. Overnight storage of information may then be granted by an Analyst supervisor. Again, the information shall be returned in a timely manner and proper security of the information is the responsibility of the analyst.
- 5.) Information stored on computers or electronic medium (removable hard drives, discs, etc.) requires the same level of scrutiny as hard copy documents. Analysts are required to articulate the materiality of all information contained on computers and electronic medium and explain the organizational method used to store the information.

The following list will help analysts define the materiality of information:

- 1.) Material to an MCD criminal investigation;
- 2.) Material to a criminal or intelligence investigation by another agency or task force;
- 3.) Material to an Open Intelligence Investigation;
- 4.) Material to a Preliminary Investigation;
- 5.) Material to an Initial Lead Investigation;
- 6.) Material to an Intelligence Control Center Lead;
- 7.) Material to the study of terrorist trends;
- 8.) Material to the study of terrorist methods, tactics, or activities;
- 9.) Material to the study of behavioral patterns associated to terrorist groups and individual;
- 10.) Material to identifying associations between individuals believed to be involved in terrorist activity;
- 11.) Material to the study of world events, country profiles and trends; and
- 12.) Training aids

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 6
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: SURVEILLANCE AND FIELD OBSERVATIONS FOR ANTI
TERRORISM INTELLIGENCE SECTION FUNCTIONS

This directive will provide guidance in distinguishing between surveillance and field observations.

- Surveillance defined
- Field observations (Monitoring) defined
- Surveillance approval

Surveillance Defined

The *Standards and Procedures for Anti-Terrorism Division, approved March 18, 2003*, (now MCD/ATIS), defines surveillance as the continuous or prolonged observation of a targeted individual or group by clandestine means for the purpose of collecting information material to an approved Preliminary Intelligence Investigation or Open Intelligence Investigation.

Field Observations (Monitoring) Defined

For the purpose of this order, monitoring is defined as: the short term or preliminary act of observing or watching (spot checks), the activities of an individual by Anti Terrorist Intelligence Section (ATIS) investigators for the purposes of gathering information relevant to an Initial Lead Investigation, Preliminary Investigation or Open Intelligence Investigation. This short term monitoring activity shall not rise to the level of "Surveillance" as defined in *Standards and Procedures for Anti-Terrorist Division, approved March 18, 2003*.

Spot checks are conducted on individuals during Initial Lead Investigations to verify residence or business locations or the whereabouts of individuals and not to conduct a clandestine surveillance.

Note: An Initial Lead investigation may evolve to the level of reasonable suspicion for a Preliminary Investigation (PI).

In these cases, an investigator may consider obtaining approval from the commanding Officer for a PI, and then utilize surveillance as an investigative technique.

Surveillance Approval

Surveillance is an approved investigative technique for Preliminary and Open Intelligence investigations. The distinction between surveillance and monitoring is based primarily on the purpose and duration of the investigative activity.

Note: Field observations or “location checks” are an investigative tool less intrusive than surveillance and does not require prior approval.

Employee responsibility: Employees requesting surveillance from either dedicated surveillance assets or another entity, shall obtain approval from their immediate supervisor and the Officer in Charge, Anti Terrorism Intelligence Section. All surveillance requires the approval of the Commanding Officer.

Supervisor responsibility: the concerned supervisor shall ensure the specific case merits surveillance and that all appropriated information, especially officer safety issues, are communicated to the assigned surveillance entity.

Note: When receiving a request from the JTTF to use MCD surveillance assets, the concerned MCD- JTTF supervisor shall complete a Surveillance Request Form (see attachment) for the purposes of obtaining approval of the Commanding Officer. When approved, the form shall be returned to the JTTF.

All surveillance logs for JTTF cases shall be stored at the JTTF facility unless being utilized for Analysis purposes.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 7
15.1

Date: April 12, 2006

TO: Concerned Personnel

From: Commanding Officer, Major Crimes Division

SUBJECT: UNDERCOVER INVESTIGATIONS FOR ANTI TERRORISM
INTELLIGENCE SECTION FUNCTIONS

This directive shall assist Anti Terrorism Intelligence Section (ATIS) personnel in understanding the approval level required for undercover investigations.

- Undercover investigation defined
- Undercover investigation approval requirements

Undercover Investigation Defined

The *Standards and Procedures for Anti Terrorist Division approved March 18, 2003*, (now MCD/ATIS), define an undercover investigation as: "A Los Angeles Police Officer who pursuant to an approved terrorist investigation, clandestinely obtains information about individuals or organizations through the development of **ongoing** relationships with such individuals or organizations."

Undercover Investigation Approval Requirements

For the purpose of this order, ATIS investigators shall be aware that the following criteria shall be satisfied prior to the conducting of an ATIS undercover operation.

1. Ensure that other investigative techniques are available or ineffective to achieve the investigative objectives of the Department.
2. Obtain approval from the Commanding Officer, Major Crimes Division and the Commanding Officer, Counter Terrorism and Criminal Intelligence Bureau.
3. Obtain approval of the Police Commission as outlined in the *Standards and Procedures for Anti Terrorist Division, approved March 18, 2003*.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 8
15.1

Date: April 12, 2006

TO: Concerned Personnel (ATIS and OCS)

FROM: Commanding Officer, Major Crimes Division

SUBJECT: DISSEMINATION OF INTELLIGENCE INFORMATION

This directive will assist personnel in understanding the criteria for disseminating intelligence information:

- Dissemination defined
- Dissemination limits
- Dissemination of information from the Investigator's Working Folder
- Joint agency investigations

Dissemination defined

The communication of any Intelligence File information to any person not assigned to Major Crimes Division's direct chain of command. All dissemination is based on a need to know and right to know."

Note: Intelligence File information is that information maintained for an Open Intelligence Investigation such as an Intelligence Report, Form 1.89.

Any member of Major Crimes Division (MCD) who copies, permits inspection of, or disseminates intelligence information directly from intelligence files shall record the:

- Date
- Name of officer disseminating
- Name of the individual receiving
- The reason for the dissemination
- The information disseminated
- Reliability of the information

The above listed requirements shall be satisfied by completing the Information Dissemination Log (IDL), see attachment.

Note: dissemination of information requiring an IDL is specific Intelligence File information, not general or non-specific information.

Dissemination Limits

Only that information specifically justified by the need and right to know may be disseminated. Not all dissemination that meets the need and right to know criteria merits a total disclosure of information. Each request for a dissemination of information should be based on the specific need, on a case by case basis.

Dissemination of information from the Investigator's Working Folder

The materials contained in the Investigator's Working Folder are NOT considered part of the intelligence file and information may be disseminated based on a need and right to know.

Joint Agency Investigations

In the case of joint investigation, the Commanding Officer, MCD, may authorize a free flow of information on the particular individuals(s) and organization(s) being investigated, as long as a need and right to know exists.

Note: MCD personnel shall not disseminate information deemed **classified** by the United States government without receiving permission from the involved federal agency and **verifying** appropriate federal clearances are in order.

Third Party Dissemination

Permission is required for third party dissemination whether the information is classified or not.

MAJOR CRIMES DIVISION

D I V I S I O N A L O R D E R NO. 9
15.1

Date: April 12, 2006

TO: Major Crimes Division Personnel

FROM: Commanding Officer, Major Crimes Division

SUBJECT: USE OF LACLEAR FOR ALL INVESTIGATIONS

This directive will assist personnel in understanding and properly:

- Accessing the Los Angeles County Regional Criminal Information Clearinghouse (LACLEAR)
- Initial Lead Inquiry (Not Stored)
- Making an LACLEAR Inquiry (Stored)

Procedure for Accessing LACLEAR

The primary purpose of LACLEAR is deconfliction of events in order to avoid tactical confrontations between agencies and to connect investigators together to confer on concurrent investigative interests.

Employee Responsibility. The Investigating Officer of the particular case shall be responsible for checking the LACLEAR database and making a notation of the date on the chronological record. All LACLEAR inquiries require a completion of the LACLEAR Control Form, which shall be stored in the working folder. Personnel shall telephonically contact the LACLEAR region office at [REDACTED]

Note: Information deemed proprietary by another agency such as the Joint Terrorism Task Force (JTTF) shall not be checked without the express permission of the concerned agency.

Making an Inquiry (Not Stored)

Initial Lead information that does not meet the reasonable suspicion standard of 28 CFR shall be checked with LACLEAR, however it will NOT BE STORED.

Only information meeting the 28 CFR standard can be stored in the LACLEAR database. This information will be stored for a period of five years.

Note: 28 CFR is the federal law controlling the storage of intelligence information in governmental databases. This law requires that there is reasonable suspicion that the subject of the information is or may be involved in criminal conduct or activity.

Making an Inquiry (Storing Information)

Identifying information, such as name, DOB, address, telephone and license plate number(s) shall be entered into LACLEAR on all criminal cases, preliminary and open intelligence investigations. Since these investigations meet the reasonable suspicion standard of 28 CFR, this information shall be designated as **stored**.

Participation in the system does not require summaries or investigative information other than the type of suspected criminal activity the subject may be involved.

There are three (3) levels of confidentiality: Open, Limited, and Restricted. Generally, investigating officers should designate the confidentiality level as "**limited**." In this category, a "hit" on the limited information will result in an immediate notification to the Investigator. The agency member initiating the query will receive from LACLEAR only the investigating officer's name and phone number. The assigned investigator will then make a decision on what if anything will be shared with the other agency making the query. Dissemination of both criminal and intelligence information shall be based on a need and right to know.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 10
15.1

November 20, 2006

TO: Concerned Personnel

FROM: Commanding Officer, Major Crimes Division

SUBJECT: INITIAL LEAD AND PRELIMINARY INVESTIGATION TIME
LIMITS

This directive will clarify issues related to the below:

- Investigative start and ending dates for Initial Lead Investigations
- Documenting the conclusion of Preliminary Investigations

INITIAL LEAD INVESTIGATION

Currently, most telephonic Initial Lead (IL) investigations are forwarded to the Joint Regional Intelligence Center (JRIC) where they are processed and a determination is made on what agency (FBI, local jurisdiction, etc) will conduct the investigation. Thus, the 60-time period for ATIS personnel to conduct the IL investigation, starts on the date ATIS receives the IL back from the JRIC as an assigned lead.

Note: In an emergency situation where ATIS receives an IL that is determined to be investigated by ATIS personnel without assignment by the JRIC, the commencement date begins upon receipt of the IL.

Employee's Responsibility. The assigned Investigating Officer shall document on the chronological log and the follow up report, the date that the IL was received from JRIC for investigation or the date ATIS assigned the IL to the investigator if it did not go to the JRIC first. In addition, the date the investigation ceased should be noted in the chronological log and report narrative.

Supervisor's Responsibility. Supervisors shall ensure that the date received is documented on the chronological log and follow up report and that the investigation was completed within 60 days when approving the closure of the case.

PRELIMINARY INVESTIGATION

The Preliminary Investigation (PI) shall be closed using an Employees Report, Form 15.7 to the Commanding Officer, Major Crimes Division. This report shall include the date that investigation ceased. This date will document that the investigation was conducted within the 120-day time limit. In addition, the follow up report narrative shall also include a notation on when the investigation was concluded.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 11
15.1

Date: March 16, 2007

TO: Concerned Personnel (Anti-Terrorism Intelligence Section)

FROM: Commanding Officer, Major Crimes Division

SUBJECT: INVESTIGATOR'S WORKING FOLDER (AMENDMENTS)

This directive will provide additional guidance to personnel in regards to documents required for the Investigator's Working Folder (IWF).

- Requirement for creating an Investigator's Working Folder
- Inclusion of Initial Lead and Preliminary Investigations into the IWF

Requirement for creating an Investigator's Working Folder

Individual Open Intelligence Investigations

Employee's Responsibility. The Investigating Officer shall be responsible for creating an Investigator's Working Folder for each individual who is the subject of an approved Open Intelligence Investigation.

Organization Intelligence Investigation

It is optional to create an Investigator's Working Folder for an approved Organization Open Intelligence Investigation. However, information contained in the Intelligence Report shall be properly cited or referenced in the narrative of the Intelligence Report as appropriate.

The decision to create or not to create an Investigator's Working Folder shall rest with the Officer in Charge, ATIS, with appropriate written justification for not creating one. The justification will be documented in the intelligence file itself.

Supervisor's Responsibility. Supervisors shall ensure that an IWF is completed for individual investigations and that sources of information are properly referenced when completing the narrative of the organization intelligence report.

Inclusion of Initial Lead and Preliminary Investigations into the IWF

A copy of the Initial Lead or Preliminary Investigation report(s) shall be included in the Investigator's Working Folder when the reports are associated to or contribute to the reasonable suspicion to initiate the Open investigation.

In addition, any applicable crime reports or documents that contribute to the reasonable suspicion shall also be included in the Investigator's Working Folder.

Employee's Responsibility. The Investigating Officer shall be responsible including a copy of the concerned Initial Lead, Preliminary Investigation Report or other related document when applicable, to the Investigator's Working Folder for all Open Intelligence Investigations.

Supervisor's Responsibility. Supervisors shall ensure that periodic reviews are conducted to ensure that a copy of the appropriate Initial Lead or Preliminary Investigation Report and other applicable documents are included in the Investigator's Working Folder.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 12

October 30, 2008

SUBJECT: SURVEILLANCE APPROVAL PROCEDURE

Procedure: This Order provides a standardized surveillance approval process and the centralized storage of approved surveillance requests. Prior to conducting surveillance for approved investigations, Major Crimes Division (MCD) personnel shall obtain approval from the Commanding Officer, MCD.

Employee's Responsibility. When requesting MCD surveillance assets, or prior to initiating surveillance on a subject, the Investigating Officer (I/O) shall be responsible for ensuring that a MCD Surveillance Request is completed prior to conducting surveillance (see attachment). All pertinent information shall be entered on the Surveillance Request to provide surveillance personnel with the appropriate background information on the subject.

Upon completion of the Surveillance Request, the I/O shall submit the completed form to their immediate supervisor for review and approval. The form shall then be forwarded to the Officer in Charge of the respective section for approval.

NOTE: Surveillance conducted during spontaneous situations without an approved Surveillance Request, should be documented on the chronological record of the case. Any subsequent surveillance of the subject will require adherence to these procedures.

Supervisor's Responsibility. Supervisors shall ensure that the Surveillance Request is properly completed and approve the request by affixing his/her signature to the form. The completed Surveillance Request shall then be submitted to the Commanding Officer, MCD for approval. The approved request shall be forwarded to the Officer-in-Charge, Surveillance Support Section (SSS).

Officer in Charge Responsibility-Surveillance Support Section. The Officer in-Charge, SSS, shall ensure that an approved Surveillance Request is completed prior to assigning MCD-SSS personnel to a case.

NOTE: During exigent circumstances, the Commanding Officer, MCD may provide verbal approval for surveillance. A Surveillance Request shall be completed as soon as practicable by the Investigating Officer.

In addition, the Officer in Charge, SSS, shall ensure that all MCD Surveillance Requests are properly stored and maintained. A copy of the Surveillance Request should be kept in the Investigator's case package. Only one approved request is required per subject.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 13

February 18, 2009

TO: Concerned Personnel (Anti-Terrorist Intelligence Section)

From: Commanding Officer, Major Crimes Division

SUBJECT: FOLLOW UP INTELLIGENCE REPORT

Background: This Order changes the language contained in Division Order No. 1, issued April 12, 2006, regarding the reporting requirements for completion of Follow-Up Intelligence Reports related to Open Intelligence Investigations.

This order deletes the "twice per year" period requirement and changes the reporting requirement to **every six months**.

NOTE: The date that the Commanding Officer, Major Crimes Division, approves the initial Intelligence Report (Form 1.89), shall serve as the starting date for the six month period. For example, if a report is approved by the Commanding Officer on Jan 1, 2009, a follow up report is due no later than July 1, 2009.

Employee's Responsibility. The assigned lead Investigating Officer (I/O) is responsible for completing a Follow-Up Intelligence Report every six months. In addition, the I/O is responsible for completing the report and submitting it in a timely manner for appropriate approval by the Detective III and Officer in Charge respectively. The I/O shall allow sufficient time for the report to complete the review cycle.

Supervisor's Responsibility. Supervisors shall ensure that a follow up Intelligence Report is completed every six months and submitted in a timely manner.

Officer-in-Charge Responsibility. The Officer-in-Charge, Anti-Terrorist Intelligence Section (ATIS) shall ensure that Follow-Up Intelligence Reports are completed every six months.

Compliance Officer Responsibility. The Major Crimes Division/ATIS Compliance Officer shall have audit responsibility to ensure compliance with this order.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 14

February 18, 2009

TO: Concerned Personnel (Anti-Terrorist Intelligence Section)

From: Commanding Officer, Major Crimes Division

SUBJECT: INVESTIGATOR'S WORKING FOLDER AUDIT PROCEDURES

Background: The need to properly document the supervisory review of the Investigator's Working Folder (IWF) using a standardized audit control form has been identified. This Order covers the below issues related to the Investigator's Working Folder.

- Change of auditing requirement to every 3 months
- Standardized Audit Control Form

Procedure: Each active IWF shall be audited by a supervisor every 3 months. The ATIS Audit Control Form (see attachment) shall be used to record the audit of the IWF by a supervisor.

NOTE: The date that the Commanding Officer, Major Crimes Division approves the initial Intelligence Report (Form 1.89), shall serve as the starting date for the approval period. For example, if the initial 1.89 is approved on June 1, 2009, there shall be an audit no later than September 1, 2009.

Employee Responsibility. Each Lead Investigating Officer shall ensure that the Audit Control Form is included in the IWF for each Open Individual and Organization IWF.

Supervisor's Responsibility. Supervisors assigned to the Anti-Terrorist Intelligence Section (ATIS) shall ensure that the Investigator's Working Folder for personnel within their span of control is audited at least every 3 months. The concerned supervisor shall complete a notation on the Audit Control Form for each audit.

Officer-in-Charge Responsibility. The Officer-in-Charge, Anti-Terrorist Intelligence Section (ATIS) shall ensure that the Investigator's Working Folder is audited at least every 3 months.

Compliance Officer Responsibility. The Major Crimes Division/ATIS Compliance Officer shall have audit responsibility to ensure compliance with this order.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 15

February 18, 2009

TO: Concerned Personnel (Anti-Terrorist Intelligence Section)

From: Commanding Officer, Major Crimes Division

SUBJECT: INTEGRATED CASE BRIEFING SYSTEM

Background: This Order establishes a formalized schedule of briefings for personnel assigned to the Anti-Terrorist Intelligence Section (ATIS).

Procedure: An Integrated Case Briefing shall be held at least every three months per calendar year. The purpose of the briefing is threefold:

- Present a case update to supervisors to assess case viability
- Provide a scheduled period for a supervisor to review each Investigator's Working Folder (IWF) and complete the Audit Control Form.
- Review any applicable Follow Up Intelligence Reports

Employee's Responsibility. Each assigned lead Investigating Officer (I/O) shall make the IWF available for each respective Open Investigation. The I/O shall also be prepared to present a case briefing of assigned investigations and have any applicable follow up intelligence reports available for review.

Supervisor's Responsibility. Supervisors shall ensure that a review of the IWF is conducted during the case briefing period.

Officer-in-Charge Responsibility: The Officer-in- Charge, Anti-Terrorist Intelligence Section shall ensure that an Integrated Case Briefing is held at least every 3 months per calendar year.

Compliance Officer Responsibility. The Major Crimes Division/ATIS Compliance Officer shall have audit responsibility to ensure compliance with this order.

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 16

August 27, 2009

TO: Major Crimes Division Personnel

FROM: Commanding Officer, Major Crimes Division

SUBJECT: PRIVACY GUIDELINES FOR EVALUATION ENVIRONMENT INITIATIVE

Initiative Responsibility: The Commanding Officer, Major Crimes Division (MCD), shall have primary responsibility for participation in the Information Sharing Environment – Suspicious Activity Report (ISE-SAR) Evaluation Environment Initiative and for the enforcement of all policies and procedures related to the Initiative.

Privacy Officer: The Commanding Officer, MCD, will designate and ensure the MCD Privacy Officer receive the appropriate training. The MCD Privacy Officer shall be responsible for:

1. Handling reported violations of policy related to the Initiative;
2. Ensuring that MCD adheres to applicable provisions of the ISE Privacy Guidelines for handling terrorism-related information;
3. Continually identifying and assessing laws, orders, policies and procedures applicable to ISE-SAR information. In so doing, make recommendations to the Commanding Officer, MCD, or other appropriate official(s), regarding changes in LAPD/MCD policy related to ISE-SAR information.

Application of 28 CFR Part 23: All ISE-SAR information posted to LAPD's shared space under the Initiative shall meet applicable provisions of 28 CFR Part 23. This is to include applying the operating policies set forth in 28 CFR § 23.20 to all individual and organizational criminal subjects, the establishment and use of sensitivity and confidence (source reliability and content validity) codes and the receipt and collection of criminal intelligence information (CII). It also includes secure storage, access and dissemination, retention, periodic review, validation and appropriate purge of CII.

All ISE-SAR information in the shared space will be labeled as CII, subject to recipients following 28 CFR Part 23 operating policies with respect to the use and security procedures. Such information will be available only to law enforcement agencies with a need and right to know in the performance of a law enforcement activity.

Investigation of Errors: MCD shall, with regard to ISE-SAR information:

1. Investigate, in a timely manner, alleged errors and deficiencies and correct or delete information found to be erroneous or deficient;

2. Reevaluate the labeling of such information in the shared space when new or updated information is received that has an impact on confidence in the information;
3. Make every reasonable effort to ensure that such information will be corrected or deleted from the shared space upon concluding that the information is:
 - Erroneous, misleading, obsolete, or otherwise unreliable;
 - The information was gathered illegally or without authority.

When the rights of the subject of inaccurate, incomplete, incorrectly merged, or out of date information may be affected by the use of such information, all recipient agencies of the information will receive electronic notification of the need to destroy the information.

Analysis: ISE-SAR information received by MCD or accessed from other sources shall be collated and analyzed only by qualified personnel who have successfully completed a background check and any required security clearance.

Merger: ISE-SAR information about an individual or organization from two or more sources shall be merged only if there is sufficient identifying information to reasonably conclude the information is about the same individual or organization. If there is a partial match the information may be associated if accompanied by a clear statement that the match has not been fully established.

Information Access and Redress: ISE-SAR information shall not be available to the public, as provided by applicable LAPD policy, nor shall the existence or nonexistence of specific information be confirmed to persons or agencies that are not eligible to receive the information.

If an individual, using existing LAPD information request/complaint mechanisms, has a complaint or objection to the accuracy or completeness of ISE-SAR information about him or her that is alleged to be held by LAPD or MCD, MCD will acknowledge the complaint and state that it will conduct an appropriate review. If there is any personal information about that individual in an ISE-SAR, the information will be (1) reviewed and verified, or (2) corrected or deleted from the ISE-SAR shared space if the information is determined to be erroneous, include incorrectly merged information or is out of date. A record will be kept of all complaints and requests for corrections and the resulting action, if any.

Security: The Commanding Officer, MCD, will designate a security officer for the ISE-SAR Initiative and ensure they are adequately trained. MCD will operate in a secure environment that is protected from external intrusion, using secure internal and external safeguards against network intrusions of ISE-SAR and other sensitive information. Only ISE-SAR information reaching the 'reasonable suspicion' threshold will be submitted to the shared space. Outside access to the ISE-SAR shared space will be allowed only over secure networks. ISE-SAR information in the shared space will be secured such that it cannot be added to, modified, accessed, destroyed, or purged except by authorized MCD personnel. Access to ISE-SAR information within LAPD will be granted only to properly screened and trained personnel whose positions and job duties require such access. The Commanding Officer, MCD, shall ensure that

adequate review and audit mechanisms (including access logs) are in place to ensure that policies and procedures are at least as comprehensive as the ISE Privacy Guidelines requirements.

Data Breach: In the event of a data security breach, MCD will follow existing LAPD data breach notification policy found in the the Los Angeles Police Department Intelligence Guidelines.

Retention and Destruction: All ISE-SAR information in the shared space (CII) shall be reviewed for record retention (validation or purge) within 5 years of entry into the shared space in accordance with 28 CFR Part 23. Information submitted and determined to qualify as an ISE-SAR, but which does not reach the reasonable suspicion standard of 28 CFR Part 23, will be retained as a temporary file for up to one-year to permit the information to be validated or refuted and its credibility and value to be assessed. If the information remains under active review or investigation and continues to have credibility and value at the end of the one-year period, it may be retained for an additional one-year period with the approval of the Commanding Officer, MCD. Temporary files that are evaluated during their retention period and determined to meet applicable 28 CFR Part 23 and ISE-SAR criteria, shall be submitted to the shared space. When ISE-SAR information has no further value or meets the applicable criteria for purge, it will be removed from the shared space or the temporary file closed, as appropriate.

Transparency: The LAPD and MCD policies for ISE-SAR information shall be available to the public upon request or be made available on the LAPD web site. The Commanding Officer, MCD, is the point of contact for receiving and responding to inquiries and complaints about ISE-SAR. The Commanding Officer, MCD, shall facilitate public awareness of LAPD/MCD privacy policies and procedures related to ISE-SAR information.

Enforcement: MCD personnel and other authorized LAPD users shall report violations or suspected violations of LAPD/MCD policy applicable to ISE-SAR information to the MCD Privacy Officer. If an authorized user is not in compliance with LAPD/MCD ISE-SAR policies, the Commanding Officer, MCD, shall take appropriate action. This action includes, but is not limited to, suspension or discontinuation of access, suspension, demotion or termination of individuals, as authorized. If an external agency, request that such agency initiate appropriate sanctions or refer the matter to appropriate authorities for criminal prosecution.

MCD personnel shall cooperate with authorized audits and reviews related to the collection, receipt, review, collation and analysis, use, storage, dissemination, review and validation or purge of ISE-SAR information.


GREG R. HALL, Captain
Commanding Officer
Major Crimes Division

MAJOR CRIMES DIVISION

DIVISIONAL ORDER NO. 17
15.1

March 16, 2010

TO: Major Crimes Division Personnel

FROM: Commanding Officer, Major Crimes Division

SUBJECT: SECURITY PROCEDURES FOR MAJOR CRIMES DIVISION

Employees assigned to Major Crimes Division (MCD) should be aware that the nature of their work is confidential and sensitive. Information received and developed by MCD employees shall only be disseminated on a need and right to know basis. Additionally, employees assigned to Anti-Terrorism Intelligence Section (ATIS) shall be governed by the Standards and Procedures approved by the Board of Police Commissioners. The following are security precautions that MCD personnel shall consider during their daily assignment. This list will be periodically updated at the direction of the Commanding Officer of MCD to ensure that security procedures remain relevant and effective.

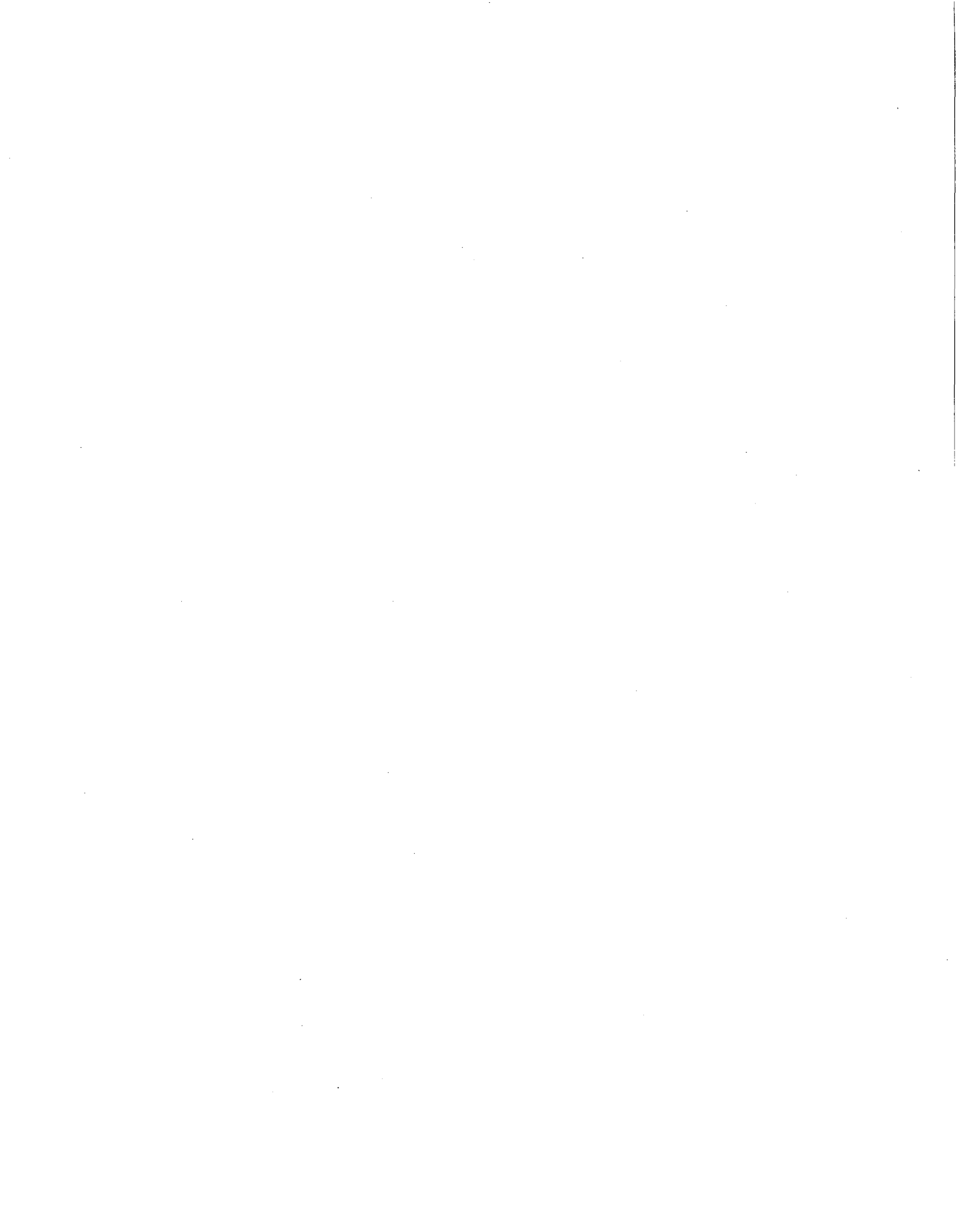
- Discussion of MCD information with non-MCD personnel is strictly prohibited, unless a need and right to know exists. MCD information would include: active criminal investigations, intelligence investigations, source reporting, surveillance reports or any other information not considered open source information. Under no circumstances shall MCD information be discussed with relatives, friends or former MCD employees. Former MCD employees shall be prohibited from discussing the above information upon conclusion of their assignment at MCD.
- While inside the MCD offices, all personnel are required to display appropriate law enforcement credentials. Visitors to MCD shall be escorted and display appropriate law enforcement or visitor identification. The MCD employee who allows office access to maintenance, repair and delivery personnel shall escort them, or assign another MCD employee the responsibility of escort. Unescorted visitors shall be challenged in order to determine the legitimacy of their presence in MCD offices.
- MCD personnel shall ensure that computers, laptops, and any storage devices containing sensitive and confidential information are not left unattended. The LAN system "G" drive (guarded drive) should be utilized for storage of sensitive or confidential information. External drives (i.e. thumb drives) should be utilized as a backup and should generally be secured in a locked cabinet during off hours. Information removed from the MCD office, whether hard copy or on an external storage device, should not be

left unsecured or in an unattended vehicle. ATIS personnel should be guided by the Standards and Procedures with regards to storage of intelligence.

- When no longer needed or eligible for retention, all sensitive and confidential MCD information shall be destroyed utilizing the Divisional shredders. This will ensure that inappropriate dissemination of information does not occur. Additionally, employees shall lock file cabinets and remove all sensitive and confidential material from the workspace.
- MCD personnel should consider utilizing conference rooms when discussing sensitive operations, source information or other confidential case related issues.
- Any employee who gains access to the MCD office during off-hours shall notify their immediate supervisor. That supervisor must ensure access was within the scope of their official duties.
- MCD personnel periodically receive calls requesting MCD information or employment verification. If the identity of the caller is in question, a return call shall be made to verify the caller's identity and their need and right to know, prior to the release of any information.
- MCD personnel having Federal Bureau of Investigation (FBI) security clearances shall be cognizant of the requirement to report any planned official or unofficial foreign travel, 10 days prior to departure. All foreign travel, including trips to Mexico and Canada, shall be reported in accordance with Department of Justice regulations. Unplanned trips to border countries shall be reported as soon as possible upon return to the United States. These notifications are to be made to the FBI Security Officer, at the FBI Office, 11000 Wilshire Blvd, West Los Angeles.



STEVEN S. SAMBAR, Captain
Commanding Officer
Major Crimes Division



OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 1

January 2, 2012

SUBJECT: REPORTING INCIDENTS POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM - REVISED AND RENAMED; SUSPICIOUS ACTIVITY REPORT, FORM 03.24.00 - ACTIVATED; SUSPICIOUS ACTIVITY REPORT NOTEBOOK DIVIDER, FORM 18.30.03 - REVISED; AND INVESTIGATIVE REPORT, FORM 03.01.00 - REVISED

EFFECTIVE: IMMEDIATELY

PURPOSE: This Order revises and renames Department Manual Section 4/271.46, *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*; revises the Investigative Report (IR), Form 03.01.00; and revises the Suspicious Activity Report (SAR) Notebook Divider, Form 18.30.03. Additionally, this Order activates the Suspicious Activity Report, Form 03.24.00.

The IR shall only be used to report criminal activity and shall no longer be used to report any act of suspicious activity. The IR has been modified to delete the "Suspicious Activity" checkbox on the IR face sheet. All acts of suspicious activities shall be reported on the Suspicious Activity Report.

PROCEDURE:

I. REPORTING INCIDENTS POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM - REVISED AND RENAMED. Department Manual Section 4/271.46, *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*, has been renamed as *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism* and has been revised as follows:

A. **Suspicious Activity Report.** A Suspicious Activity Report (SAR) is a stand-alone report used to document any reported or observed behavior/activity that may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may result from observations or investigations by police officers, or may be reported to them by private sources.

Suspicious activities reported on a SAR shall only consist of the following:

* **Breach/Attempted Intrusion.** Unauthorized individuals attempting to or actually entering a facility/infrastructure or protected site;

- * **Misrepresentation.** Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity. Impersonation of any authorized personnel (e.g., police, security, or janitor);
- * **Theft/Loss/Diversión.** Stealing or diverting (obtaining or acquiring) something associated with a facility/infrastructure [e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility];
- * **Sabotage/Tampering/Vandalism.** Damaging, manipulating, or defacing part of a facility/infrastructure or protected site;
- * **Cyber Attack.** Compromising or attempting to compromise or disrupt an organization's information technology infrastructure;
- * **Expressed or Implied Threat.** Communicating a spoken or written threat to damage or compromise a facility/infrastructure, protected site, and cyber attacks;
- * **Aviation Activity.** Operation or attempted operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people, buildings/facilities, infrastructures, or protected sites. Such operation may or may not be a violation of Federal Aviation Administration regulations;
- * **Eliciting Information.** Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person;
- * **Testing or Probing of Security.** Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities;
- * **Recruiting.** Building of operations teams and contacts, personal data, banking data or travel data;
- * **Photography.** Taking pictures or videos of facilities/buildings, infrastructures, or protected sites in a manner that would arouse suspicion in a reasonable person. Examples include taking pictures or videos of ingress/egress, delivery locations, personnel performing security functions (e.g., patrol, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.;

- * **Observation/Surveillance.** Demonstrating unusual interest in facilities/buildings, infrastructures or protected sites beyond mere casual or professional (e.g., engineers) interest, such that a reasonable person would consider the activity suspicious. Examples include observations through binoculars, taking notes, attempting to measure distances, etc.;
- * **Materials Acquisition/Storage.** Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would consider the activity suspicious;
- * **Acquisition of Expertise.** Attempts to obtain or conduct training in security concepts, military weapons or tactics, or other unusual capabilities such that a reasonable person could consider the activity suspicious;
- * **Weapons Discovery.** Discovery of unusual amounts of weapons, explosives, or their components that would arouse suspicion in a reasonable person; or,
- * **Sector-Specific Incident.** Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems or functions.

Note: These activities may be constitutionally-protected activities and should therefore not be reported in a SAR, absent articulable facts and circumstances that support the source's suspicion that the behavior observed is not innocent, but rather reasonably indicative of suspicious activity associated with terrorism. Race, color, religion, national origin, gender, age, physical or mental disability, marital status, sexual orientation, gender identity, gender expression, creed, ancestry, or medical condition shall not be considered as factors that create suspicion, although these factors may be used as specific-involved person descriptors.

- B. **Involved Person.** An involved person (IP) is an individual that has been observed engaging in suspicious activity, when no definitive criminal activity is identified, thus precluding their identification as a suspect.
- C. **Potential Target.** A potential target is a person, facility/building, infrastructure or protected site that is or may be the object of the suspicious activity.

II. REPORTING AND INVESTIGATIVE RESPONSIBILITY FOR SAR-RELATED INCIDENTS AND CRIME AND/OR ARREST REPORTS. All reports of suspicious activity shall be reported on a SAR. The Division of Records (DR) number for all associated reports (e.g., Property Report, Form 10.01.00; IR, Form 03.01.00; and Arrest Report, Form 05.02.00) shall be listed in the space provided on the upper left-hand corner of the SAR face sheet.

A. **Employee's Responsibilities.** Any Department employee receiving any information regarding suspicious activity and/or observing any suspicious activity shall investigate and take appropriate action, to include any tactical response or notifications to specialized entities.

Note: This section does not preclude, in any way, an employee taking immediate action during the commission of a criminal act or in circumstances which require the immediate defense of life, regardless of the nature of origin.

1. If the suspicious activity observed (e.g., suspicious behaviors or activities only) is not directly related to a reportable crime and/or any other type of investigation:

- * Record the information collected from the person reporting, or officer's observations on a SAR;
- * If the potential target of the activity can be identified (e.g., government, person, building/facility, infrastructure or protected site, or an official being surveilled), that location or individual shall be listed within the "Potential Target" section of the SAR. Otherwise, the "City of Los Angeles" shall be listed as the potential target;
- * List the person reporting within the "Witness" section of the SAR. If the person reporting refuses to identify themselves, list them as "Anonymous";
- * List any additional witnesses;
- * List the parties engaged in the suspicious behavior as Involved Persons within the "Involved Persons" portion of the SAR. With no reportable crime, they cannot be listed as suspects. Utilize page 2 of the SAR to include additional descriptive information;

- * Notify the watch commander, Area of occurrence. Upon approval by the watch commander, ensure that the Area Records Unit is made aware of the report and immediately assigns a DR and incident number for the SAR. Refer to the Area Records Unit's Responsibilities Note Section regarding manual DR numbers;
- * If there is property or evidence associated with the suspicious activity, a separate Property Report shall be completed. The Property Report shall bear a separate DR and incident number from the SAR, along with the following:
 - a. The Evidence box shall be marked;
 - b. The Investigative Unit box shall be Major Crimes Division (MCD);
 - c. The Connecting Reports box shall be marked "None";
 - d. In the narrative portion of the report, officers shall write, "Do not release or destroy prior to contacting MCD. Below listed property booked on advice from MCD";
- * The Property Report DR number shall be referenced in the "Prop Rpt DR#" box provided on the upper left-hand corner of the SAR face sheet;
- * The booked property and the Property Report shall remain in the division of occurrence;
- * Send the original SAR to Counter Terrorism and Special Operations Bureau (CTSOB)/MCD, Stop 400, as soon as practicable, but no later than 24 hours after the report is taken and faxed to MCD. No copies of the SAR shall be maintained at the Area.

Note: The SAR DR and incident numbers shall not be referenced in the Property Report or any other report.

2. If the suspicious activity observed is related to a criminal or other type of investigation (e.g., bomb threat, vandalism, trespass, assault, domestic violence, impound, narcotics, property report, etc.), officers shall complete the following:
- * Complete the investigation and any appropriate reports [e.g., IR; Arrest Report; Property Report; Vehicle Report, CHP 180 (impound) and/or any other related reports];
 - * Complete a SAR with a separate DR and incident number. Refer to the Area Records Unit's Responsibilities Note Section regarding manual DR numbers;
 - * Ensure that the DR number(s) of all completed crime, arrest, and/or property reports are listed and referenced in the appropriate boxes provided in the upper left-hand corner of the SAR face sheet. Include any additional information that provides the nexus to terrorism within the narrative of the SAR on page 2;
 - * Ensure that the SAR DR and incident numbers are not referenced in any other reports, e.g., crime, arrest, etc.;

Note: The physical disclosure of a SAR during criminal and/or civil discovery should only occur pursuant to a lawful court order.

- * Notify the watch commander, Area of occurrence. Upon approval by the watch commander, ensure that the Area Records Unit is made aware of the report. These reports shall be processed separately;
- * Notify MCD [contact Real-Time Analysis and Critical Response Division (RACR) for off-hours notification] if the report involves an arrest or a crime with follow-up potential; and,
- * Send the original SAR, including a copy of all associated reports, to CTSOB/MCD, Stop 400, as soon as practicable, but no later than 24 hours after the report is taken and faxed to MCD. No copies of the SAR shall be maintained at the Area.

Note: Employees may reference that a SAR was completed and indicate the SAR DR number only, and not the involved person's information in their Daily Field Activities Report (DFAR), Form 15.52.00, e.g., "A SAR report was completed, DR No. ___." The involved person's name(s) from the SAR shall not be documented on the aforementioned report or any other related reports, e.g., IR, Arrest, etc.

B. Watch Commander's Responsibilities. Upon notification that officers have received information regarding a suspicious activity, the watch commander shall:

- * Ensure that the information supports the completion of a SAR and that no greater law enforcement response or notifications to MCD are currently needed;
- * Review the SAR report for completeness; and,
- * Ensure that the Area Records Unit immediately assigns a DR number for the SAR, enters the information into the Consolidated Crime Analysis Database (CCAD) system, forwards the **original SAR**, including a **copy of all associated reports** to MCD, and faxes all reports to MCD no later than 24 hours after the report is taken. Refer to the **Area Records Unit's Responsibilities Note Section** regarding manual DR numbers.

Note: Supervisors and watch commanders may reference that a SAR was completed and indicate the SAR DR number only, and not the involved person's information in their Sergeant's Daily Report, Form 15.48.00, or Watch Commander's Daily Report, Form 15.80.00, e.g., "SAR report completed, DR No. ___." The involved person's name(s) from the SAR shall not be documented on the aforementioned reports or any other related reports, e.g., IR, Arrest, etc.

C. Major Crimes Division's Responsibilities. Upon receiving a telephonic notification of a suspicious activity, MCD personnel shall, when appropriate, conduct immediate debriefs of arrestees, and/or witnesses, and provide the appropriate guidance to patrol officers.

Upon receiving a SAR which has been forwarded and faxed to MCD, assigned MCD personnel shall follow established protocols regarding the processing of such information. Refer to the Area Record Unit's Responsibilities Note Section regarding manual DR numbers and MCD's responsibilities in reference to this.

D. **Area Records Unit's Responsibilities.** Upon receipt of the original SAR and associated reports (e.g., Property Report, IR, and/or Arrest Report, etc.) records personnel shall:

- * Assign DR number(s) for the SAR reports and other related reports, as appropriate;

Note: If unable to obtain a DR number, DO NOT obtain a manual DR number for the SAR and do not keep a copy of the SAR. Forward the original SAR to the SAR Unit, Major Crimes Division, Stop 400 and fax it to MCD. The SAR Unit personnel will obtain the required DR number and incident number. If an arrest is involved, MCD will notify the Area of a manual SAR DR number.

- * Ensure that the DR number(s) of all associated reports (crime, arrest, property, and/or impound report, etc.) are listed in the appropriate boxes provided on the face sheet of the SAR;
- * Enter the information into the CCAD system, including any appropriate CTSOB-related codes; and,
- * Send the original SAR, including a copy of all associated reports, to CTSOB/MCD, Stop 400, as soon as practicable, but no later than 24 hours after the report is taken and faxed to MCD. No copies of the SAR shall be maintained at the Area.

E. **Area Detective's Responsibilities.** Upon receipt of a SAR and any associated reports, (e.g. Property Report, IR, and/or Arrest Report, etc.), which arrive at an Area Detective Division without having been reviewed by MCD personnel, Area detectives shall:

- * Immediately notify MCD and forward the SAR to MCD (No copies of the SAR shall be retained at the Area) and fax copies of the SAR and all reports to MCD. Refer to the Area Records Unit's Responsibilities Note Section regarding manual DR numbers;

- * Ensure the SAR has been screened by MCD personnel;
and,
- * Complete any criminal investigation per existing
Department policies and guidelines.

III. SUSPICIOUS ACTIVITY REPORT, FORM 03.24.00 - ACTIVATED.
The Suspicious Activity Report, Form 03.24.00, is
activated.

- A. Use of Form. The SAR is a STAND-ALONE REPORT and is
to be used when reporting all acts of suspicious
activities as defined in Section I. A. above.
- B. Completion. This form shall be completed by ANY
sworn Department employee either observing or
receiving information of a suspicious activity.
- C. Distribution.
 - 1 - Original, Commanding Officer, MCD.
 - 1 - TOTAL

IV. INVESTIGATIVE REPORT, FORM 03.01.00 - REVISED. The
Investigative Report, Form 03.01.00, has been revised to
delete the checkbox indicating "Suspicious Activity" on
its face sheet. The IR shall no longer be used to report
any act of suspicious activity.

The completion and distribution of this form remain
unchanged.

V. SUSPICIOUS ACTIVITY REPORT NOTEBOOK DIVIDER,
FORM 18.30.03 - REVISED. The SAR Notebook Divider has
been revised accordingly.

FORM AVAILABILITY: The SAR, the SAR Notebook Divider, and the
revised IR, are available in LAPD E-Forms on the Department's
Local Area Network (LAN). The previous version of the printed
IR form is still valid and can be used until the current stock is
depleted; however, it should not be used for reporting suspicious
activity. The revised IR form and the new SAR will be available
for ordering from the Department of General Services,
Distribution Center, in four weeks. All other versions of the
SAR Notebook Divider shall be marked "obsolete" and placed into
the divisional recycling bin. The copies of all three forms are
attached for immediate use and duplication.

January 2, 2012

AMENDMENTS: This Order amends Section 4/271.46 of the Department Manual, activates the SAR, revises the SAR Notebook Divider, and revises the IR. The "Form Use Link" applicable to the SAR is accessible in Volume V of the Department Manual.

MONITORING RESPONSIBILITY: The Commanding Officer, Major Crimes Division, shall have monitoring responsibility for this directive.

AUDIT RESPONSIBILITY: The Commanding Officer, Internal Audits and Inspections Division, shall review this directive and determine whether an audit or inspection shall be conducted in accordance with Department Manual Section 0/080.30.



CHARLIE BECK
Chief of Police

Attachments

DISTRIBUTION "D"

SUSPICIOUS ACTIVITY REPORT

These guidelines should be followed for investigations of Suspicious Activity.

DEFINITIONS:

SUSPICIOUS ACTIVITY

A Suspicious Activity is any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism.

SUSPICIOUS ACTIVITY REPORT

A Suspicious Activity Report (SAR) is a stand-alone report used to document any reported or observed behavior/activity that may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may result from observations or investigations by police officers, or may be reported to them by private sources. A SAR will generally consist of the completion of a SAR, Form 03.24.00.

Note: A SAR shall only be completed for those activities and behaviors specifically listed or defined under "reportable suspicious activities."

INVOLVED PERSON

An involved person (IP) is an individual that has been observed engaging in suspicious activity when no definitive criminal activity can be identified, thus precluding their identification as a suspect.

POTENTIAL TARGET

A potential target is a person, facility/building, infrastructure or protected site that is or may be the object of the suspicious activity.

EMPLOYEE'S REPORTING RESPONSIBILITIES

Any Department employee receiving any information regarding suspicious activity and/or observing any suspicious activity shall investigate and take appropriate action, to include any tactical response or notifications to specialized entities.

I. If the suspicious activity observed (e.g., suspicious behaviors or activities only) is not directly related to a reportable crime and/or any other type of investigation:

- Record the information collected from the person reporting, or officer's observations on a SAR, Form 03.24.00;
- If the potential target of the activity can be identified (e.g., government, person, building/facility, infrastructure or protected site, or an official being surveilled), that location or individual shall be listed within the "Potential Target" section of the SAR. Otherwise the "City of Los Angeles" shall be listed as the potential target;
- List the person reporting within the "Witness" section of the SAR. If the person reporting refuses to identify themselves, list them as "Anonymous";
- List any additional witnesses;
- List the parties engaged in the suspicious behavior as Involved Persons within the "Involved Persons" portion of the SAR. **With no reportable crime, they cannot be listed as suspects.** Utilize page 2 of the SAR to include additional descriptive information;
- Notify the watch commander, Area of occurrence. Upon approval by the watch commander, ensure that the Area Records Unit is made aware of the report and immediately assigns a DR and incident number for the SAR. **Refer to the Area Records Unit's Responsibilities Note Section regarding manual DR numbers:**
- If there is a property or evidence associated with the suspicious activity, **a separate Property Report shall be completed. The Property Report shall bear a separate DR and incident number from the SAR, along with the following:**

- a. The Evidence box shall be marked;
- b. The Investigative Unit box shall be Major Crimes Division (MCD);
- c. The Connecting Reports box shall be marked "None";
- d. In the narrative portion of the report, officers shall write, "Do not release or destroy prior to contacting MCD. Below listed property booked on advice from MCD";

- The Property Report DR number shall be referenced in the "Prop Rpt DR#" box provided on the upper left-hand corner of the SAR face sheet;
- The booked property and the Property Report shall remain in the division of occurrence;
- Send the original SAR to Counter Terrorism and Special Operations Bureau (CTSOB)/MCD, Stop 400, as soon as practicable, but no later than 24 hours after the report is taken and faxed to MCD. **No copies of the SAR shall be maintained at the Area.**

Note: The SAR DR and incident numbers shall not be referenced in the Property Report or any other report.

II. If the suspicious activity observed is related to a criminal or other type of investigation (e.g., bomb threat, vandalism, trespass, assault, domestic violence, impound, narcotics, property report, etc.), officers shall complete the following:

- Complete the investigation and any appropriate reports [e.g., IR; Arrest Report; Property Report; Vehicle Report, CHP 180 (impound) and/or any other related reports];
- Complete a SAR with a separate DR and incident number. Refer to the Area Records Unit's Responsibilities Note Section regarding manual DR numbers;
- Ensure that the DR number(s) of all completed crime, arrest, and/or property reports are listed and referenced in the appropriate boxes provided in the upper left-hand corner of the SAR face sheet. Include any additional information that provides the nexus to terrorism within the narrative of the SAR on page 2;
- Ensure that the SAR DR and incident numbers are not referenced in any other reports, e.g., crime, arrest, etc.;

Note: The physical disclosure of a SAR during criminal and or civil discovery should only occur pursuant to a lawful court order.

- Notify the watch commander, Area of occurrence. Upon approval by the watch commander, ensure that the Area Records Unit is made aware of the report. **These reports shall be processed separately:**
- Notify MCD [contact Real-Time Analysis and Critical Response (RACR) Division for off-hours notification] if the report involves an arrest or a crime with follow-up potential; and,
- Send the original SAR, including a copy of all associated reports, to CTSOB/MCD, Stop 400, as soon as practicable, but no later than 24 hours after the report is taken and faxed to MCD. **No copies of the SAR shall be maintained at the Area.**

Note: Employees may reference that a SAR was completed and indicate the SAR DR number only and not the involved person's information in their Daily Field Activities Report (DFAR), Form 15.52.00, e.g., "A SAR report was completed, DR No. ___." The involved person's name(s) from the SAR shall not be documented on the aforementioned report, or any other related reports, e.g., IR, Arrest, etc.

SUSPICIOUS ACTIVITY REPORT

These guidelines should be followed for investigations of Suspicious Activity.

SUPERVISORS & WATCH COMMANDERS may reference that a SAR was completed and indicate the SAR DR number only, and not the involved person's information in their Sergeant's Daily Report, Form 15.48.00, or Watch Commander's Report, Form 15.80.00, e.g., "SAR Report completed, DR No: ___." The involved person's name(s) from the SAR shall not be documented on the aforementioned reports, or any other related reports, e.g., IR, Arrest, etc. **Please refer to Department Manual Section 4/271.46 for the supervisor's and watch commander's responsibilities.**

NOTIFICATIONS:

Notify CTSOB/MCD (contact RACR Division for off-hours notification) for guidance if the report involves any incident of significance, an arrest or a crime with any follow-up potential.

POLICY STATEMENT:

It is the policy of the Los Angeles Police Department to make every effort to accurately and appropriately gather, record and analyze information of a criminal or non-criminal nature that could indicate activities or intentions related to either foreign or domestic terrorism, in a manner that protects the information, privacy and legal rights of Americans.

REPORTABLE SUSPICIOUS ACTIVITIES:

A suspicious activity reported on a SAR shall only include the following:

- **Breach/Attempted Intrusion.** Unauthorized individuals attempting to or actually entering a facility/infrastructure or protected site;
- **Misrepresentation.** Presenting false or misusing insignia, documents, and/or identification to misrepresent one's affiliation to cover possible illicit activity. Impersonation of any authorized personnel (e.g., police, security, or janitor);
- **Theft/Loss/Diversion.** Stealing or diverting (obtaining or acquiring) something associated with a facility/infrastructure [e.g., badges, uniforms, identification, emergency vehicles, technology or documents (classified or unclassified), which are proprietary to the facility];
- **Sabotage/Tampering/Vandalism.** Damaging, manipulating, or defacing part of a facility/infrastructure or protected site;
- **Cyber Attack.** Compromising or attempting to compromise or disrupt an organization's information technology infrastructure;
- **Expressed or Implied Threat.** Communicating a spoken or written threat to damage or compromise a facility/infrastructure, protected site, and cyber attacks;
- **Aviation Activity.** Operation or attempted operation of an aircraft in a manner that reasonably may be interpreted as suspicious or posing a threat to people, buildings/facilities, infrastructures, or protected sites. Such operation may or may not be a violation of Federal Aviation Administration regulations;
- **Eliciting Information:** Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person;
- **Testing or Probing of Security:** Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel or cyber security capabilities;
- **Recruiting:** Building of operations teams and contacts, personal data, banking data or travel data;
- **Photography:** Taking pictures or videos of facilities/buildings, infrastructures, or protected sites in a manner that would arouse suspicion in a reasonable person.

Examples include taking pictures or videos of ingress/egress, delivery locations, personnel performing security functions (e.g., patrol, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.;

- **Observation/Surveillance:** Demonstrating unusual interest in facilities/buildings, infrastructures or protected sites beyond mere casual or professional (e.g., engineers) interest, such that a reasonable person would consider the activity suspicious. Examples include observations through binoculars, taking notes, attempting to measure distances, etc.;
- **Materials Acquisition/Storage:** Acquisition and/or storage of unusual quantities of materials, such as cell phones, pagers, fuel, chemicals, toxic materials, and timers, such that a reasonable person would consider the activity suspicious;
- **Acquisition of Expertise:** Attempts to obtain or conduct training in security concepts; military weapons or tactics; or other unusual capabilities such that a reasonable person could consider the activity suspicious;
- **Weapons Discovery:** Discovery of unusual amounts of weapons, explosives, or their components that would arouse suspicion in a reasonable person; or,
- **Sector-Specific Incident:** Actions associated with a characteristic of unique concern to specific sectors (such as the public health sector) with regard to their personnel, facilities, systems or functions.

Note: These activities may be constitutionally-protected activities and should therefore not be reported in a SAR, absent articulable facts and circumstances that support the source's suspicion that the behavior observed is not innocent, but rather reasonably indicative of suspicious activity associated with terrorism. Race, color, religion, national origin, gender, age, physical or mental disability, marital status, sexual orientation, gender identity, gender expression, creed, ancestry, or medical condition shall not be considered as factors that create suspicion, although these factors may be used as specific-involved person descriptors.

SOURCE: Special Order No. 1, 2012/Department Manual Section 4/271.46, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism.*

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 11

March 5, 2008

SUBJECT: REPORTING INCIDENTS POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM

PURPOSE: Current anti-terrorism philosophy embraces the concept that America's 800,000 law enforcement officers fill a critical position in the area of terrorism prevention. Law enforcement authorities must carry out their counter-terrorism responsibilities within the broader context of their core mission of providing emergency and non-emergency services in order to prevent crime, violence and disorder. In support of this, the Department's Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) is engaging in an effort to more thoroughly gather, analyze and disseminate information and observations, of either a criminal or suspicious nature, which may prove critical to the intelligence cycle.

This Order establishes Department policy for investigating and reporting crimes and non-criminal incidents that represent indicators of potential foreign or domestic terrorism, and incorporates within the Department Manual a procedure for gathering and maintaining information contained in such reports.

POLICY: It is the policy of the Los Angeles Police Department to make every effort to accurately and appropriately gather, record and analyze information, of a criminal or non-criminal nature, that could indicate activity or intentions related to either foreign or domestic terrorism. These efforts shall be carried out in a manner that protects the information privacy and legal rights of Americans, and therefore such information shall be recorded and maintained in strict compliance with existing federal, state and Department guidelines regarding Criminal Intelligence Systems (28 Code of Federal Regulations (CFR), Part 23 and applicable California State Guidelines).

PROCEDURE:

I. DEFINITIONS.

- A. Suspicious Activity Report.** A Suspicious Activity Report (SAR) is a report used to document any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result

of observations or investigations by police officers, or may be reported to them by private parties.

Incidents which shall be reported on a SAR are as follows:

- * Engages in suspected pre-operational surveillance (uses binoculars or cameras, takes measurements, draws diagrams, etc.)
- * Appears to engage in counter-surveillance efforts (doubles back, changes appearance, evasive driving, etc.);
- * Engages security personnel in questions focusing on sensitive subjects (security information, hours of operation, shift changes, what security cameras film, etc.);
- * Takes measurements (counts footsteps, measures building entrances or perimeters, distances between security locations, distances between cameras, etc.);
- * Takes pictures or video footage (with no apparent esthetic value, i.e. camera angles, security equipment, security personnel, traffic lights, building entrances, etc.);
- * Draws diagrams or takes notes (building plans, location of security cameras or security personnel, security shift changes, notes of weak security points, etc.);
- * Abandons suspicious package or item (suitcase, backpack, bag, box, package, etc.);
- * Abandons vehicle (in a secured or restricted location i.e. the front of a government building, airport, sports venue, etc.);
- * Attempts to enter secured or sensitive premises or area without authorization (i.e. "official personnel," closed off areas of airport, harbor, secured areas at significant events such as appearances by politicians, etc);
- * Engages in test of existing security measures (i.e. "dry run", security breach of perimeter fencing, security doors, etc., creating false alarms in order to observe reactions, etc.);
- * Attempts to smuggle contraband through access control point (airport screening centers,

- security entrance points at courts of law, sports games, entertainment venues, etc.);
- * Makes or attempts to make suspicious purchases, such as large amounts of otherwise legal materials (i.e. pool chemicals, fuel, fertilizer, potential explosive device components, etc);
 - * Attempts to acquire sensitive or restricted items or information (plans, schedules, passwords, etc);
 - * Attempts to acquire illegal or illicit explosives or precursor agents;
 - * Attempts to acquire illegal or illicit chemical agent (nerve agent, blood agent, blister agent, etc.);
 - * Attempts to acquire illegal or illicit biological agent (anthrax, ricin, Ebola, small pox, etc.);
 - * Attempts to acquire illegal or illicit radiological material (uranium, plutonium, hospital x-ray discards, etc.);
 - * In possession, or utilizes, explosives (for illegal purposes);
 - * In possession, or utilizes, chemical agent (for illegal purposes, i.e. dry ice bomb, chlorine, phosgene, WMD attack, etc);
 - * In possession, or utilizes, biological agent (for illegal purposes, i.e. terrorist device, WMD or a tool of terrorism, etc.);
 - * In possession, or utilizes, radiological material (for illegal purposes, i.e. as a weapon, etc.);
 - * Acquires or attempts to acquire uniforms without a legitimate cause (Service personnel, government uniforms, etc);
 - * Acquires or attempts to acquire official or official-appearing vehicle without a legitimate cause (i.e. emergency or government vehicle, etc.);
 - * Pursues specific training or education which indicate suspicious motives (flight training, weapons training, etc);
 - * Stockpiles unexplained large amounts of currency;
 - * In possession of multiple passports, identifications or travel documents issued to the same person;
 - * Espouses extremist views (verbalizes support of terrorism, incites or recruits others to engage in terrorist activity, etc.);

- * Brags about affiliation or membership with extremist organization ("white power", militias, KKK, etc.);
- * Engages in suspected coded conversations or transmissions (i.e. email, radio, telephone, etc., i.e. information found during a private business audit is reported to police);
- * Displays overt support of known terrorist networks (posters of terrorist leaders, etc.);
- * Utilizes, or is in possession of, hoax/facsimile explosive device;
- * Utilizes, or is in possession of, hoax/facsimile dispersal device;
- * In possession of, or solicits, sensitive event schedules (i.e. Staples Center, Convention Center);
- * In possession of, or solicits, VIP Appearance or Travel Schedules;
- * In possession of, or solicits, security schedules;
- * In possession of, or solicits, blueprints to sensitive locations;
- * In possession of, or solicits, evacuation plans;
- * In possession of, or solicits, security plans;
- * In possession of, or solicits, weapons or ammunition;
- * In possession of, or solicits, other sensitive materials (passwords, access codes, secret government information, etc.); and,
- * In possession of coded or ciphered literature or correspondence.

B. **Involved Party (IP).** An involved party (IP) is an individual that has been observed engaging in suspicious activity of this nature, when no definitive criminal activity can be identified, thus precluding their identification as a suspect.

II. REPORTING AND INVESTIGATING.

A. **Employees - Responsibilities.** Any Department employee receiving any information regarding suspicious activity of this nature shall:

- * Investigate and take appropriate action, to include any tactical response or notifications to specialized entities.

Note: This section does not preclude, in any way, an employee taking immediate action during the commission of a criminal act, or in circumstances which require the immediate defense of life, regardless of the nature or origin.

- * If the activity observed is not directly related to a reportable crime, officers shall record the information collected from the person reporting, or their own observations, on an Investigative Report (IR), Form 03.01.00, titled "Suspicious Activity" in accordance with the following guidelines:
 - * If the person reporting (R) is willing to be contacted by investigators, they shall be listed within the Involved Persons portion of the IR. Officers shall consider utilizing a "Request for Confidentiality of Information," Form 03.02.00, to ensure confidentiality. If absolutely necessary, officers can enter "Anonymous" for person reporting. Any desire by a person reporting to remain anonymous does not exempt officers from the requirement to complete an IR.
 - * If the potential target of the activity can be identified, such as a government building or official being surveilled, that location or individual shall be listed within the "Victim" portion of the IR. Otherwise the "City of Los Angeles" shall be listed as the victim.
 - * If the information includes an involved party(IP), officers shall identify or fully describe IPs within the narrative (page 2) of their report, along with any vehicle descriptions or other pertinent information.

- * If the information is related to a regular criminal investigation (such as a bomb threat, criminal threats, trespassing, etc.), the officers shall complete the criminal investigation, make any appropriate arrests and complete any related reports. The officers shall include any additional information that provides the nexus to terrorism within the narrative of the crime or arrest report.
- * Should officers come across information that indicates possible terrorism-related activity while investigating an unrelated crime or incident (e.g., such as officers conducting a domestic violence investigation observe possible surveillance photographs and a map of the region surrounding a government facility), or should they conduct an impound or found property investigation which is suspicious in nature, the officers shall make no mention of this potential terrorism-related material or activity within the impound, property, crime or arrest report. Under these circumstances, the officers shall complete a separate SAR in addition to the crime or arrest report, and shall note the criminal investigation, impound or found property investigation as their source of their activity.
- * Officers shall note on the left margin of any arrest facesheet or IR that the report is to be sent to CTCIB, Major Crimes Division.

Note: The Investigative Report is currently being revised to include "SAR" and "Original to CTCIB, Major Crimes Division" boxes to be checked when appropriate. The revised IR will also include additional entries for involved parties and involved vehicles.

- * Notify Major Crimes Division (contact Real-Time Analysis and Critical Response [RACR] Division for off hours notification) for guidance or if the report involves an arrest or a crime with follow-up potential.
- * Notify the Watch Commander, Area of occurrence.

- * Upon approval by the Watch Commander, ensure the Area Records Unit is made aware of the report, immediately assigns a DR number and forwards the original report to MCD.

Note: Nothing in this Order alters existing policies regarding notifications to required specialized units such as Bomb Squad, Hazardous Materials Unit, Criminal Conspiracy Section or RACR Division.

- B. **Hazardous Materials and Devices Section, Emergency Services Division - Responsibility.** Personnel assigned to the Bomb Squad, Hazardous Materials/ Environmental Crimes, or Airport K-9 Bomb Detection Unit shall ensure that a SAR is completed on all incidents on which they respond where a potential nexus to terrorism exists. Suspicious Activity Reports completed by personnel assigned to these units shall be processed through a geographic Area Records Unit as directed below.
- C. **Watch Commanders - Responsibilities.** Upon notification that officers have received information regarding suspicious activity, the Watch Commander shall:
 - * Ensure the information supports the completion of a SAR report and that no greater law enforcement response or notifications to MCD are currently needed;
 - * Review the report for completeness; and,
 - * Ensure the Area Records Unit immediately assigns a DR Number and forwards the original report to MCD.
- D. **Major Crimes Division - Responsibility.** Upon receiving a telephonic notification of suspicious activity, MCD personnel shall, when appropriate, conduct immediate debriefs of arrestees, or provide the appropriate guidance to patrol officers. Upon receiving a SAR report forwarded to MCD, assigned personnel shall follow established protocols regarding the processing of such information.

E. **Records Personnel - Responsibilities.** Upon receipt of a SAR-related incident, crime or arrest report, records personnel shall:

- * Enter the information into the CCAD system, including any appropriate CTCIB-related codes; and,
- * Send the original report to "CTCIB/Major Crimes Division, Stop 1012" as soon as practicable, but no later than 24 hours after the report is taken. No copies of the report shall be maintained at the Area.

F. **Area Detectives Personnel - Responsibilities.** Upon receipt of a SAR-related crime or arrest report Area detectives shall:

- * Ensure the report has been screened by MCD personnel and referred back to the geographic Area for investigation; and,
- * Complete the investigation per normal policies and guidelines.

Note: If the report is a SAR-related incident only, or a crime or arrest report which arrives at an Area Detective Division without having been reviewed by MCD personnel, Area detectives shall immediately forward the report to MCD (no copies shall be retained at the Area).

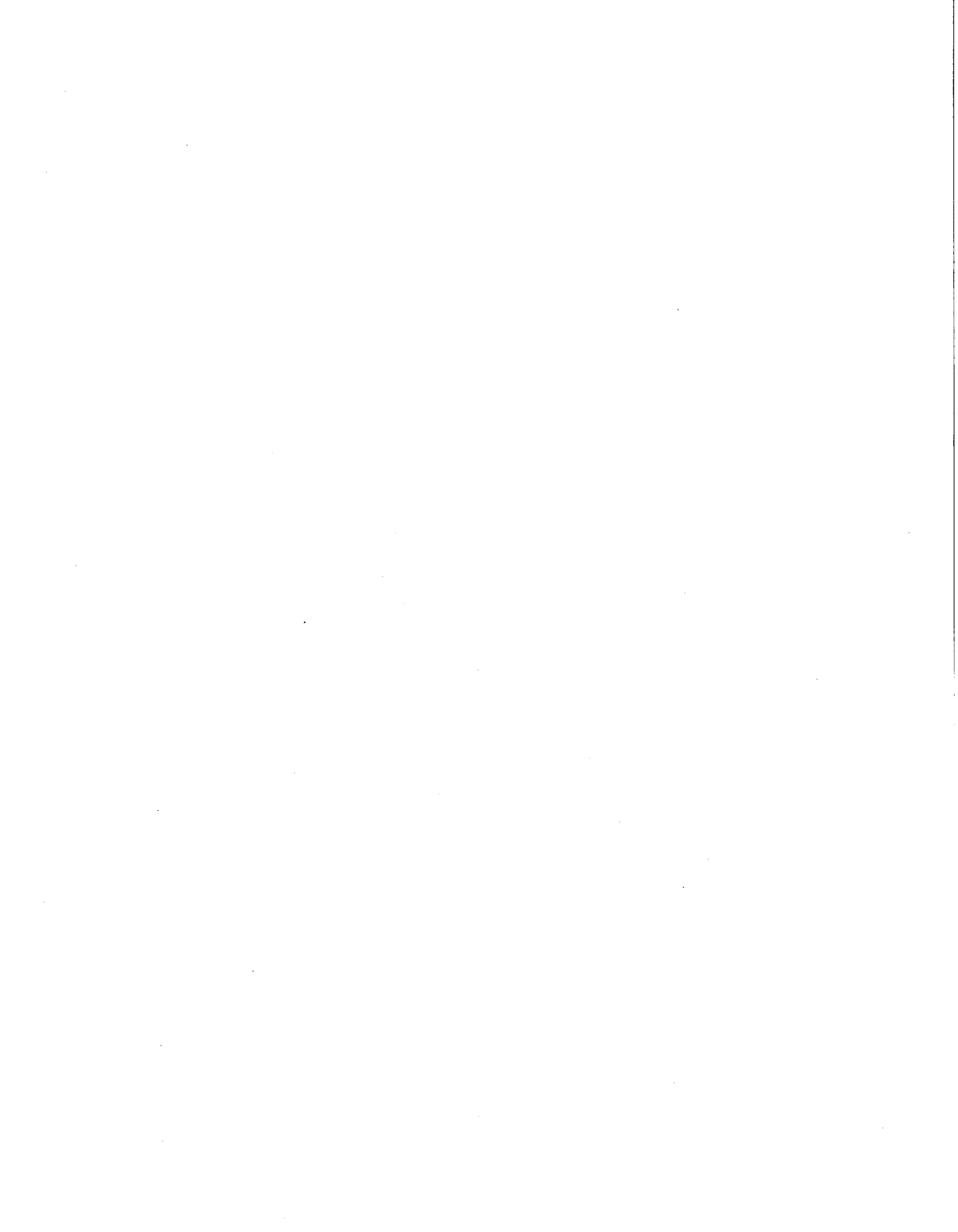
G. **Counter-Terrorism and Criminal Intelligence Bureau - Responsibility.** Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) is responsible for providing Department personnel with training pertaining to the proper handling of suspected terrorism-related activity and ensuring adherence to the guidelines established regarding developmental information and intelligence systems.

AMENDMENTS: This Order adds section 4/271.46 to the Department Manual.

AUDIT RESPONSIBILITY: The Commanding Officer, Counter Terrorism and Criminal Intelligence Bureau, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30 and shall ensure that all information is collected and maintained in strict compliance with existing federal, State and Department guidelines regarding Criminal Intelligence Systems (28 C.F.R., Part 23 and applicable California State Guidelines).

WILLIAM J. BRATTON
Chief of Police

DISTRIBUTION "D"



OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 26

June 8, 2009

SUBJECT: TERRORISM LIAISON OFFICER PROGRAM - REVISED

PURPOSE: The Terrorism Liaison Officer (TLO) Program has been revised to allow Area/division commanding officers more flexibility in designating Area/division TLOs.

PROCEDURE: The commanding officer of each geographic area and specialized divisions shall designate a minimum of two, and a maximum of five TLOs to represent and disseminate information to their respective divisions.

NOTE: The commanding officers shall assign their training coordinators and senior lead officer (SLO) supervisors as TLOs. It is recommended the remaining TLOs be assigned based on their familiarization with intelligence, the intelligence cycle and the concept of intelligence oversight. The remaining TLOs should be assigned irrespective of rank and should possess good communication skills. It is recommended that a TLO be assigned from detectives, patrol and/or specialized units within the division to facilitate the flow of information to their respective entities.

I. TERRORISM LIAISON OFFICER'S RESPONSIBILITIES.

The TLO shall be responsible for the following:

- * Acting as a point of contact with Major Crimes Division (MCD);
- * Be familiar with reporting of possible terrorist activity as outlined in Special Order No. 11, 2008, *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism*, as well as www.tlo.org, which is a direct link for officers and civilians alike to report suspicious activity in their area;
- * Relaying advisories and other terrorism related information provided by MCD, and the Joint Regional Intelligence Center (JRIC) to Area/division personnel in the form of roll call training at a minimum of once every two weeks, preferably on rotating watches;
- * In the event of real-time transmission of threat information, utilizing Department communications technologies (ACC, MDC, ASTRO, etc.) to disseminate the information as deemed appropriate;
- * Informing MCD of TLO personnel changes;
- * Attending periodic coordination and training meetings; and,

- * Terrorism Liaison Officers shall attend the California Commission on Peace Officer Standards and Training (POST) certified TLO Basic Course no later than six months after being assigned as a TLO. Currently the training consists of a no cost 8-hour block of instruction. The TLOs shall coordinate with MCD or JRIC to arrange this training.

Note: It is important to remember that TLOs are not considered intelligence and/or terrorism experts; they are to be trained in terrorism awareness and the proper procedure for reporting the information to MCD and their division. Additionally, they shall be required to be recertified on an annual basis or as prescribed by statute.

Terrorism Liaison Officers are not responsible for collecting and disseminating information to the public regarding terrorism related activity. However, once TLOs receive terrorism related information from MCD or JRIC, they shall notify the Area/division command staff, and as directed, to Area/division personnel, so they may relay pertinent information to officers and/or the community, as appropriate.

II. AREA/DIVISION COMMANDING OFFICER'S RESPONSIBILITIES.

A. The commanding officer of each Area shall:

- * Designate two to five sworn employees as TLOs to represent their respective Area. One of the TLOs shall be the Area training coordinator. The other TLO shall be the SLO supervisor. The remaining TLO positions shall be assigned at the commanding officer's discretion, irrespective of rank;
- * Ensure that each TLO is properly coordinating with the MCD Terrorism Liaison Section on terrorism-related issues;
- * Ensure that each TLO is properly coordinating with the JRIC on regional terrorism-related issues;
- * Ensure an Interdepartmental Correspondence, Form 15.02.00, be generated from the Area/division commanding officer to the Commanding Officer, MCD, designating the respective Area/division assigned TLOs;

- * Ensure the TLOs attend the POST certified TLO Basic course within six months of being designated as a TLO; and,
- * Monitor the regular JRIC informational products in regard to terrorism and homeland security issues that may affect their jurisdiction.

Note: Commanding officers may consider that officers in their command may have experience, knowledge and/or military experience who may be suitable for the TLO position.

B. The commanding officer of each specialized division shall:

- * Designate two to five employees as the TLOs representing their respective division. One TLO shall be the training coordinator. The chosen TLOs shall have overall knowledge of the terrorist issues related to the division;
- * Ensure that each TLO is properly coordinating with the MCD Terrorism Liaison Section on terrorism-related issues;
- * Ensure that each TLO is properly coordinating with the JRIC on regional terrorism-related issues;
- * Ensure an Interdepartmental Correspondence be generated from the Area/division commanding officer to the Commanding Officer, MCD, designating the respective Area/divisions assigned TLOs;
- * Ensure that the TLOs attend the POST-certified TLO Basic Course within six months of being designated as a TLO; and,
- * Monitor the regular JRIC informational products in regard to terrorism and homeland security issues that may affect their jurisdiction.

Note: Specialized divisions include, but are not limited to, the four bureau traffic divisions; Scientific Investigation Division; Hiring and Evaluation Section of Personnel Group; specialized detective divisions from Detective Bureau (Gang Operations and Support Division); and Special Operations Bureau (i.e., Air Support Division, and Metropolitan Division).

III. MAJOR CRIMES DIVISION RESPONSIBILITIES. Major Crimes Division is responsible for the following:

- * Authorizing terrorism-related advisories, alerts and warnings;
- * Maintaining a liaison with the Area/division TLOs;
- * Coordinating regular information-sharing meetings and training for TLOs; and,
- * Acting as a conduit for information provided by the TLOs to the JRIC.

Note: The Los Angeles JRIC is staffed by representatives from several federal, state and local agencies, functions as the fusion center for terrorism intelligence, analysis, and leads the intake for the Federal Bureau of Investigations Los Angeles field office area. This area covers the counties of Los Angeles, Orange, Riverside, San Bernardino, San Luis Obispo, Santa Barbara, and Ventura. The Joint Regional Intelligence Center also serves as the Los Angeles Regional Terrorism Threat Assessment Center (LA-RTTAC) for the State of California. The Joint Regional Intelligence Center TLO Coordination Branch is staffed full-time with sworn federal and local law enforcement personnel, and representatives from each of the TLO disciplines. Its mission is to provide coordination and support to TLOs throughout the region, as well as building and maintaining a cohesive, well-trained team that enhances our ability to detect, deter, and defend against terrorism.

In addition, MCD shall act as an intake center for the following:

- * Information pertaining to possible terrorism or terrorism related activity; and,
- * Dignitary security issues.

IV. MAJOR CRIMES DIVISION COMMANDING OFFICER'S RESPONSIBILITY. The Commanding Officer, MCD, is designated as the Department's TLO Program Coordinator.

- * The Department TLO Program Coordinator shall exercise Citywide oversight on Area/division TLOs; and,
- * Ensure that effective communication is maintained between all TLOs and MCD.

AMENDMENTS: This Order amends Department Manual Sections 2/295.17 and 4/271.45.

AUDIT RESPONSIBILITY: The Commanding Officer, Internal Audits and Inspections Division, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30.



WILLIAM J. BRATTON
Chief of Police

DISTRIBUTION "D"



Memorandum of Understanding

**Los Angeles
Joint Regional Intelligence Center**

Copy

LOS ANGELES JOINT REGIONAL INTELLIGENCE CENTER

MEMORANDUM OF UNDERSTANDING

THIS MEMORANDUM OF UNDERSTANDING (MOU), made and entered into this 14th day of April, 2009 by and between the Los Angeles Joint Regional Intelligence Center (JRIC) Executive Committee which consists of an Special Agent in Charge, Federal Bureau of Investigation (FBI), a Deputy Chief of the Los Angeles Police Department (LAPD) and a Commander from the Los Angeles Sheriff's Department (LASD), herein referred to as "JRIC", a federal-state-local law enforcement collaborative, and the State of California, Department of Justice, Division of Law Enforcement, a public entity, herein after referred to as "Agency," collectively referred to as "Parties," and

WHEREAS, the Parties provide Public Safety services within their jurisdictions; and

WHEREAS, the Parties have found it to be of mutual benefit to provide for the most efficient utilization of their resources and services in the application to Public Safety efforts within their jurisdictions; and

WHEREAS, the Parties are committed to complete cooperation and coordination in providing the highest level of Public Safety services to the public, guided by the principle that performing cooperatively is in the best interest of the public; and

NOW, THEREFORE, for and in consideration of the covenants contained herein, the parties hereby agree as follows:

1. PURPOSE:

The purpose of this MOU is to provide for the administration of a grant that was awarded to establish the Los Angeles Joint Regional Intelligence Center (JRIC), which will provide a local and coordinated approach to addressing the complex problem of terrorism affecting the State of California and the United States of America; including the staffing arrangements for those public entities contribution of human resources to work in the JRIC.

2. MISSION AND OBJECTIVES:

The JRIC will focus primarily on International and Domestic terrorism matters, and will facilitate interagency planning, manage information resources, and function as an operational resource for incident commanders in the areas of technical expertise and decision alternatives. The JRIC will function as an information gathering, fusion, dissemination and advisory group and its recommendations will not be binding on any of the Parties.

3. ORGANIZATION, STRUCTURE AND DIRECTION:

- a. Agency has agreed to support the efforts and philosophy of the JRIC. In addition, Agency may decide to assign one or more members of its staff to the JRIC, for the purpose of executing JRIC activities and functions.
- b. The JRIC will operate with the organizational structure of the Executive Director being a representative from the FBI and the Section Manager being a representative from LASD. This organization has been determined to be consistent with the JRIC grant and the JRIC Executive Committee regulatory framework. Responsibility for overall policy and direction of the JRIC will rest with the JRIC Executive Committee through its designee, the JRIC Executive Director. Decisions on matters of mutual concern to all Parties, relating to such policy and direction, will be reported in a timely fashion at the bi-monthly JRIC Executive Committee meetings.
- c. The number of staff the Agency details to the JRIC and the authority to assign general tasks to agency's employees, within the mission and objectives of the JRIC, will be retained by Agency.
- d. Day-to-day operations of the JRIC will be the responsibility of the JRIC Executive Director.

4. MOU CHANGES:

Any changes and additions to the MOU shall be made by written amendments to this MOU, and shall not be effective until approved in writing by the Parties. Annually, or more frequently as requested by the Parties, a joint review of this MOU shall occur to identify needed changes, which may be amended by written mutual agreement of the Parties.

5. PHYSICAL LOCATION AND SUPPORT:

The FBI will arrange for and provide office space and basic office equipment, such as facsimile and photocopy machines, automation and technical support, for daily operations of the JRIC.

6. EQUIPMENT:

Safety equipment for all peace officers assigned to the JRIC will be provided by each of the Parties to their respective employee(s).

7. PERSONNEL COMMITMENTS:

Agency will assign staff to fulfill the mission of the JRIC, and continued personnel assignments will be made at the discretion of the respective Parties. Responsibility for the conduct of the personnel assigned to the JRIC will remain with their respective agency heads. All JRIC personnel will keep their respective superiors completely informed of pertinent

developments. Agency will retain responsibility for evaluating and disciplining its own personnel while assigned to the JRIC. The Executive Director of the JRIC, or his/her designee, may, at his/her sole discretion and without cause, request the employing agency to remove its personnel from the JRIC, and in that case, Agency will comply.

8. MEDIA RELATIONS:

The JRIC as an entity will not respond to, nor issue, information or statements to the media. Inquires or information for public release will be referred to the respective agency that has jurisdiction over the matter. Matters of concern to multiple agencies will be handled externally by the JRIC utilizing existing relationships between participating agencies. Any media releases regarding the mission or operations of the JRIC will generally require prior approval of the department heads of the Parties.

9. RECORDS AND REPORTS:

All JRIC records generated by those assigned to the JRIC will be maintained at the JRIC office, if they are not otherwise disseminated. Dissemination of any information from the JRIC will be done only in compliance with applicable state and federal laws, standards and procedures on a need to know and right to know basis.

Classified material containing information or security files as defined in section

(f) of the California Government Code will be restricted by JRIC and will only be released to other agencies on a need to know basis.

10. BACKGROUND INVESTIGATION:

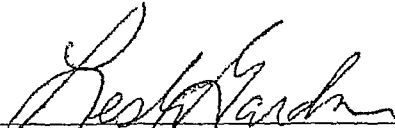
Due to the sensitive nature of the information gathered, processed and disseminated by the JRIC, access to such sensitive information by any sworn or civilian (non-sworn) staffer assigned to the JRIC will only be done subsequent to satisfactory completion of a background check which includes a criminal history check. Each of the Parties will be responsible for completing the appropriate background check on their employee prior to assignment to the JRIC. Background checks may include secret and/or top secret level clearances performed and determined by the Federal Bureau of Investigation.

11. SALARY AND BENEFIT COMPENSATION:

Salaries and benefits for agency personnel assigned to the JRIC will be paid by Agency. It is expressly agreed that JRIC will not reimburse Agency for any costs of personnel assigned to the JRIC under this agreement.

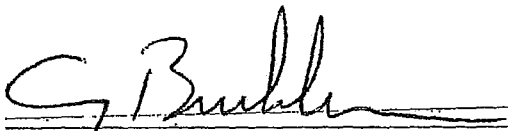
12. DURABILITY:
This MOU shall become operational and effective upon execution by the Parties. The MOU shall remain for a term of five years, and may be extended by amendment of this agreement. Parties may terminate the MOU agreement at any time by giving written notice to the other Parties at least sixty (60) days prior to the effective date of termination.
13. BENEFITS AND IMMUNITIES:
The Parties shall agree that the provisions of this MOU are not intended to directly benefit, and shall not be enforceable by any person or entity not a party to this MOU. This MOU is not intended to confer any legal rights or benefits on any person or entity other than the Parties of this MOU.
14. INDEMNIFICATIONS:
Notwithstanding the provisions of Government Code Section 895.2, ~~Parties shall defend, indemnify, and hold harmless every other party and its officers, agents, employees and representatives from any and all losses, liability, damages, claims, suits, actions and administrative proceedings, and demands and all expenditures and cost relating to acts or omissions of the indemnitor, its officers agents or employees arising out of or incidental to the performance of any of the provisions of this MOU. Parties do not assume liability for the acts or omissions of persons other than the respective officers, its employees, agents and officers.~~
15. SIGNATORIES NOT AGENTS:
Parties to this MOU shall have no authority, express or implied, to act on behalf of any signatory in any capacity whatsoever as an agent. The Parties shall have no authority, express or implied, pursuant to this MOU to bind each other to any obligation whatsoever.
16. ASSIGNMENT PROHIBITED:
Parties to this MOU may not assign any right or obligation pursuant to this MOU. Any attempted or purported assignment of any right or obligation pursuant to this MOU shall be void and of no effect.
17. NON-DISCRIMINATION:
No person shall, on the grounds of race, color, religion, ancestry, gender, age (over 40), national origin, medical condition (cancer), physical or mental disability, sexual orientation, pregnancy, childbirth or related medical condition, marital status, or political affiliation be denied any benefits or subject to discrimination under this agreement.

IN WITNESS WHEREOF, the parties hereto have executed this MOU on the date as written below.



Leslie Gardner, Executive Director of JRIC
Federal Bureau of Investigation

5/7/09
DATE



Craig Buehler, Chief
Bureau of Investigation and Intelligence
Division of Law Enforcement

4/16/09
DATE



LOS ANGELES POLICE DEPARTMENT



MAJOR CRIMES DIVISION – ANALYSIS SECTION (RFI11003_11072011)

Suspicious Activity Reporting and The Photographer's Rights

Brief History:

The American Civil Liberties Union (ACLU) recently filed a lawsuit against the Los Angeles County Sheriff's Department and several of its deputies alleging harassment, illegal search and detention of photographers. While photography is one of the SAR reporting criteria, *photography is a constitutionally protected activity* and should not be reported in a SAR absent **articulable facts and circumstances** that supports the source's suspicion that the behavior observed is not innocent, but rather *reasonably indicative* of suspicious activity associated with terrorism.

What YOU NEED TO KNOW?

- Laws concerning Consensual Encounters – California Peace Officers Legal Source Book
- Training Bulletin – Legal Contacts with the Public (Consensual Encounters)
- Vol. XXXVIII, Issue 1 April 2006
- Office of the Chief of Police Notice 1.1 Constitutional Policing
- Special Order No. 11 (Currently being revised)

A consensual encounter is one method an officer can use to approach an individual in a public place and assess whether he or she is involved in legitimate photography or potential criminal behavior.

A consensual encounter is a contact that is not coerced, is not a detention, and it is not an arrest or seizure.

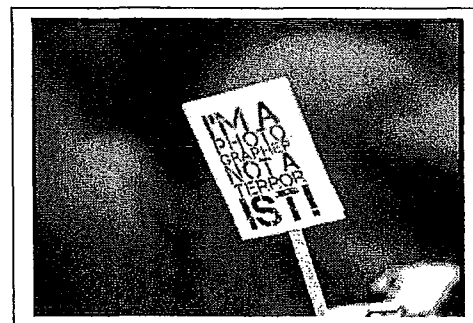
The objective question is: Would a reasonable person believe he or she was free to leave?

Reasonable questions to ask during a Consensual Encounter:

- Can I talk to you?
- May I talk to you?
- Would you mind talking to me for a second?

Elements that could change the encounter into a detention:

- The officer uses a harsh accusatorial tone of voice.
- The officer orders the person to do something, such as:
 - Stop, let me see your hands, don't move, or come over here.
- The officer demands to see ID and does not return it.



Consensual Encounters are contacts that you can make on a daily basis. Knowing the limits of this type of encounter will allow you to be more effective when you are speaking to the general public.

Photography Activists know their rights and have published, "The Photographer's Right, Your Rights and Remedies When Stopped or Confronted for Photography," dated November 2006. Photography Activists are TESTING your knowledge of the law and willing to be detained and arrested to prove their point.

Following are internet sites for further information:

<http://animalnewyork.com/2011/10/aclu-sues-lapd-for-harassing-photographers/>
http://pdinfoweb.lapd.lacity.org/files/RefLib/Training_Bulletins/2006/Police%20Contacts.pdf
http://pdinfoweb.lapd.lacity.org/files/RefLib/Notices/OCOP/2010/OCOP_111510.pdf
http://www.nppa.org/news_and_events/news/2005/08/rights.pdf
<http://www.krages.com/ThePhotographersRight.pdf>

OFFICE OF THE CHIEF OF POLICE

NOTICE 1.1

November 15, 2010

TO: All Department Personnel

FROM: Chief of Police

SUBJECT: CONSTITUTIONAL POLICING AND BIASED POLICING

Policing in a constitutional manner is the responsibility of each and every one of us.

The purpose of this Notice is to reaffirm my commitment to Constitutional Policing, reiterate the anti-bias policy and communicate my expectations of you.

POLICY:

In summary, federal and state laws and Department policy prohibit conducting police actions solely on the basis of race, color, ethnicity, national origin, gender, gender identity, gender expression, sexual orientation, or disability. Police-initiated stops or detentions, and activities following stops or detentions, shall be unbiased and based only on legitimate, articulable facts, consistent with the standards of reasonable suspicion or probable cause, as required by federal and state laws (Department Manual Section 1/345).

Note: The fact that it is ultimately determined that the person you stopped committed a traffic violation or equipment violation may still result in a finding that you violated this policy if it is determined that your initial decision to conduct the stop was based not on the violation itself, but rather on any of the prohibited factors listed above.

POLICE OFFICER'S AND DETECTIVE'S EXPECTATIONS:

I expect you to practice constitutionally-sound policing and demonstrate your awareness and application of laws relative to detentions, arrests, searches and seizures. It is crucial that you had reasonable suspicion or probable cause and are able to sufficiently articulate the reasons for your police actions in a manner that demonstrates the constitutionality of all of your actions. Equally as important, research has shown that in some instances, allegations of biased policing are as much about courtesy and respect as they are about bias. It is my expectation that when you stop someone, inconvenience them, etc., that you explain to them why you took the actions you did, when it is safe to do so.

SUPERVISOR'S EXPECTATIONS:

I expect you to take issues of biased policing seriously. Do not allow joking about "profiling," regardless of the setting or who is involved, but especially when subordinates are present.

Treat each complaint of biased policing seriously and each person making the complaint with respect and keep these investigations confidential. When conducting personnel complaint "intake," do a thorough job as possible by thoroughly interviewing the complaining party and all available civilian witnesses, collecting evidence, and taking photos, when needed. Most importantly, insist that your officers treat the community members with dignity and respect.

STAFF AND COMMANDING OFFICER'S EXPECTATIONS:

I expect each of you to communicate to your commands the seriousness with which the Department takes issues of bias. Ensure that everyone is aware of the policy and abides by its tenets.

When adjudicating personnel complaints involving issues of bias, it is incumbent upon you to thoroughly examine the constitutionality and appropriateness of the actions of your personnel, as well. If you identify training issues, take immediate action to ensure that members of your command understand and possess the tools needed to comply with my expectations regarding Constitutional Policing.

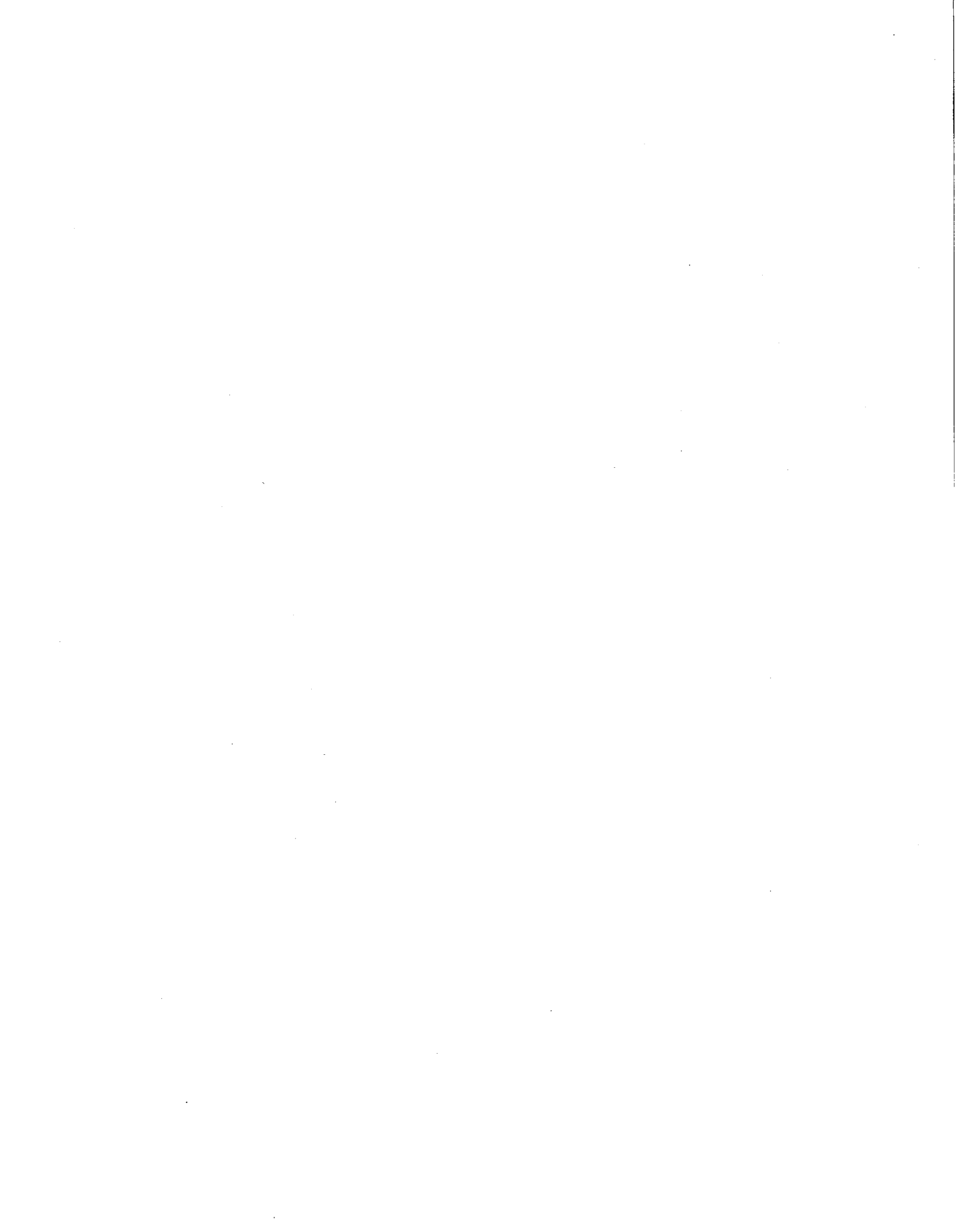
Should you have questions in regard to this Notice, please contact my Chief of Staff,

[REDACTED]



CHARLIE BECK
Chief of Police

DISTRIBUTION "A"



LOS ANGELES POLICE DEPARTMENT



MAJOR CRIMES DIVISION – ANALYSIS SECTION (RF11004_11092011)

[REDACTED]

Brief History:

[REDACTED] is an extremist international animal rights campaign to close down [REDACTED] Europe's largest contract animal-testing laboratory. [REDACTED] conducts research and tests medical and non-medical substances on animals for the development of consumer products.

[REDACTED]

Known crimes and acts of violence:

Arson, Bomb Threats, Vandalism, Cyber and Telephonic Attacks

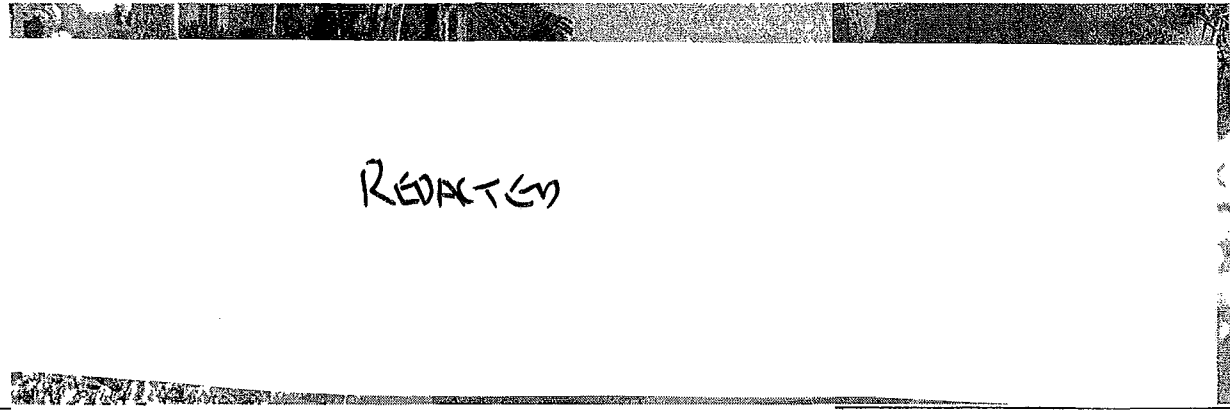
Targets:

- Investor companies [REDACTED]
- Subsidiary companies [REDACTED]
- Universities [REDACTED]
- Restaurants and Businesses that use or serve animal products
- Animal Shelters
- Employees/family members of all connected companies

What Should YOU Look For?

- [REDACTED]
- Graffiti depicting [REDACTED]
- [REDACTED]
- [REDACTED]

EXAMPLES of Vandalism:



Officers responding to crime scenes involving animal rights groups shall protect the crime scene; contact **Major Crimes Division, ATIS** at [REDACTED] during day watch hours and after hours notification shall be made to **RACR Division** at [REDACTED]. Major Crimes Division ATIS will respond to assist. Officers shall complete all crime/arrest reports to include a SAR. Copies of crime and arrest reports and original SAR shall be sent to MCD, SAR Unit Stop #400.

LOS ANGELES POLICE DEPARTMENT



MAJOR CRIMES DIVISION – ANALYSIS SECTION

Sovereign Citizens – How to Identify and Report Suspicious Activities via a SAR in Your Area

Brief History:

The "sovereign citizen" (SC) movement is a loosely organized collection of groups and individuals who have adopted a right-wing anarchist ideology originating in the theories of a group called the Posse Comitatus in the 1970s. Its followers believe that virtually all existing government in the U.S. is illegitimate and they seek to "restore" an idealized, minimalist government that never actually existed.

What Should YOU Look For?

- [REDACTED]ense
- [REDACTED]
- [REDACTED]s
- [REDACTED]

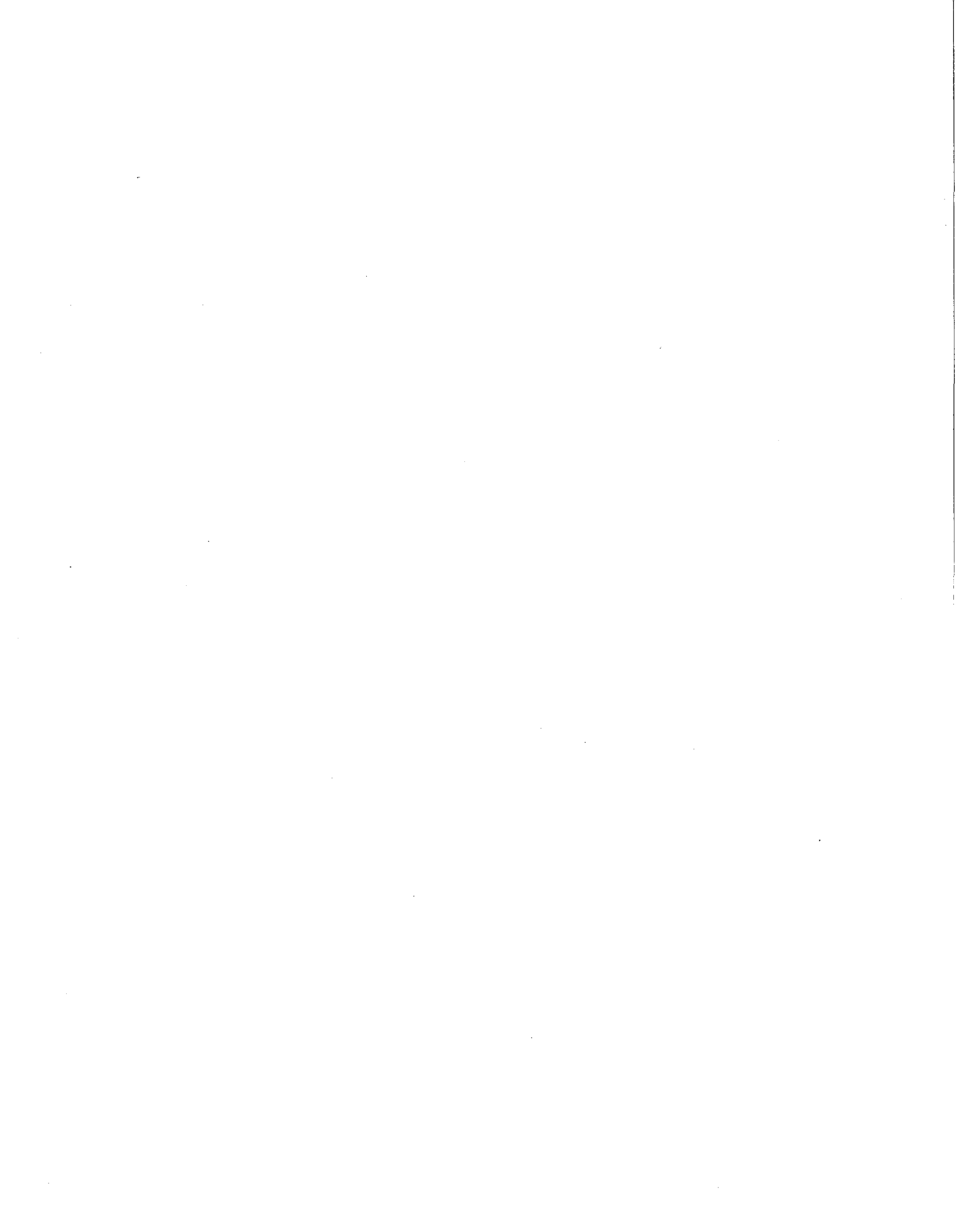
EXAMPLES of Driver Licenses and ID Cards

REDACTED

Upon encountering SCs, Officers shall complete an LAPD Suspicious Activity Report (SAR) and attach any copies or photos of the above mentioned material. They may also call the Analysis Section of Major Crimes Division at [REDACTED]

Links to Intelligence Bulletins or News Footage concerning Sovereign Citizens:

- www.cbsnews.com/video/watch/?id=7365985
- www.youtube.com/watch?v=gjkk8fVLoNk
- www.cfix@ocfl.net
- www.wordpress.com





TRAINING BULLETIN

Los Angeles Police Department

William J. Bratton, Chief of Police

Volume XXXVIII, Issue 1

April 2006

LEGAL CONTACTS WITH THE PUBLIC

Police officers have daily contact with the public for a variety of reasons. Each public contact is classified by law as a "consensual encounter," a "detention," or an "arrest." The purpose of this bulletin is to assist officers in identifying and articulating the unique and specific details of encounters which may lead to an arrest.

The Fourth Amendment

The first part of the Fourth Amendment of the U.S. Constitution deals with the right of people to be free from unreasonable searches and seizures. A Fourth Amendment "seizure" i.e., detention, does not occur merely because an officer approaches an individual and asks a few questions, or asks for identification, as in a consensual encounter. However, a detention may result from physical restraint, unequivocal verbal commands, or words or conduct by the officer which clearly relate to the investigation of specific criminal acts.

CONSENSUAL ENCOUNTER

A consensual encounter is an encounter between a police officer and an individual in which the individual **voluntarily agrees** to stop and speak with the officer. These encounters can take place on streets and sidewalks, in cars, on busses, in airports, homes, or businesses. A consensual encounter allows an officer who has a hunch or some minimal information that a person may be violating the law, to engage the person in a brief conversation for the purpose of confirming or dispelling the officer's suspicions.

What makes these encounters unique, is that officers, because they have neither reasonable suspicion to detain nor probable cause to arrest, **cannot legally prevent the individual from just walking away**. The individual has a right to refuse to cooperate, in which case officers must leave the individual alone. Refusal to cooperate, by itself, is not reason enough to detain. Nor would a refusal to cooperate constitute a violation of Penal Code § 148, which makes it unlawful for a person to willfully resist, delay, or obstruct an officer in the performance of his or her duties. So, officers must seek the individual's cooperation, which mean force, threats, and intimidation are out of

the question. To be successful in a consensual encounter, officers must rely on a combination of their persuasive ability, personal restraint, common sense, and a good working knowledge of the law.

During a consensual encounter officers can gather information, interview witnesses at the scene of a crime or accident, have a casual conversation, and disseminate information. Officers may also approach an individual and **request** the individual to show identification, remove hands from pockets, or step to the side and answer questions. Officers **cannot require** the individual to stay and talk with them, or require the individual to identify him/herself. The key element is that the person remains totally free to leave or not cooperate.

REDACTED

Elevating Consensual Encounters

The exact words officers use, and even their tone of voice, are extremely important to a court that is trying to decide if the contact was voluntary or not. If an officer starts to **give orders, demand answers, display a weapon, use a harsh tone, tell the person to stop what he or she is doing, or to move to some other location**, the encounter will be viewed as a detention, and it will be illegal unless supported by "reasonable suspicion." The courts have ruled the following commands to a suspect rendered the subsequent encounter a detention:

- Come over here. I want to talk to you.
- Stop.
- Stay there.
- Hold it.
- Police.
- Step away from your car.
- Sit on the curb.
- Put your hands on the dashboard.
- Get off your bicycle, lay it down, and step away from it.
- Put your hands up and get out of the car.

REDACTED

There are normally alternate actions that an officer can take to avoid elevating a consensual encounter into a detention.

Possible Elevating Actions	Alternate Actions
Use of emergency lights	Use a spotlight rather than emergency lights
Location of the officer or the police vehicle that prevents the person or car from leaving	Select an unobstructive position or location
Issuing orders or commands	Request consent, seek voluntary cooperation
Use of accusatory questioning or tone of voice	Use of nonaccusing, helpful, inquisitive tone of voice; request compliance rather than ordering it
Conducting patdown searches without legal justification	Ask for consent to patdown
Obtaining and/or keeping a person's identification	Request identification and return it when finished or upon request

REASONABLE SUSPICION

An officer may need to detain a person in order to investigate that person's involvement in possible criminal activity. To be lawful, a detention must be based on reasonable suspicion that criminal activity has taken place or is about to take place, and that the person detained is connected to that activity. This "suspicion" must be supported by **articulable facts** rather than hunch or instinct. These facts can be drawn from the officer's observations, personal training and experience, or information from eyewitnesses, victims, or other officers.

In some cases, the decision to detain is based on a single circumstance; e.g., the individual matched the description of a wanted person or a person who had just committed a crime in the area. But often the decision to detain is based on a variety of circumstances which, when considered as a whole, are sufficiently suspicious to justify a detention.

Contributing Factors

The following are some of the factors that contribute to establishing reasonable suspicion. **Although none of these circumstances standing alone will usually justify a detention, various combinations of them will.**

- Appearance of suspect (intoxicated, resemblance to wanted person),
- Actions (hiding objects, looking furtively, flight from officers or crime scene),
- Driving behaviors,
- Prior knowledge of the person (criminal record or conduct),
- Demeanor (nonresponsive, nervous, lying),
- Time of day (unusualness),
- Area of the detention (near crime scene, known criminal activity in area), and
- Officer training and experience (modus operandi, expertise in certain area such as narcotics or gang activity).

REDACTED

REDACTED

Investigative Actions

Once officers have stopped or detained a suspect, they may take whatever investigative actions are reasonable under the circumstances to determine the suspect's possible participation in a crime. **A detainee is not obligated to answer any questions** an officer may ask during a lawful detention. The refusal to answer questions alone does not provide probable cause for escalating a detention to an arrest.

Common investigative actions include:

- questioning the suspects about their identities and conduct;
- contacting other persons to confirm explanations, verifying identification, or determining whether a person is wanted (warrant check);
- checking premises, examining objects, or contacting neighbors or other individuals to determine whether a crime (e.g. burglary) actually occurred; or
- conducting a field show-up.

Length of Detention

A detention must be temporary and last no longer than is necessary to carry out the purpose of the stop. A detention which is legal at the beginning will become invalid if it is extended beyond what is reasonably necessary under the circumstances.

REDACTED

If the suspect answers all questions about the suspicious circumstances satisfactorily, so that suspicion decreases or disappears, the suspect must be released. Of course, it is possible for an officer's original suspicion to dissipate, while suspicion about a different or unrelated offense arises. There is no problem in "switching offenses" this way, as long as the original detention isn't unlawfully prolonged before your suspicion about the second offense begins.

REDACTED

Patdown Search

Normally, no searches are permitted during a detention unless the person gives voluntary consent. However, if an officer reasonably suspects that the person is carrying a concealed weapon or dangerous instrument, the officer is justified in conducting a patdown search to protect the officer or others from unexpected assault. The scope of the search is limited to a patdown of the outer clothing for possible weapons only.

Officers must be able to articulate the specific facts which lead to the search. Some specific factors that have been recognized as being contributors for establishing reasonable suspicion for conducting a patdown are:

- person's clothing (e.g., a bulge in clothing, or wearing a heavy coat on a hot night);
- person's actions (e.g., trying to hide something, overly nervous, threatening);
- prior knowledge of suspect for carrying weapons or violent behavior;
- isolated location so officer is unlikely to receive immediate aid if attacked;
- time of day (e.g., a dark, moonless night may increase likelihood that the officer might be attacked);
- reason for detention is serious, violent, or armed offense;
- similar patdown of detainee's companion revealed a weapon; or
- ratio of suspects to officers.

REDACTED

PROBABLE CAUSE

The Fourth Amendment requires probable cause to make an arrest. Probable cause to arrest is a set of facts that would cause a person of ordinary care and prudence to entertain an honest and strong suspicion that the person to be arrested is guilty of a crime. Definite information, or enough to convict the individual is not needed, only the fair probability that the individual committed the crime.

No matter what the context is, "probable cause" always boils down to the same question: Does an officer possess enough factual knowledge or other reliable information so that it is reasonable for him/her, in light of his/her training and experience, to believe "X."

For example, in the context of a warrantless search of a vehicle, it means enough information to believe that the object of the search is in a particular portion of the car. In the context of the plain view doctrine, it means enough information to reasonably believe the object is contraband, stolen property, or evidence of a crime. In search warrant context, "probable cause" means enough credible information to reasonably provide a "fair probability" that the object sought will be found in the place the officer wants to search. In the context of arrests, "X" means enough information for the officer to believe the person is guilty of a crime.

In addition to the facts, knowledge, training, expertise, experience, observations, etc., that the officer personally has, probable cause can consist of information conveyed to the officer by others (such as victims, citizens, other officers, and "official channels," informants, tipsters, etc.), as long as it is reasonable to rely on this information under the totality of the circumstances.

Increased Suspicion

Often what officers see and hear during the detention (evasiveness, nervousness, other conduct or property) will increase their suspicion and provide probable cause for arrest.

REDACTED

REDACTED

Factors that contribute to establishing reasonable suspicion can also be used to establish probable cause, or can escalate into probable cause.

Factors for Reasonable Suspicion	Probable Cause to Arrest
Possible influence of alcohol or drugs	Illegal level of intoxication, contraband
Actions/words/demeanor during detention	Self-incrimination, contraband, stolen property
Erratic driving behaviors	DUI, contraband
Patdown for weapons	Possession of illegal weapons or contraband
Possible connection to burglary/robbery	Discovery of stolen property

Documenting Probable Cause

Officers must be able to articulate in court and convey in the arrest report, the facts leading up to the arrest. The specific details of each incident and all relevant circumstances that reasonably caused the officer to believe the suspect was engaged in criminal activity must be documented, usually in chronological order, so that no obvious questions are left unanswered. Not only does the arrest report provide investigative leads and a basis for prosecution, it is also critical for refreshing an officer's recollection of events prior to testifying in court.

REVIEW

The following scenario shows how a consensual encounter can escalate into probable cause to arrest.

Note: The tactics used in this scenario run counter to the tactics taught by the Department. Officers contacting an individual while seated in their vehicle seriously compromise their ability to react and defend themselves should they encounter an armed suspect. This scenario is provided because of its legal significance.

REDACTED

REDACTED

CONCLUSION

It will be to the officer's advantage to have a thorough understanding of consensual encounters, reasonable suspicion and probable cause. Proper application directly impacts the officer's ability to enforce the law in a fair and impartial manner. Becoming confident in expressing the corresponding facts in reports and testimony will ensure that prosecutors file charges and cases do not get dismissed in court.

REFERENCES

California Peace Officers Legal Sourcebook
Point of View, Volume 28, Number 3, 2000, Alameda County District Attorney's Office
Legal Bulletin, Volume 20, Issue 2, October 15, 1996
California Commission on Peace Officer Standards and Training, LD # 15, 1998

This Bulletin cancels and supercedes Volume XXXIII, Issue 2, March 2001

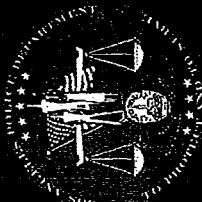
Field Training Services Unit
Training Division

Distribution "A"





LOS ANGELES POLICE DEPARTMENT



Terrorist Screening Center (TSC)

Official Use Only

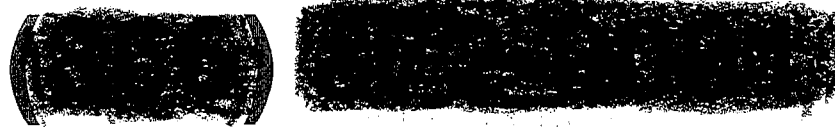


LOS ANGELES POLICE DEPARTMENT



TERRORIST SCREENING CENTER

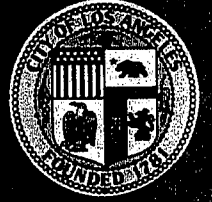
**Always Call TSC when a “hit”
occurs during a name check**



- **Handling Code 1**
- **Handling Code 2**
- **Handling Code 3**
- **Handling Code 4**



LOS ANGELES POLICE DEPARTMENT



TSC Handling Code 1

- High Risk Terrorist
- Arrest on Contact
 - If the Arrest Warrant is not showing, contact TSC
- Notify the TSC of the TSC hit
- Notify the Watch Commander
- Complete a SAR (Suspicious Activity Report)



LOS ANGELES POLICE DEPARTMENT

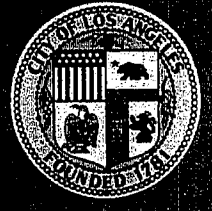


TSC Handling Code 2

- Associated with Terrorism
- May show a warrant
 - Do not arrest or detain
 - Call TSC to verify what action should be taken
- Notify the TSC of the TSC hit
- Notify the Watch Commander
- Complete a SAR



LOS ANGELES POLICE DEPARTMENT



TSC Handling Code 3

- On Terrorist Watchlist
- Try to get as much information as legally possible
- Notify the TSC of the TSC hit
- Notify the Watch Commander
- Complete a SAR



LOS ANGELES POLICE DEPARTMENT



TSC Handling Code 4

- Has been detained by Department of Defense overseas
- Try to get as much information as legally possible
- Notify the TSC of the TSC hit
- Notify the Watch Commander
- Complete a SAR



LOS ANGELES POLICE DEPARTMENT



Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO. SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7	SENT RECALL SHIFT F8	PAGE BACK SHIFT F9	PRINT SCREEN SHIFT F10	COMPRESSED PRINT MSG SHIFT F11	
LOGOFF Esc	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7	RCVD RECALL F8	PAGE FRWD F9	PRINT MSG F10	GET NEXT MSG WAITING F11	SEND KEYPAD ENTER F12

UNAUTHORIZED DISCLOSURE IS PROHIBITED.

PAGE 040

REDACTED

y be on
ge 49

MORE PAGES

SEND (Click here or F12 or Keypad Enter)



LOS ANGELES POLICE DEPARTMENT



INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING - APPROACH WITH CAUTION

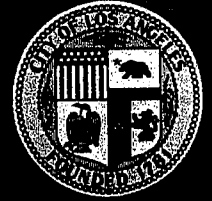
LAW ENFORCEMENT SENSITIVE INFORMATION

HLIST.***

REDACTED



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7	SENT RECALL SHIFT F8
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7	RCVD RECALL F8

TO: IC17 FROM: NCIC

11/03/08 15:27:44

PAGE

CA0190081

***MESSAGE KEY QWA SEARCHES ALL NCIC PERSONS FILES WITHOUT LIMITATIONS.
 LAW ENFORCEMENT SENSITIVE INFORMATION

CONTACT THE TSC IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER
 IMMEDIATELY CALL THE NTC.



LOS ANGELES POLICE DEPARTMENT



INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING - APPROACH WITH CAUTION

LAW ENFORCEMENT SENSITIVE INFORMATION

MKE

ST.***

6

REDACTED



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7

Beginning pages under the aliases there will be a NIC Number.

- If the NIC Number begins with a T then it is a TSC hit

AKA/ [REDACTED]

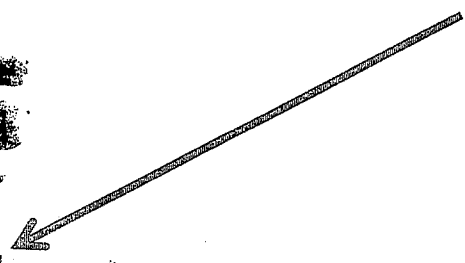
MNU [REDACTED]

MNU/ [REDACTED]

MNU/ [REDACTED]

CTZ/US

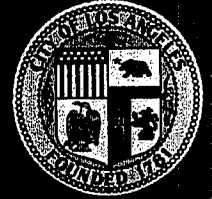
NIC/ [REDACTED] DATE [REDACTED] 1556 EDT



WARNING - STANDING ALONE, NCIC VIOLENT GANG AND TERRORIST ORGANIZATIONS FILE INFORMATION DOES NOT FURNISH GROUNDS FOR THE SEARCH OR SEIZURE OF ANY INDIVIDUAL, VEHICLE, OR DWELLING.



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7

AKA/ [REDACTED]

MNU/ [REDACTED]

MNU/ [REDACTED]

MNU/ [REDACTED]

CTZ/US

NIC/ [REDACTED] DTE/ [REDACTED] 1556 EDT

Need to rely on case by case basis:

- Consensual
- Vehicle Stop
- Arrest
- Etc.



WARNING - STANDING ALONE, NCIC VIOLENT GANG AND TERRORIST ORGANIZATIONS FILE INFORMATION DOES NOT FURNISH GROUNDS FOR THE SEARCH OR SEIZURE OF ANY INDIVIDUAL, VEHICLE, OR DWELLING.

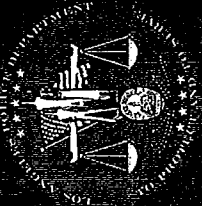


LOS ANGELES POLICE DEPARTMENT



Conclusion:

- Upon receipt of a TSC Hit (Cat. 1, 2, 3 or 4), call the TSC Dispatcher at [REDACTED]
- LAPD Officer encountering the Individual should complete a SAR at the conclusion of the stop



LOS ANGELES POLICE DEPARTMENT



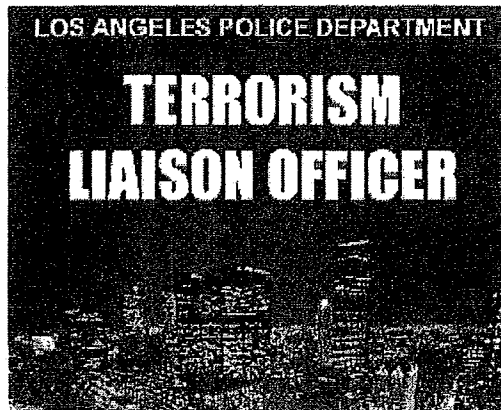
Questions?

TSC -- (██████████) ██████████ Available 24/7

LAPD Major Crimes Division -- (██████████) ██████████

LAPD RACR-- (██████████) ██████████ After Hours

TERRORISM LIAISON OFCR (TLO) PROGRAM



Citywide TLO Roster	TLO Special Order 26 (6/2009)	SAR Special Order 11 (5/2008)	SAR Notebook Divider	2011 Upcoming Training
Alerts	How to handle a Terrorism Screening Center Inquiry Hit	Sar Exemplar	Seven Signs of Terrorism	TLO.org

Shortly after 9/11, several police chiefs in the South Bay area of Los Angeles County organized a Terrorism Advisory Group as an effort to share information. One of the concepts that came out of this effort was that each agency should designate a Terrorism Liaison Officer (TLO). These officers became the principal points of contact for all terrorism-related information for their respective agencies.

Recognizing the extraordinary potential for the TLO program, the Los Angeles Police Department adopted a TLO program of their own. On September 16, 2005, Special Order No. 24, "Terrorism Liaison Officer Program - Established" was authorized for distribution. The order established the TLO program and procedures for the TLOs to follow and educate Department personnel in terrorism awareness.

A Terrorism Liaison Officer (TLO) is an individual that serves as the principal point of contact for their respective division in matters related to terrorism information. The TLO, though not an expert in terrorism, attends meetings and receives terrorism-related information from Major Crimes Division. The TLO then educates others within his or her division, thereby enhancing situational awareness, early warning, and operational preparedness. TLOs are a vital link in keeping patrol officers knowledgeable about current terrorist tactics, techniques, and practices. Through the diligent performance of their duties, patrol officers are alerted to indicators and warnings of potential terrorist activity that might otherwise go unnoticed and unreported. The TLOs will be the persons contacted when any suspicious activity is encountered in respective divisions. They then will ensure information is forwarded to Major Crimes Division.

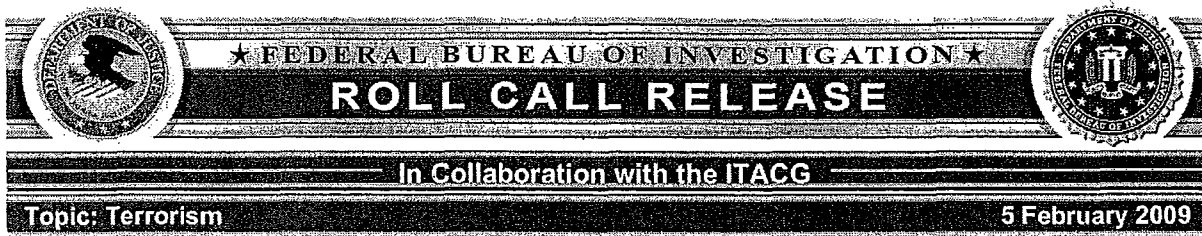
Important Phone Numbers:

Analytical Section of Major Crimes Division (SAR Unit): [REDACTED]
Off-Hour Reporting, call RACR for MCD On-Call Team: [REDACTED]
SAR Faxes: [REDACTED]
For All Emergencies: Call 911

For Public Use: 1-877-A-THREAT

TLO Coordinators:

Detective [REDACTED] (OSB/Divisions): [REDACTED]
Detective [REDACTED] (OVB & OWB/Divisions): [REDACTED]
Officer [REDACTED] (OCB/Divisions): [REDACTED]

**Terrorist Screening Center (TSC)**

TSC's 24/7 Call Center: [REDACTED]

The TSC operates a 24/7 call center to assist law enforcement, intelligence agencies, and other government authorities. TSC Operations Specialists work with callers to determine whether persons encountered are positive or negative identity matches to known or reasonably suspected terrorists listed in the Terrorist Screening Database (TSDB)—a US Government-consolidated, terrorist watchlist maintained by the Center. TSC personnel access various data sources to resolve identity matches. All positive and inconclusive matches are passed to the FBI's Counterterrorism Division for follow-up action.

National Crime Information Center (NCIC)

REDACTED

NCIC/ VGTOF provides access to a significant portion of the consolidated terrorist watchlist. Law enforcement personnel receiving messages to contact the TSC as part of a response to their NCIC transaction must contact the TSC to determine whether the individual who has been encountered is a positive identity match to the known or reasonably suspected terrorist.

(U) This *Roll Call Release* item was prepared by the FBI. The ITACG reviewed/and or commented on the product from the perspective of our non-federal partners. The TSC was established by Homeland Security Presidential Directive 6 and began operations on December 1, 2003. It is administered by the FBI with support from the Department of Homeland Security, the Department of State, the Department of Justice, the Department of Defense, the Director of National Intelligence, and the Department of the Treasury. Questions and comments may be directed to the TSC Outreach Coordinator, at [REDACTED]

SPECIAL ORDER #26
Terrorism Liaison Officer

VIDEO



-Definition

-Requirements

-Importance (Passion/Desire)

-Information flow

-LMS automation

DEFINITION:

-A TLO is a person who serves as the principal contact for their division in matters related to terrorism

-They disseminate information received from MCD, JRIC, and other Federal, State, and local intelligence sources

The TLO educates others within their division enhancing situational awareness, operational preparedness, and early warning

REQUIREMENTS:

Per Special Order #26 there are two mandatory TLO's; the Training Coordinator, and the S.L.O. Sergeant. The other three available positions are at the discretion of the divisional C/O. It is strongly recommended that a Detective be selected, to guarantee dissemination of info and training on terror related topics.

- Minimum POST Certified Basic TLO course.

- Provide Roll call training at a minimum of once every two weeks, preferably on rotating watches.

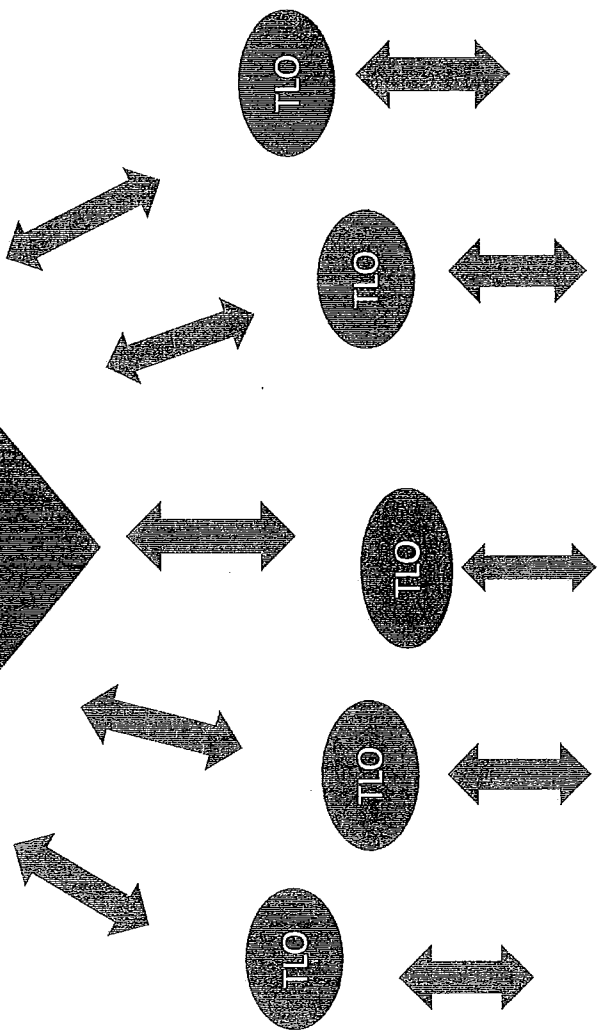
IMPORTANCE:

History has demonstrated to us that we are under attack not just abroad but domestically. We have to inspire the entire department to be vigilant in recognizing and reporting terrorism.

Only with your help can we remain safe.
The line officer has been a great barrier
against terrorism due to the training and the
nature of the work we do. If we fail to
continue to inspire them we not only fail the
City of L.A., we fail our country.

INFORMATION

TLO
COORDINATOR(S)

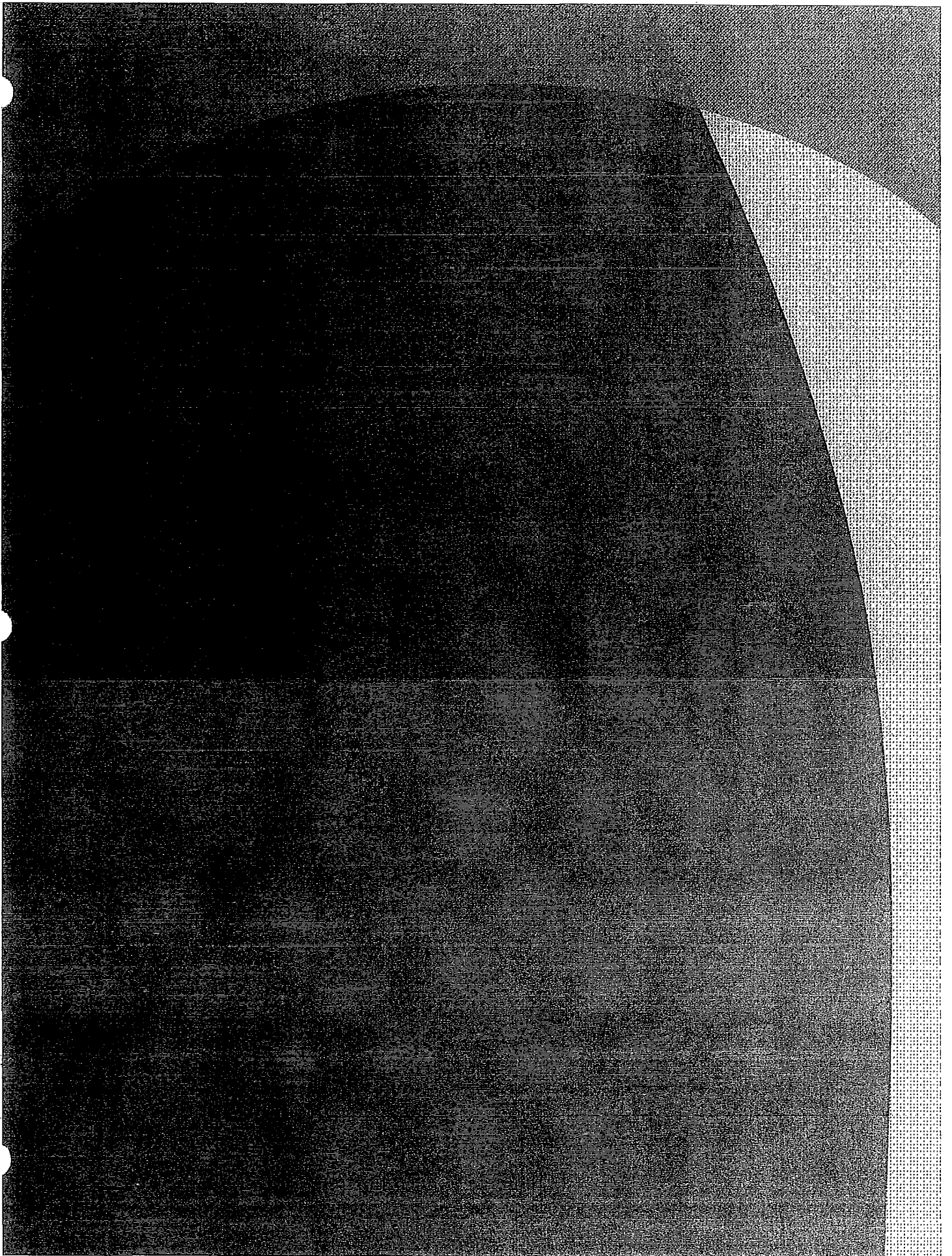


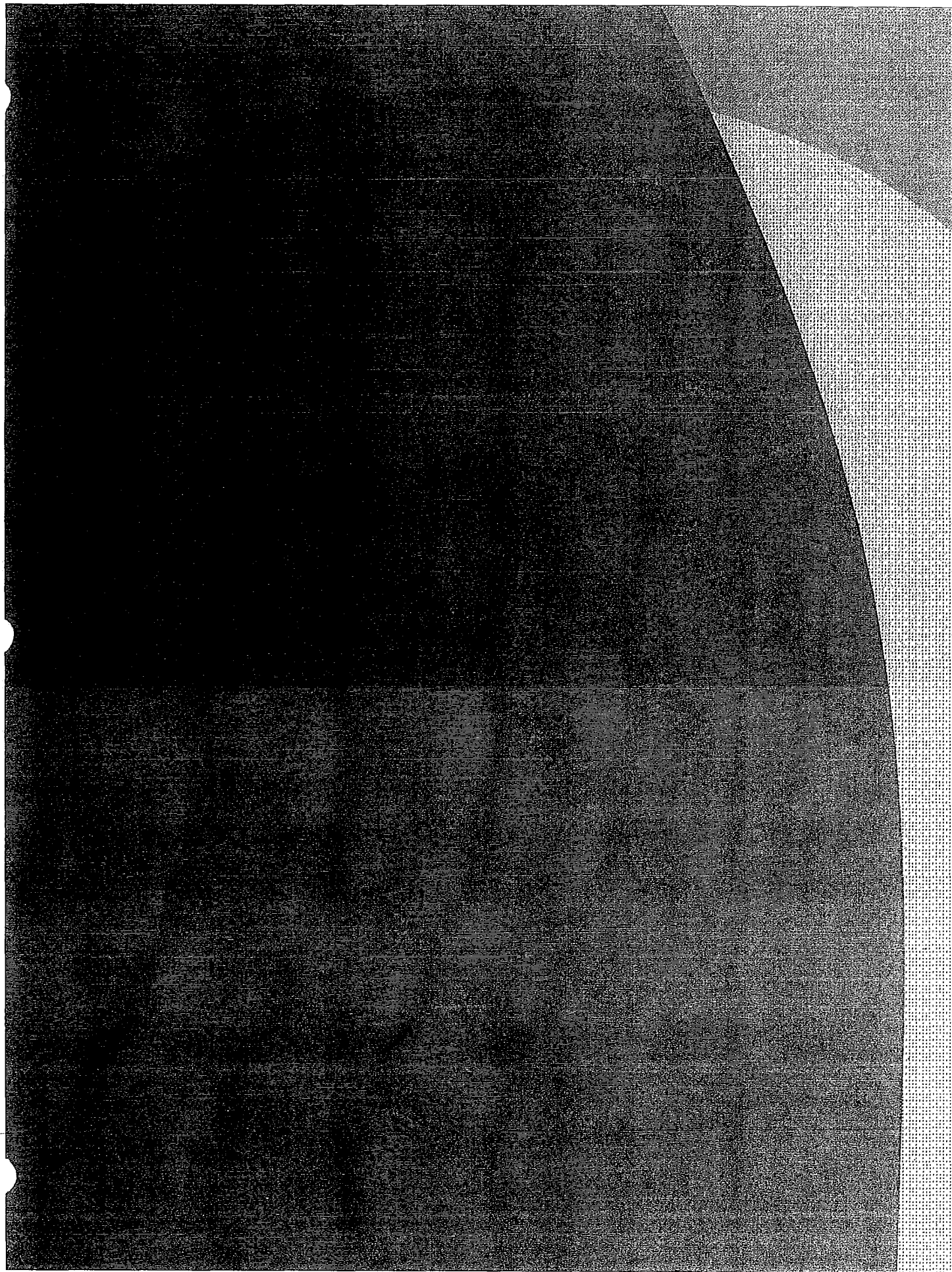
PATROL ROLL CALLS
DETECTIVE SQUAD MEETINGS
SUPERVISOR MEETINGS

Learning Management System

- Electronic Automation of the TLO Program
- Streamline the tracking of TLO's and required training
- Currently in testing phase

Questions ???







Terrorist Screening Center (TSC)

Official Use Only



Terrorist Screening Center (TSC)

- **An active Call Center operated by the FBI to assist Law Enforcement personnel, Intelligence Agencies, & various government authorities with investigative activities**
- **Established in Dec 2003 by the Department of Homeland Security (DHS)**



Terrorist Screening Center (TSC)

- **Purpose – Provide a dynamic Global Screening Network to support the detection of Terrorists**
- **Manned by Operations Specialists 24/7, to determine whether persons encountered in the field are listed in the Terrorist Screening Database (TSDB)**



Terrorist Screening Center (TSC)

- **Contents – TSC uses consolidated information from unclassified, sensitive, and classified databases to help law enforcement officers identify terrorist-related activities**
- **Manned by Operations Specialists 24/7, to determine whether persons encountered in the field are listed in the Terrorist Screening Database (TSDB)**

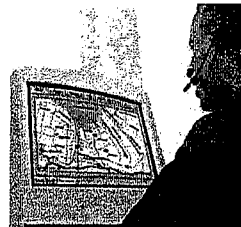


Basic Encounter Scenario

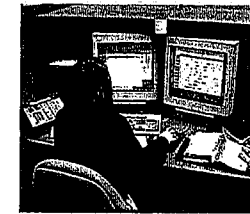
1. Police Officer Queries NCIC



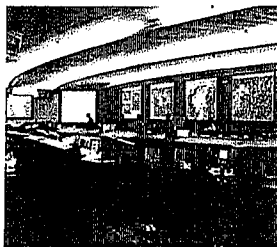
2. Dispatcher or Officer contacts TSC pursuant to NCIC



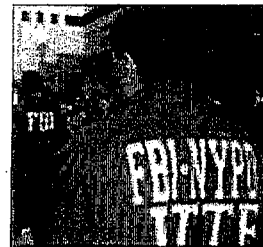
3. TSC confirms match and conferences into FBI TSOU



4. TSOU advises Caller and contacts Local JTTF to coordinate Investigation



5. JTTF responds and reports back to TSOU and TSC



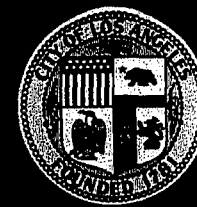
6. Information collected is disseminated to TSOU, FBI, DHS, and Others



7. If an FBI case does not exist on the individual (or associates) encountered, a Threat Assessment is initiated directly from the TSC



POLICE DEPARTMENT LOS ANGELES MENT



Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7	SENT RECALL SHIFT F8	PAGE BACK SHIFT F9	PRINT SCREEN SHIFT F10	COMPRESSED PRINT MSG SHIFT F11	
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7	RCVD RECALL F8	PAGE FRWD F9	PRINT MSG F10	GET NEXT MSG WAITING F11	SEND KEYPAD ENTER F12

UNAUTHORIZED DISCLOSURE IS PROHIBITED.

PAGE 049

INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

REDACTED

MORE PAGES

SEND (Click here or F12 or Keypad Enter)



LOS ANGELES POLICE DEPARTMENT



INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING - APPROACH WITH CAUTION

LAW ENFORCEMENT SENSITIVE INFORMATION

***[

T.***

REDACTED



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7	SENT RECALL SHIFT F8
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7	RCVD RECALL F8

TO: IC17 FROM: NCIC

11/03/08 15:27:44

PAGE

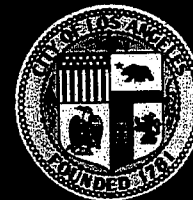
1L01
CA0190081

***MESSAGE KEY QWA SEARCHES ALL NCIC PERSONS FILES WITHOUT LIMITATIONS.
LAW ENFORCEMENT SENSITIVE INFORMATION

CONTACT THE TSC IMMEDIATELY THEREAFTER. IF YOU ARE A BORDER PATROL OFFICER IMMEDIATELY CALL THE NTC.



LOS ANGELES POLICE DEPARTMENT



INFORMATION THAT THIS INDIVIDUAL MAY BE ON A TERRORIST WATCHLIST IS THE PROPERTY OF THE TSC AND IS A FEDERAL RECORD PROVIDED TO YOUR AGENCY ONLY FOR INTELLIGENCE AND LEAD PURPOSES. THIS RECORD, AND ANY INFORMATION CONTAINED WITHIN IT, MAY NOT BE DISCLOSED OR USED IN ANY PROCEEDING WITHOUT THE ADVANCE AUTHORIZATION OF THE TSC.

WARNING - APPROACH WITH CAUTION

LAW ENFORCEMENT SENSITIVE INFORMATION

HLIST.***

5

REDACTED



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7

AKA [REDACTED]

MNU [REDACTED]

MNU [REDACTED]

MNU [REDACTED]

CTZ/US

NIC/[REDACTED] DTE [REDACTED] 1556 EDT

WARNING - STANDING ALONE, NCIC VIOLENT GANG AND TERRORIST ORGANIZATIONS FILE INFORMATION DOES NOT FURNISH GROUNDS FOR THE SEARCH OR SEIZURE OF ANY INDIVIDUAL, VEHICLE, OR DWELLING.



LOS ANGELES POLICE DEPARTMENT



JDIC

Local Help Password JDIC Contacts

LOGON SHIFT ESC	INFO SHIFT F1	SAV SCREEN LIST SHIFT F2	RCVD MSG LIST SHIFT F3	RCVD MSG FRWD SHIFT F4	RCVD MSG BACK SHIFT F5	UPDATE SHIFT F6	ADMIN SHIFT F7
LOGOFF ESC	HELP F1	SAVE SCREEN F2	ERASE FIELD F3	ERASE DATA F4	ERASE DISP F5	ENTRY F6	INQUIRY F7

AKA: [REDACTED]

MNU/ [REDACTED]

MNU/ [REDACTED]

MNU/ [REDACTED]

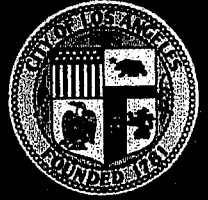
CTZ/US

NIC/ [REDACTED] DTE [REDACTED] 1556 EDT

WARNING - STANDING ALONE, NCIC VIOLENT GANG AND TERRORIST ORGANIZATIONS FILE INFORMATION DOES NOT FURNISH GROUNDS FOR THE SEARCH OR SEIZURE OF ANY INDIVIDUAL, VEHICLE, OR DWELLING.



LOS ANGELES POLICE DEPARTMENT

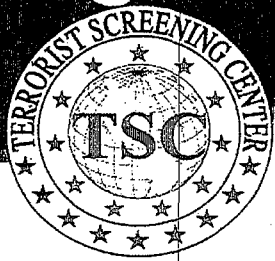


TERRORIST SCREENING CENTER

Always Call TSC when a "hit" occurs during a name check

(213) 485-2222

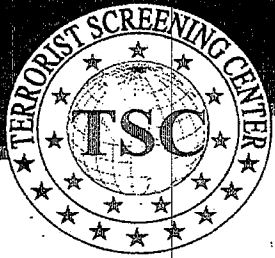
- **Handling Code 1**
- **Handling Code 2**
- **Handling Code 3**



NCIC Users and Law Enforcement Dispatcher

What can happen if you DO NOT contact the TSC when you see the NCIC "Banner"???

- A potentially important law enforcement encounter can go undetected, and officer safety could be jeopardized.
- The intelligence that could have been obtained from that law enforcement encounter will never get to the investigative agency.
- The Sheriff or the Chief of Police will never know that a positive law enforcement encounter was recorded in his jurisdiction, thus losing out on potential intelligence that could be used by the intelligence and law enforcement communities.
- The State Fusion Center will not receive notification that a positive encounter has taken place in their region.



Terrorist Screening Center

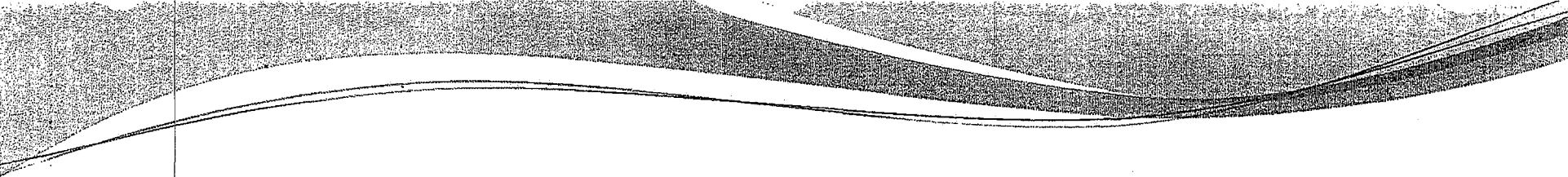
Conclusion:

- Upon receipt of a TSC Hit (Cat. 1, 2 or 3), call the TSC Dispatcher at [REDACTED]
- LAPD Officer who encountered the Individual should complete a SAR at the conclusion of the stop



Terrorist Screening Center

Questions?



Major Crimes Division
Analysis Section

TLO Duties - Successful Strategies



Terrorism Readiness

- May 1, 2011 the death of Usama bin Ladin
- One of the Departments 5 goals for 2011 is prevention and response to terrorism incidents.



Terrorism Readiness

Dissemination of Intelligence Information

- Crime Information Bulletins (Hot Sheets)
- Roll Call Training by: TLO's, MCD, and Divisional Detectives
- Bulletin Board Updated Information



Terrorism Readiness

Training of Divisional Personnel

- SAR Procedures – Special Order # 11, 2008 (SAR notebook dividers)
- TLO Program – Special Order #26. 2009 (Division should Have 5 TLO's)
- Standing Plans – Critical Infrastructure Awareness



Terrorism Readiness

Emphasis on Sound Basic Policing

- Traffic Enforcement
- FI's
- Detailed Crime Reports w/ emphasis on MO's
- Extra Patrol Locations to include selected Critical sites identified in the Standing Plans



Terrorism Readiness

Station Security

- Watch Commander Inspections (to include the gas pumps and natural gas valves)
- Station lighting during the hours of darkness.
- Station entrances and side doors (covered in Watch commander's Inspections)



Terrorism Readiness

- **Security Controls (twelve specific security controls)**
 1. Non-uniformed employees shall attach their identification card to an outer garment before entering the station
 2. Sworn and civilian personnel shall normally enter the station via the rear doors or the doors specific to your station
 3. Unescorted visitors shall enter and exit via the front lobby doors only and shall attach a visitor's pass to an outer garment while inside the station
 4. Door leading to all rooms and offices not in normal use shall be locked



Terrorism Readiness

5. All containers (briefcases, lunch boxes, etc.) carried into the station by Area personnel shall bear the owner's name and serial number in a conspicuous location. (any officer observing a suspicious package shall notify the watch commander immediately).
6. All Department vehicles shall be locked when not in use. Shotguns shall be returned to the station gun locker if the vehicle is to be out of service for an extended period of time and at change of watch.
7. Unattended private vehicles belonging to Department personnel shall be locked when parked on station property.



Terrorism Readiness

8. Screen on the TV security console located in the watch commander's office shall be closely monitored on a 24-hour basis to ensure responsible security.
9. Personnel shall challenge all unfamiliar persons attempting to walk or drive onto station property. Officers shall establish the identity and intent of all unfamiliar person requesting admittance to station facilities.
10. Unfamiliar persons loitering outside the station in restricted areas shall be interviewed and if the person is unable to provide adequate identification and explain their presence, he /she shall be interviewed by the watch commander.



Terrorism Readiness

11. Area personnel shall record the description of pedestrians and vehicles that appear to be cruising the station. The watch commander shall be notified immediately.

12. At all times, the following doors shall remain locked.

These doors can be made specific to your division i.e. Lockers rooms, telephone equipment rooms and doors to garages and patios and fuel pump area.

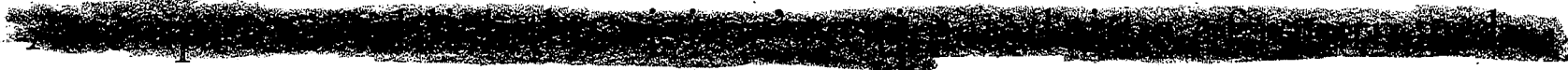




Terrorism Readiness

- **Desk Personnel Duties (six areas of tasks and security concern)**
 1. Require visitors to identify themselves and complete the visitor's roster prior to proceeding past the reception area.
 2. Require visitors carrying packages, briefcases, valises or any other containers to submit items for cursory inspection before or upon entering the police facility.
 3. Issue a visitor's card to each visitor and instruct the visitor to wear the card in a visible location on an outer garment. The card shall be retrieved when the visitor leaves the station.



Terrorism Readiness

4. Prior to permitting visitors to enter the officers of the Area and Patrol Commanding officers, the Crime Prevention Office of the Detective squad room, the respective officer shall be contacted to ascertain that an employee is available to receive the visitor.
5. 


6. If an attack appears imminent, all doors should be secured to prevent any unlawful entry. Due consideration of the situation should be made prior to allowing anyone's entrance.



Constitutional Policing

POLICY

- In summary, federal and state laws and Department policy prohibit conducting police actions solely on the basis of race, color, ethnicity, national origin, gender, gender identity, gender expression, sexual orientation, or disability.



Constitutional Policing

- Police-initiated consensual encounters regarding SAR activity, shall be unbiased and based only on legitimate, articulable facts, consistent with the suspicious activity that has a nexus to international and/or domestic terrorism.
- It is important to remember that suspicious activity itself is just that, suspicious activity and is not a crime there for you can not conduct a lawful detention solely based on the suspicious activity.



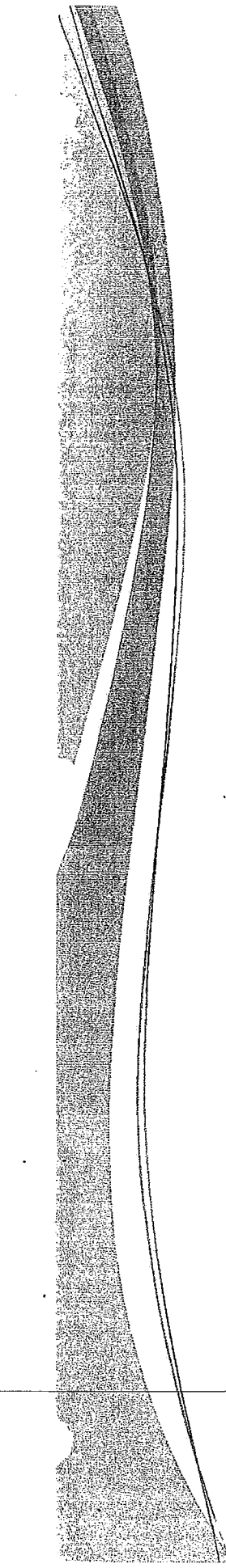
Constitutional Policing

- Some activities may be First Amendment-protected activities and/or privacy rights and should not be reported in a SAR, absent articulable facts and circumstances that support the source's suspicion that the behavior observed is not innocent, but rather reasonably indicative of suspicious activity associated with terrorism. Race, color, religion, national origin, gender, age, physical or mental disability, marital status, sexual orientation, gender identity, gender expression, creed, ancestry, or medical condition should not be considered as factors that create suspicion, although these factors may be used as specific involved party descriptors.



Constitutional Policing

- Risk Management
- Career survival
- Positive impact on the community

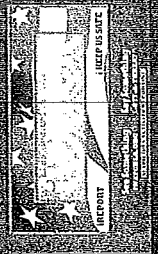
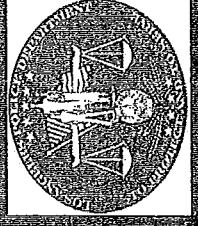


Questions ?

**Los Angeles Police Department
Counter Terrorism Special
Operations Bureau**

SAR REPORT

**Major Crimes Division
Analysis Section, SAR Unit**



Suspicious Activity Report (SAR)

What's New?

- Stand alone report
- Non-crime report
- No more “check box”

Suspicious Activity Report (SAR)

The IR shall no longer be used to report any act of Suspicious Activity and has been modified to delete the "Suspicious Activity" checkbox on the IR face sheet. All acts of suspicious activity shall be reported on the

Suspicious Activity Report, Form

03.24.00.0

Title of report

Los Angeles Police Department
SUSPICIOUS ACTIVITY REPORT

03.22.00 (06/10)
LAW

Page _____ of _____
NCP



Target

DR # Reference

Suspicious
Activity

REDACTED

IP not Suspect

Definition of Suspicious Activity

“Suspicious activity” is defined as an “observed **BEHAVIOR/ACTIVITY** that may be reasonably indicative of intelligence gathering or pre-operational planning related to terrorism, criminal, or other illicit intention.”

NOT A VALUE
NOT A VALUE
NOT A VALUE
NOT A VALUE

Definitions

Involved Party:

- An involved party is an individual that has been observed engaging in suspicious activity, remember suspicious activity is just that suspicious activity and is not a crime therefore the involved party can not be indentified as a suspect.

Definitions

Potential Target:

- A potential target is a person, facility/building, infrastructure or protected site that is or may be the object of the suspicious activity.

Criminal Activity

- Any criminal activity connected to suspicious activity shall be documented on the appropriate report and receive a separate Incident and DR Number. The DR Number shall be annotated in the upper left hand corner of the SAR report in the space provided.
- The SAR report Incident and DR Number shall not be annotated anywhere on any other report.

Property

- If there is property or evidence associated with the suspicious activity, a separate *Property Report* shall be completed. *The Property Report shall bear a separate DR and incident number from the SAR Report*
 - The evidence box shall be marked
 - The investigation unit shall be Major Crimes Division (MCD)

Property Report

- The connecting reports box shall be marked "None"
- In the narrative portion of the report, Officers shall write, "Do not release or disclose information connecting MICHELE BLOVINS to any case."

Definitions

- The Property Report DR number shall be referenced in the space provided on the upper left hand corner of the SAR face sheet

THE BOOKS OF THE
PROPERTY REPORT
SECURITY

SAR Completion

- Watch Commander review and approval
- Reports shall be ~~FAXED~~ to Major Crimes Division 213 ~~XXXXXX~~
- Original SAR and one copy of all related reports shall be gray mailed to Major Crimes Division, SAR Unit, STOP #400 within 24hours.

Questions

?

568. RADIO AND ELECTRONIC INVESTIGATION EQUIPMENT.

568.05 ELECTRONIC SURVEILLANCE EQUIPMENT - DEFINED. Electronic surveillance equipment is that apparatus used to detect, locate, observe, photograph, record or intercept information about persons under Department investigation without their knowledge. Electronic surveillance equipment is divided into two categories:

- **Restricted Items.** Restricted items normally include all electronic surveillance equipment designed or adapted for concealed use. Included are items such as: pen registers; trap traces; transmitters capable of being concealed in an automobile, room or telephone; body transmitters; induction coils; and receivers and recorders when used with hidden transmitters. Tracking or tailing devices and other non-visual equipment are also restricted items. Use of restricted electronic surveillance equipment requires authorization of a command or staff officer. Restricted electronic surveillance equipment shall also include any electronic equipment that is used to breach a person's reasonable expectation of privacy as recognized by all applicable statutes and case law.

Note: With the exception of miniature recorders, on-duty employees shall not possess or use privately owned restricted electronic surveillance equipment. When used, privately owned miniature recorders are subject to the same authorization requirements as other restricted items.

Discretionary Items. Discretionary items are those items not specifically designed for concealed use, but which can be used in a concealed manner. When used for such purposes, discretionary items temporarily become restricted items of electronic surveillance equipment and, as such, their use is controlled. Discretionary items include tape recorders, mini-recorders, hand-held radio receivers, T.V. cameras and video recorders, night-viewing devices, repeaters and cameras.

Note: A surveillance van is considered a discretionary item unless it is used in conjunction with a camera and lens at which time it is considered a restricted item.

Equipment Storage. Restricted electronic surveillance equipment shall generally be stored in a secured location within a Department facility. However, if it is required by the nature of the investigation, equipment used by specialized units in certain divisions (e.g. Gang and Narcotics Division, Vice Division, Major Crimes, Professional Standards Bureau, etc.) may be stored in vehicles, as long as it remains under the command and control of the investigating officer and as long as it remains in good working order.

Provide Security. All employees using electronic surveillance equipment shall provide security for the equipment while it is in their possession.

Time Restrictions. Restricted electronic surveillance equipment shall generally be used for a period of time not to exceed 30 days. However, equipment used in investigations by specialized units in certain divisions (e.g. Gang and Narcotics Division, Vice Division, Major Crimes Division, Professional Standards Bureau, etc.) may be used for the duration of the investigation, in excess of 30 days, provided that the equipment is accounted for, remains in good working order and prior approval is obtained. Should the investigation exceed the 30-day time limit, the investigating officer shall complete an Employee's Report, Form 15.07.00, documenting the reasons for the additional time required and the condition of the equipment. The Employee's

Report shall be completed and approved prior to the expiration of the due date. The investigating officer shall forward the Employee's Report to his/her commanding officer for approval.

The divisional, Area or patrol commanding officer will review and, if appropriate, approve the investigating officer's written request for the extended use of the equipment for each additional 60-day period. Once approved, the Employee's Report shall be forwarded to the Department entity originally furnishing the equipment so that it may be filed with the original Request to Use Electronic Equipment Form.

Return Equipment. Ensure that the equipment is safely returned to the assigned unit as soon as possible after the equipment's usage.

568.10 REQUESTS FOR USE OF RESTRICTED ELECTRONIC SURVEILLANCE EQUIPMENT. The following procedure shall be followed for every use of restricted electronic surveillance equipment.

Restricted Electronic Surveillance Equipment Policy – Defined. Investigating officers that require the use of restricted surveillance equipment shall comply with all current State and Federal Laws.

Obtain Authorization. Employees shall obtain proper authorization prior to using restricted electronic surveillance equipment.

Complete Training. Prior to using electronic surveillance equipment, employees shall satisfactorily complete required training.

Investigating Officers. Investigating officers who require the use of restricted surveillance equipment shall complete the top portion of an Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00, and submit the form to a supervisor for approval.

The investigating officer requesting extended use of the restricted electronic surveillance equipment shall:

- Include the request to use the restricted equipment for an extended period of time not to exceed 30 days; and,

Note: Equipment used in investigations by specialized units in certain divisions (e.g. Gang and Narcotics Division, Vice Division, Major Crimes Division, Professional Standards Bureau, etc.) may be used for the duration of the investigation, in excess of 30 days, provided that the equipment is accounted for, remains in good working order and prior approval is obtained.

- Include a notation as to the method and location of storage (e.g., locker, secured desk, etc.) when restricted equipment is not being utilized.

Upon approval by a supervisor and a Captain or above, Form 12.41.00 shall be submitted to the concerned equipment coordinator or Scientific Investigation Division (SID) Electronics personnel for equipment issuance. Daily usage of the restricted electronic surveillance equipment shall be documented on the Restricted Electronic Surveillance Equipment Monthly Usage Log, Form 12.41.01. The log shall be completed in the following manner:

- Entries shall be completed daily;
- Each entry shall be reviewed and signed by the supervisor of the concerned investigative unit; and,
- Upon completion of the investigation and the usage of the restricted electronic surveillance equipment, attach the completed log with the Authorization to Use Restricted Electronic Surveillance Equipment, and submit the completed forms to their supervisor for review.

Note: The use of restricted electronic surveillance equipment does not always require the use of an Authorization to Use Restricted Electronic Surveillance Equipment Form, Form 12.41.00. It is only required if the equipment is used to breach a person's reasonable expectation of privacy or is requested by the concerned commanding officer. Should the completion of the Authorization to Use Restricted Electronic Surveillance Equipment Form be required, upon approval by a supervisor and a captain or above, it shall be submitted to the concerned equipment coordinator, the Scientific Investigation Division (SID) Electronics Personnel or the relevant Department entity issuing the equipment.

Note: When the investigation is of a sensitive nature, only the shaded items are required to be completed.

Supervisors. Supervisors reviewing the Authorization to Use Restricted Electronic Surveillance Equipment shall be responsible for:

- Reviewing the Authorization to Use Restricted Electronic Surveillance Equipment, and discuss the intended use of the equipment with the investigating officer(s).
- Pre-approving the Authorization to Use Restricted Electronic Surveillance Equipment, and ensuring it is submitted to the concerned Captain or above for approval; and,
- Upon completion of the investigation and use of the surveillance equipment, review the Restricted Electronic Surveillance Equipment Monthly Usage Log and the Authorization to Use Restricted Electronic Surveillance Equipment form and ensure the forms are forwarded to the concerned commanding officer.

Note: When exigent circumstances exist, the Department Command Post, Communications Division, may be contacted for assistance in locating a *staff* officer. Bureau commanding officers or staff officers may grant telephonic authorization to use restricted electronic surveillance equipment, when the circumstances of the situation do not allow for approval through normal channels. When telephonic approval is granted, the name of the approving bureau commanding officer or staff officer shall be printed on the line where they would normally sign and the notation "telephonic" shall be placed next to the staff officer's name.

Commanding Officer's Responsibilities. In addition to established responsibilities delineated in Department Manual Section 3/568.15, the commanding officer, of the rank of Captain or above shall:

- Review and approve the Authorization to Use Restricted Electronic Surveillance Equipment; and,
- Ensure the Authorization to Use Restricted Electronic Surveillance Equipment and the Restricted Electronic Surveillance Equipment Monthly Usage Log are forwarded to the concerned staff officer for review.

568.15 REVIEW. Upon completion of the investigation and return of the equipment, the concerned commanding officer *and* a staff officer shall review the Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00.

Commanding Officer's Responsibility. The commanding officer reviewing the restricted electronic surveillance equipment usage shall:

- Evaluate the equipment usage for its compliance with all the aspects of technical, legal, and procedural requirements for the use of restricted electronic surveillance equipment. Appropriate comments, if any, shall be made in the "After Action Evaluation" portion of the Form.
- Determine if the equipment was used as authorized. Whenever modifications or deviations are noted they shall be explained in the "After Action Evaluation."
- Ensure that serial numbers of any tape(s) used, and the date and time the equipment was returned to the issuing unit, are recorded in the appropriate sections of the "After Action Evaluation."
- Certify that a review of the equipment usage has been conducted by signing the "After Action Evaluation" section of the Form 12.41.00.
- Cause the Form 12.41.00 to be delivered to the concerned staff officer for review.

Bureau Commanding Officer's or Staff Officer's Responsibility. The bureau commanding or staff officer reviewing the use of restricted electronic surveillance equipment shall:

- Ensure that the concerned commanding officer has reviewed the Form 12.41.00 and properly evaluated the technical, legal, and procedural aspects of the equipment usage.
- Document the review of the equipment usage by signing and dating the Form 12.41.00.
- Forward the completed Form 12.41.00 to the concerned equipment coordinator, Scientific Investigation Division, electronics personnel or the relevant Department entity issuing the equipment.
- Notify the Chief of Police of any concerns and/or problems that arise from electronic surveillance equipment usage.

Chief of Detectives, Detective Bureau - Responsibility. The Chief of Detectives, Detective Bureau, shall review all uses of restricted electronic surveillance equipment and shall be responsible for the following special duties relating to the use of such equipment:

- Maintaining a confidential file of all approved Authorizations to Use Restricted Electronic Surveillance Equipment, Form 12.41.00; and,
- Evaluate equipment needs for maintenance, planned replacement, assessments of future technology and/or efficiency, and effectiveness of the Department equipment resources.

568.20 REQUESTS FOR ASSIGNMENT OF STORED ELECTRONIC

INVESTIGATION EQUIPMENT. Requests for assignment of electronic investigation equipment stored at Scientific Investigation Division shall be made by commanding officers on an Intradepartmental Correspondence, Form 15.02.00, in duplicate. Requests for assignment on a permanent basis shall be submitted through channels to the Commanding Officer. Administrative

Services Bureau. Requests for assignment on a temporary basis shall be submitted through channels to the Commanding Officer, Scientific Investigation Division. Electronic investigation equipment assigned on a temporary basis by Scientific Investigation Division shall be returned upon completion of the assignment.

Note: In an emergency, the Officer in Charge, Electronics Unit, Scientific Investigation Division, may temporarily assign electronic investigation equipment pending the approval of the Commanding Officer, Scientific Investigation Division.

568.30 DUTIES OF COMMANDING OFFICER, INFORMATION TECHNOLOGY BUREAU - ASSIGNMENT OF STORED ELECTRONIC INVESTIGATION EQUIPMENT.

Upon receiving a request for the permanent assignment of electronic investigation equipment which is stored at Scientific Investigation Division, the Commanding Officer, Information Technology Bureau, shall determine the necessity for the requested equipment.

If the request is approved, forward the original copy to Scientific Investigation Division and return the approved duplicate to the division receiving the equipment.

If the request is disapproved, return the request to the originator with an explanation for the disapproval.

568.40 CONTROL OF ELECTRONIC SURVEILLANCE EQUIPMENT. Control of electronic surveillance equipment is the responsibility of the commanding officers of the following organizational entities:

Unit to Which Equipment is Assigned-Responsibilities. The commanding officer of every unit which maintains and uses electronic surveillance equipment shall be responsible for:

- Maintaining control over issuance of all electronic surveillance equipment assigned to the unit. The Electronic Surveillance Equipment Inventory Card, Form 12.42.00, may be used for this purpose.
- Submitting within 30 days, the inventory records of all electronic surveillance equipment acquired since the last annual inventory.
- Determining if persons requesting the loan of electronic surveillance equipment are sufficiently qualified to properly use the equipment.
- Maintaining, in proper working order, all electronic surveillance equipment assigned to the unit.
- Ensuring that personnel have been properly trained prior to using electronic surveillance equipment. Such training shall encompass technical, legal, and operational aspects of equipment usage.

Note: The commanding officer of every unit which frequently uses or regularly maintains electronic surveillance equipment shall appoint a minimum of two officers to act as unit electronic surveillance equipment coordinators. Officers appointed to this position shall perform their duties in addition to their regular assignment. Officers in this assignment shall have their days off and vacations scheduled so that one coordinator is always available during the unit's normal duty hours.

Unit Using Equipment-Responsibilities. The commanding officer of every unit using electronic surveillance equipment shall:

- Ensure that all officers using equipment are trained in the technical, legal, and operational aspects of electronic surveillance equipment usage.
- Ensure that each use of restricted electronic surveillance equipment is documented by a completed and approved Authorization to Use Restricted Electronic Surveillance Equipment, Form 12.41.00.
- Ensure that the equipment, while it is in the possession of the unit, is adequately secured and that it is afforded care and maintenance to ensure its continued operation.
- Ensure that all equipment is returned to the unit assigned the items as soon as possible.
- Ensure that whenever possible, all equipment installation and usage is completed in the presence of a supervisor.

Scientific Investigation Division-Responsibility. The Commanding Officer, Scientific Investigation Division, shall be responsible for the following duties and functions related to all electronic surveillance equipment:

- Functionally supervising the mechanical or technical aspects of all electronic surveillance equipment usage within the Department.
- Approving all replacement equipment for technical standards.
- Maintaining inventory records for all Department electronic surveillance equipment. The Electronic Surveillance Equipment Inventory Card, Form 12.42.00, shall be used for this purpose.
- Coordinating annual maintenance inspections and physical inventories conducted at the direction of each bureau commanding officer, and providing Scientific Investigation Division assistance in such inspections and inventories.
- Reviewing all budget and grant requests for electronic surveillance equipment and all purchases of such equipment, including component parts and attachments, to ensure Department wide compatibility.
- Inspecting all newly-acquired equipment prior to its delivery to the requesting unit and inspecting all unserviceable equipment prior to its delivery to Supply Section for disposal.

568.45 SURVEILLANCE EQUIPMENT TRAINING RESPONSIBILITY. Training in the technical, legal, and operational use of electronic surveillance equipment shall be the combined responsibility of the Commanding Officer, Training Division, and the commanding officer of any unit using electronic surveillance equipment.

Commanding Officer, Training Division-Responsibility.

- Developing a comprehensive training program to instruct members of this Department in the technical, legal, and operational aspects of electronic surveillance equipment usage.
- Incorporating electronic surveillance equipment training into Department schools for vice and narcotics officers, investigators, sergeants, lieutenants and captains.

568.50 STORAGE OF UNASSIGNED ELECTRONIC INVESTIGATION EQUIPMENT. Unassigned electronic investigation equipment shall be stored in a safe and secure place at Scientific Investigation Division.

568.60 REPAIR OF RADIO EQUIPMENT.

- When radio equipment is in need of repair, Communication Division, Information Technology Agency (ITA), shall be notified by telephone without delay.
- When emergency repairs are needed on radio equipment and personnel of Communications Division are not available, such repairs may be made by the Electronics Section, Scientific Investigation Division.
- When emergency repairs are made on radio equipment by other than ITA Communications Division personnel, the Director of Communications shall be notified as soon as practicable.
- The Director of Communications, when informed that emergency repairs have been made on radio equipment, will assign a technician to inspect the repaired equipment and make any necessary repairs or changes to bring the equipment within Department standards.

568.70 REPAIR OF ELECTRONIC INVESTIGATION EQUIPMENT. When electronic investigation equipment maintained by Scientific Investigation Division is in need of repair, the Electronics Section, Scientific Investigation Division, shall be notified by telephone, without delay:

- When emergency repairs are needed on electronic investigation equipment and personnel of Scientific Investigation Division are not available, such repairs may be made by personnel of the unit to which the equipment is assigned;
- When emergency repairs are made on electronic investigation equipment by other than Scientific Investigation Division personnel, the Electronics Section, Scientific Investigation Division, shall be notified as soon as practicable; and,
- When notification has been received by the Electronics Section, Scientific Investigation Division, that emergency repairs have been made on electronic investigation equipment, a technician shall be assigned to inspect the repaired equipment and make any necessary repairs or changes to bring the equipment within Department standards.

Exception: Repair of dictating and transcribing equipment shall be requested in the same manner as radio repairs (Manual Section 3/568.60).

568.80 TESTING OF ELECTRONIC INVESTIGATION EQUIPMENT. The officer in charge of a unit having electronic investigation equipment which is not in use shall test the equipment regularly to determine that it is in proper condition.



LOS ANGELES POLICE DEPARTMENT USE OF FORCE-TACTICS DIRECTIVE

Directive No. 11

June 2011

CROWD MANAGEMENT, INTERVENTION, AND CONTROL

PURPOSE

In a society where free speech and assembly is guaranteed by the Federal and State Constitutions, it is the mission of police officers to protect the constitutional rights of all members of the public. These constitutional rights apply to individuals participating in lawful activities such as public speeches, marches, demonstrations, picketing, rallies and celebratory events.

This Directive was developed to provide guidelines to assist officers and supervisors in identifying lawful versus unlawful assemblies. Additionally, it will provide insight into how the response and actions of law enforcement may affect the demeanor and response of a crowd. The thoughtful application of crowd management and intervention strategies will generally assist in efforts to facilitate legal First Amendment activity while at the same time removing those individuals whose illegal behavior jeopardize the purpose and safety of protected activity. The Department's Use of Force Policy relating to crowd control techniques is also reviewed in this Directive.

PROTOCOL

In determining whether First Amendment activities are lawful, police officers must not consider their personal views of either the political affiliation or the message of those persons exercising their right to assemble and engage in expressive activities. The responsibility of police officers is to objectively determine at what juncture a demonstration or assembly leaves the realm of legal protest and becomes an abridgement of the rights of others.

It is important for supervisors and officers to understand the definition of an unlawful assembly to determine the appropriate police response. Penal Code Section 407 defines an unlawful assembly as: "Whenever two or more persons assemble together to do an unlawful act, or to do a lawful act in a violent, boisterous or tumultuous manner, such assembly is an unlawful assembly." "*Boisterous or tumultuous manner*" has been interpreted by the courts to mean conduct which *poses a clear and present danger of imminent violence*.

Penal Code Section 407 identifies two different circumstances when an assembly may be declared unlawful:

The first circumstance is when people assemble to participate in an unlawful act. The unlawful act must be an act made criminal by law, or by the commission of an overt act that leads to a violation of the law. In the absence of any unlawful conduct, an assembly may be declared unlawful only if there is reasonable cause to believe, based on articulable facts, that the assembly's purpose is unlawful. If people are assembled to commit an unlawful act, then they are an unlawful assembly (e.g. unlawfully blocking entrances to public buildings, highways, sidewalks or schools, or engaging in other unlawful or riotous activity).

The second circumstance is when people assemble to do a lawful act in a "violent, boisterous or tumultuous manner." In order to be considered violent, boisterous or tumultuous, the manner in which the people are acting must be violent, or pose a clear and present danger of imminent violence. For example, a demonstration that disturbs the peaceful enjoyment of property through noisy singing and chanting is not an unlawful assembly unless it also poses a clear and present danger of imminent violence. It is important to note that one must differentiate between First Amendment activity and other activity. A loud party would not have to be violent, boisterous or tumultuous to be considered unlawful.

PROCEDURES

Any public assembly of individuals or groups, lawful or unlawful, may require support and/or intervention by law enforcement. Depending upon the situation, the response of law enforcement can range from observation and crowd management strategies, to crowd intervention and control strategies. The police response to each assembly or protest is different and will require law enforcement's flexibility, creativity, discipline and patience.

Crowd Management

First Amendment activity such as a march, demonstration, protest, rally or celebratory event is most often successfully facilitated by initially using the least amount of visible law enforcement presence necessary. An ongoing assessment of crowd behavior is critical in order for supervisors and officers to appropriately respond to the actions of a crowd or protest group. Experience has shown that the appearance of an organized, disciplined contingent of police officers will often cause a disorderly group to abandon their disruptive activities. However, if used inappropriately, the mere presence of officers and/or horses in riot gear may be perceived as aggressive and is sufficient to change the behavior of the crowd. This can cause the focus of the protest to shift from the group's original cause to the presence

Crowd Management Primary Objectives

- Establish contact with crowd
- Obtain voluntary compliance
- Minimize enforcement action

and actions of officers. Therefore, supervisors should consider this potential impact on crowd behavior and be thoughtful about the strategic deployment of police officers and horses in riot gear.

Instead of thinking about the best form of police action to control the crowd, it is important for supervisors to focus on how to act in order to encourage the crowd to manage itself. One way of achieving this is to place a major emphasis on urging crowd members to express their views in a lawful manner, even under conditions where one is aware of the presence of small isolated groups with illegal goals and even at points where these small isolated groups start to act in illegal and violent ways.

Intervention

Police officers and supervisors must understand the importance of differentiating between violent members of the crowd and peaceful protestors. When possible, officers should interact with crowd members in an effort to communicate law enforcement support of lawful First Amendment activity and rights of free speech and expression.

Crowd Intervention Primary Objectives

- Isolate unlawful behavior
- Arrest law violators
- Protect First Amendment activity
- Facilitate lawful protests

Unlawful behavior by individuals, or unlawful conduct observed in an isolated incident, should not automatically form the basis for declaring an otherwise lawful assembly to be unlawful. When it appears practical, officers should attempt to give warning to the leaders or spokesperson of the activity, the other participants, and/or the individuals about any observed unlawful or potentially unlawful conduct. When appropriate, officers should instruct them on what they must do to comply with the laws, so as to allow an opportunity to correct the conduct in question. Every effort should be made to protect and facilitate the actions of lawful demonstrators while using intervention strategies to stop illegal activity and remove law violators. However, when group behavior appears to be unlawful, aggressive, or otherwise uncontrollable, it is reasonable for the assembly to be declared unlawful.

Crowd Control and Dispersal

In the event a group or portion of a group becomes involved in violent or riotous behavior, the mission of the Department is to protect lives and property, and restore conditions to normal as rapidly and efficiently as possible. The rapid deployment of forces to contain and arrest those responsible for violent, riotous, or unlawful behavior and the dispersal of unlawful groups will help accomplish the Department's crowd control primary objectives.

Crowd Control Primary Objectives

- Protect life
- Restore and maintain order
- Arrest violators
- Protect vital facilities
- Protect property

When circumstances require crowd dispersal, the dispersal should generally not occur until control forces are in place to assist in managing the dispersed crowd, as unlawful conduct is extremely dynamic and mobile. Crowd dispersal strategies should only be used when immediate action is necessary to stop violence and/or property damage and/or sufficient resources are not present to ensure public safety.

Dispersal Orders

Methods to Deliver and Document Dispersal Orders

- Amplified sound
- Multiple languages when appropriate
- Confirm audibility from various locations
- Display signage indicating unlawful assembly and dispersal when possible
- Document with video/audio recording

The intent of a dispersal order is to permanently disperse a crowd, not to merely relocate the problem to another location. Supervisors should make a reasonable assessment to determine if the members of a crowd are attempting to comply with the dispersal order, or relocate the unlawful behavior. It should be made clear that the crowd is expected to immediately leave the area, and include a warning that force

may be used which could result in serious injury. The dispersal order must be given in a manner reasonably believed to be heard and understood by the intended audience. Based upon the circumstances, multiple announcements from various locations may be required. Dispersal orders should be delivered in English and in other languages that are appropriate for the audience. Regardless of the delivery method, the name of the individual giving the dispersal order and the date and time each order was given should be documented. Dispersal orders should not be given until control forces are in position to support crowd movement.

THE MEDIA

It is the Department's goal to provide the media as much access as legitimately possible to assist them in their duties. However, when an event is declared unlawful, all persons present, including members of the media, may be ordered to disperse. With the exception of spontaneously occurring events, whenever the Department develops an Incident Action Plan for an event that involves a public assembly, the Department will, when practicable, designate an area outside of the anticipated impacted area, but within viewing distance and audible range of the event, for members of the media to assemble.

USE OF FORCE

During crowd control situations, police officers may be required to physically engage individuals who exhibit conduct ranging from uncooperative to violent behavior. In these situations, officers may have to utilize force to move crowd members who do not respond to verbal directions, control violent individuals, or to effect an arrest. When the

use of force is appropriate in a crowd control situation, only that force reasonable to make an arrest or disperse a crowd should be used.

There are no exceptions to the Department's Use of Force Policy for crowd control situations. Officers may use only that force which is objectively reasonable. Verbalization should be used throughout the operation in an attempt to gain compliance. In determining the appropriate amount of force, officers shall evaluate each situation in light of the facts and circumstances of each particular case, including, but not limited to the seriousness of the crime(s), the level of threat or resistance presented by the individual(s) and the danger to the community.

Baton

The baton may be used to push individuals who do not respond to verbal commands and encroach upon officers on a skirmish line or who intentionally delay departure while officers attempt to disperse the crowd, whether or not a lawful dispersal order has been issued. When an individual's behavior is threatening or violent in nature, the baton can be used as an impact device.

Chemical Agents

The use of any Department approved chemical agent during a crowd control incident requires the approval of a commander or above. Chemical agents include CS gas, CN gas, OC, and all tear gas canisters. Before using any chemical agent, tactical consideration should be given to wind direction, safety equipment for officers, and the potential non-effectiveness of the chemical agent.

Additionally, OC chemical agent may be used to control an uncooperative suspect in an isolated incident when the officer reasonably believes and can articulate that the use of OC was reasonable. This would require a Use of Force Report.

Less-Lethal Munitions

Less-lethal munitions may be deployed as either target specific or non-target specific (dispersal) munitions. Less-lethal munitions can be deployed by Metropolitan Division or specially trained personnel. Both groups may deploy 37mm non-target specific dispersal rounds and the Super-Sock round form a beanbag shotgun as a target specific munitions. Only Metropolitan Division personnel may deploy the 40mm sponge round, and may do so only as target specific munitions.

Reporting a Non-Categorical Use of Force in Crowd Control Situations

In a crowd control situation, a Use of Force Report is not required when officer(s) become involved in an incident where force is used to push, move, or strike individuals who exhibit unlawful or hostile behavior and who do not respond to verbal directions by the police. This applies only to officers working in organized squad and platoon sized units directly involved in a crowd control mission. Additionally, should force be utilized

under these circumstances, officers shall notify their immediate supervisor of the use of force once the tactical situation has been resolved. The supervisor shall report the actions on Incident Command System (ICS) Form 214, or as directed by the incident commander.

A Use of Force Report is required when an officer(s) becomes involved in an isolated incident with an individual during a crowd control situation, which goes beyond the mission of the skirmish line.

Note: When a suspect has been taken into custody, the booking number or DR number of the related report shall be cross-referenced on ICS Form 214.

Medical Treatment

Any suspect taken into custody that has been injured shall receive medical treatment in accordance with established procedures.

CONCLUSION

The police response to each assembly or protest is different and will require flexibility, creativity, discipline, and patience. A non-violent, "sit-down" demonstration requires a much different police response than a violent group who has become destructive. The tactics used to manage or control a crowd should make every attempt to facilitate and protect First Amendment activity while isolating and arresting those engaged in unlawful behavior.

Points to Remember

- First Amendment Rights vs. unlawful behavior
- Keep the peace
- Protect property and vital facilities
- Maintain situational awareness
- Economy of force
- Stop unlawful behavior
- Obtain voluntary compliance
- Remain flexible



CHARLIE BECK
Chief of Police

DISTRIBUTIUN "A"

Attachments: Dispersal Order, Concepts and Strategies, Terms and Definitions

**Crowd Management, Intervention, and Control
Example Dispersal Orders**

DISPERSAL ORDER

"I am (rank and officer's name), a police officer for the City of Los Angeles. I hereby declare this to be an unlawful assembly and, in the name of the people of the State of California, command all those assembled at (give specific location for example, the area bounded by Main Street on the east, Spring Street on the west, City Hall steps on the north, and the south sidewalk of 1st Street on the south) to immediately disperse, which means to break up this assembly. If you do not do so, you may be arrested or subject to other police action. Other police action may include the use of less lethal munitions, which could cause significant risk of serious injury to those who remain. Section 409 of the Penal Code prohibits remaining present at an unlawful assembly. If you remain in the area which was just described, regardless of your purpose in remaining, you will be in violation of Section 409. The following routes of dispersal are available (give the most convenient route(s) of dispersal). You have ___ minutes (give a reasonable amount of time— take into consideration the number of participants, location of the event, and number of exit routes) to disperse."

**DISPERSAL ORDER
(Spanish)**

"Soy (officer's name and rank) oficial de policía de la Ciudad de Los Angeles. Por la presente declaro que esta reunión es ilegal y en nombre del pueblo del Estado de California ordeno que todas las personas reunidas en (give specific location, for example, the area bounded by Main Street on the east, Spring Street on the west, City Hall steps on the north, and the south sidewalk of 1st Street on the south) se dispersen inmediatamente. De lo contrario serán arrestadas o estarán sujetos a otras acciones policíacas. Otras acciones policíacas pueden incluir el uso de municiones de menos lethal, el cual puede causar riesgo significacion de heridas serias a los que permanecen. La Sección 409 del Código Penal prohíbe permanecer en una reunión ilegal. Si usted/ustedes permanecen en las áreas mencionadas, sin importar el propósito de su permanencia, usted/ustedes estarán violando la sección 409 del Código Penal de California. Las rutas que se pueden usar para disperarse son las siguientes: (give the most convenient route(s) of dispersal). Uds tienen ___ minutos (give a reasonable amount of time— take into consideration the number or participants, location of the event and number of exit routes) para dispersarse."

Crowd Management, Intervention, and Control Concepts and Strategies

Lawful Assembly	Isolated Unlawful Behavior	Unlawful Assembly	Riot
<p><i>Free Speech and assembly are protected First Amendment activity. The following are examples:</i></p> <ul style="list-style-type: none"> • Speeches • Marches • Demonstrations • Rallies • Picketing • Public assemblies • Protests • Celebratory events 	<p><i>Isolated unlawful activity by individuals or small groups within a crowd should not automatically form the basis for declaring an assembly unlawful.</i></p> <ul style="list-style-type: none"> • Isolated destruction of property • Isolated acts of violence • Isolated rock or bottle throwers • Individual sit down demonstrators 	<p>407 PC Two or more persons assemble</p> <ul style="list-style-type: none"> • To do an unlawful act or • To do a lawful act in a boisterous or tumultuous manner <p><i>Assemblies may be dispersed when they are: Violent, or pose a clear and present danger of violence, or the group is breaking some other law in the process. If a crime is occurring action may be taken to stop it prior to a Dispersal Order being given.</i></p> <ul style="list-style-type: none"> • Civil Disobedience • Sit down demonstration 	<p>404 PC Riot, (a) Any use of force or violence, disturbing the public peace, or any threat to use force or violence, if accompanied by immediate power of execution, by two or more persons acting together, and without authority of law, is a riot.</p> <ul style="list-style-type: none"> • Group violent behavior • Group acts of property damage
Police Action			
<p>Use Crowd Management strategies:</p> <ul style="list-style-type: none"> • Meet with event organizers and stakeholders • Determine the history and risk of the group • Create a planning team • Check permit limitations • Develop commanders intent • Develop Incident Action Plan and objectives • Identify and assign resources: Video unit, fixed posts, MFF, Bicycle Units, Air Support, TSE, Shadow Teams, Mounted Unit • Monitor and assess crowd behavior • Separate opposing factions • Maintain video log • Provide direction and expectations at roll call • Engender facilitation not confrontation • Ensure the appropriate uniform for the event • Interact with organizers and gain cooperation 	<p>Use Crowd Intervention strategies:</p> <ul style="list-style-type: none"> • Use organizers and monitors to gain voluntary compliance • Isolate, arrest and remove law violators as quickly as possible • Video action of officers and law violators • Use amplified sound (sound trucks or CIUVs) to communicate intent or to gain compliance • Use low profile tactics when possible. Don't become the focus of the demonstration. • Use Passive Arrest Teams, Tangle Teams, Shadow Teams, Cross Bows, Arrest Circles • When it is not possible to make an arrest, use the following strategies: <ul style="list-style-type: none"> • Use the appropriate less lethal munitions to defend officers or to disperse the crowd • Ensure only reasonable force • Report use of force and munitions • Restore traffic flow • Continue to assess; escalate and deescalate as behavior changes • Don't increase crowd tension or change crowd focus to law enforcement by unnecessary aggressive appearance or behavior 	<p>Use Crowd Control strategies:</p> <ul style="list-style-type: none"> • Obtain voluntary compliance • Video action of officers and law violators • Act quickly • Request resources (MFF) • Put control forces in place • Identify dispersal routes • Put a traffic plan in place • Move media to protected area. Use amplified sound (sound trucks or CIUVs) to communicate intent to declare an unlawful assembly • Disperse unlawful crowd • Arrest individuals who fail to disperse or who are involved in illegal activity • Use Arrest Links to move arrestees • With appropriate approval, deploy the appropriate less lethal munitions to defend officers or to disperse the crowd • Ensure only reasonable force • Report use of force and munitions • Restore traffic flow 	<p>Use Crowd Control strategies:</p> <ul style="list-style-type: none"> • Video action of officers and law violators • Immediately stop the behavior • Request resources (MFF) • Put control forces in place • Stop the illegal activity • Put a traffic plan in place • Arrest law violators • Use Arrest Links to move arrestees • With appropriate approval, deploy the appropriate less lethal munitions to defend officers or to stop violent behavior or property damage • Ensure only reasonable force • Report use of force and munitions • Restore and maintain order • Restore traffic flow • Discourage groups from forming • Protect lives, property, and vital facilities • Establish and patrol divisions • Remain present • Reassess the situation • Return to normalcy • Act quickly

Crowd Management, Intervention, and Control Terms and Definitions

Active Resistance: To intentionally and unlawfully oppose the lawful order of a peace officer in a physical manner.

Arrest Links: A method of linking multiple arrestees together for control purposes.

Arrest Protocol: The formal process of placing subjects under arrest, taking into custody, and associating the arresting peace officer(s) with the specific individual arrested.

Arrest Teams: Personnel assigned to arrest duties during civil disobedience/civil disorder operations.

Booking Teams: Personnel assigned to custodial and processing duties during civil disobedience/civil disorder operations.

Civil Disobedience: An unlawful event involving a planned or spontaneous demonstration by a group of people.

Civil Disorder: An unlawful event involving significant disruption of the public order.

Collective Behavior: The unlawful behavior of a group of persons involved in situations where normal cultural structure and controls are not observed, such as unruly crowds, civil disobedience, and riots.

Command: The authority a person lawfully exercises over subordinates by virtue of his/her rank and assignment or position.

Compliance Techniques: Reasonable, lawful use of force methods intended to encourage suspect cooperation.

Control Devices: Devices intended to assist peace officers in gaining control of subjects who refuse to submit to lawful authority (e.g., batons, TASER, restraints, chemical agents, etc.).

Cordoning: Surrounding or enclosing a particular problem area; also referred to as perimeter control.

Critical Facilities: Any location essential to the well-being and safety of the community requiring law enforcement protection during a critical incident.

Crowd: A number of persons collected into a close body.

Crowd Control: Law enforcement response to a pre-planned or spontaneous event, activity or occurrence where there is a potential for unlawful activity or the threat of violence.

Crowd Dynamics: Factors which influence crowd behavior.

Crowd Intervention: Strategies and tactics employed by law enforcement during lawful assemblies to address unlawful activity, civil disorder, and to arrest violators.

Crowd Management: Strategies and tactics employed by law enforcement to manage lawful assemblies in an effort to prevent the escalation of events into an unlawful assembly or riot.

Decontamination: Procedures taken to reduce the effects of any non-lethal chemical agent.

Discipline: Pattern of behavior consistent with demonstrating self-control, teamwork, moderation, and restraint.

Dispersal Order: Lawful orders communicated by law enforcement personnel commanding individuals assembled unlawfully to disperse.

Flashpoint: Specific location(s) which can be anticipated to attract criminal elements and become the origin or focal point of civil disorder.

Force Options: Reasonable force applications utilized by law enforcement to effect arrest, overcome resistance, and prevent escape.

Crowd Management, Intervention, and Control Terms and Definitions

Formations: Coordinated unit tactics utilized by law enforcement to control crowds, stop unlawful activity, and disperse and/or arrest violators.

Incident Command System (ICS): The statewide model for field level management of emergencies mandated by the Standardized Emergency Management System (SEMS). ICS is specifically designed to allow its users to adopt an integrated organizational structure equal to the complexity of demands of single and multiple incidents without being hindered by jurisdictional boundaries.

Less-Lethal Impact Munitions: Projectiles launched or otherwise deployed for purposes of overcoming resistance, preventing escape, effecting arrest, reducing serious injury and are without significant likelihood of causing death.

Management: The process of planning, organizing, coordinating, directing, budgeting, and controlling resources.

Mobile Arrest and Booking Teams: Mobile teams designated to assist field personnel with mass arrest and booking.

Mobile Field Force: An organized, mobile law enforcement tactical force equipped and trained to respond to unusual occurrences. The Mobile Field Force configuration is currently the statewide standard known as "Mutual Aid Response Mobile Field Force."

Mobile Tactics: specialized techniques that give Mobile Field Force (MFF) personnel the ability to respond rapidly and complete high-risk missions beyond the capabilities of other personnel. The vehicles may also be utilized for crowd control and containment.

Mob: A disorderly group of people engaged in unlawful activity.

Mounted Tactics: Tactics while mounted on horses.

Non-Compliant Behavior: Behavior which does not yield to a lawful order.

Non-Lethal Chemical Agents: Devices utilized by law enforcement agencies which may include CS, CN or OC.

Non-Target Specific Less-Lethal Impact Munitions: Less-lethal munitions fired at a crowd for the purpose of crowd control and/or dispersal (37mm, 20F Multiple Foam Rubber Projectiles).

Pain Compliance: The stimulation of nerves or the manipulation of joints to elicit a sense of unease or distress in a subject, causing that subject to comply. Examples include control holds, impact weapons, non-lethal chemical agents, TASER, etc.

Passive Arrest Teams (PAT): Organized teams of peace officers assigned to take "passive arrestees" into custody.

Passive Resistance: A commonly used term referring to non-violent opposition to the lawful directions of law enforcement during arrest situations.

Photographic Teams: Law enforcement photographers assigned to document designated activity involving civil disobedience.

Platoon: A tactical component consisting of two or more supervised squads.

Policy: Statements of principles and values which guide the performance of a specific Department activity. Policy establishes limits of action and reflects a statement of guiding principles that should be followed in order to achieve an agency's objective.

Procedure: A method of performing an operation, or a manner of proceeding on a course of action, within limits of policy.

Public Disruption: The interruption or disturbance of public order.

Crowd Management, Intervention, and Control Terms and Definitions

Shadow Team: A squad sized plain clothes unit made up of [REDACTED] each having a supervisor that is responsible for working within crowds to identify individuals involved in illegal behavior, and when possible monitor their behavior, and/or arrest and remove them from the crowd as quietly as possible.

Uniformed Shadow Support Team: A squad of [REDACTED] and two supervisors that are responsible for coordinating with, and supporting Shadow Teams.

Stakeholder: Entities having a legal, professional, economic or community interest/responsibility in the event.

Standardized Emergency Management System (SEMS): A system required by the California Government Code for managing response to multi-agency and multi-jurisdictional emergencies in California. SEMS consists of five organizational levels that are activated as necessary: Field Response, Local Government, Operational Area, Region and State.

Target Specific Less-Lethal Impact Munitions: Less-lethal munitions fired at a specific/identifiable target for purpose of selectively and temporarily incapacitating an individual or to cause the individual(s) to stop aggressive/combative actions: 12-gage Super-Sock Projectiles; 40mm Exact Impact Sponge Munitions (Metro)

- Aggressive/Combative actions: Unlawful behavior (must include actions/movements)
- "Objectively" confrontational
 - Physical attacks on persons/public safety
 - A fighting disposition, i.e., clenched fist; threats of violence coupled with "reasonable" ability to carry out threat
 - Behavior (more than "stoic or uncooperative")
 - Destruction of property

Unlawful Assembly: Penal Code Section 407 defines an "unlawful assembly" as: "Whenever two or more persons assemble together to do an unlawful act, or to do a lawful act in a violent, boisterous or tumultuous manner, such assembly is an unlawful assembly." "Boisterous or tumultuous manner" has been interpreted by the courts to mean conduct which poses a clear and present danger of imminent violence.

Statement of

**Michael P. Downing
Commanding Officer
Counter-Terrorism/Criminal Intelligence Bureau
Los Angeles Police Department**

Before the

**Committee on Homeland Security's and Governmental Affairs
United States Senate**

Presented on

October 30, 2007

I. Introduction

Chairman Lieberman, Ranking Member Collins, and Members of the Subcommittee, thank you for the opportunity to discuss the Los Angeles Police Department's (LAPD) efforts to identify and counter violent extremism, which happens in this case, to be ideologically based.

Local law enforcement has a culture and capacity that no federal agency enjoys - the know-how and ability to engage communities that today are a vital part of the equation. Part of this engagement process is the demonstration of sensitivity to terminology that offends and/or isolates communities, hence, "*Ideologically Based Violent Extremism.*"

No agency knows their landscape better than local law enforcement; we were designed and built to be the eyes and ears of communities – the First Preventers of terrorism. What is important to law enforcement is that we carefully and accurately define those who we suspect will commit a criminal-terrorist act within our communities. That job needs to be done with the kind of balance and precision that inspires the support and trust of the American people in order to aid us in the pursuit of our lawful mission.

Prior to 2001, much of America overlooked Muslim communities in the United States (U.S). Iranians who immigrated to the U.S. following the hostage crisis received some media attention but the broader Muslim community in this country was not at the forefront of the national psyche. The reverse is now true as a result of the post-9/11 media coverage and the wars in Iraq and Afghanistan. Muslim communities here and abroad have become centerpieces of coverage for the print and broadcast media. While this coverage has, in many cases, helped to educate the American public, it has also put Muslims under a very bright spotlight. Feelings of persecution and vulnerability by large swaths of Muslim communities have created anxiety and uncertainty about the future.

Before 9/11, law enforcement was equally unaware of this community, both at a federal and statewide level. Even with our newfound awareness, law enforcement personnel are working from a disadvantage because of the obstacles we face as we approach wary communities deeply concerned with issues such as the implications of the Patriot Act, racial-profiling in the transportation industry, and the mischaracterization of Islam in the media. High-profile arrests and investigations of violent extremists such as the Fort Dix 6 play into Muslims' fears that they are under increased scrutiny. These underlying dynamics play a role in how these communities interact with all facets of American society, especially law enforcement.

One major role that law enforcement can play in the fight against violent ideological extremism is that of educator. Teaching all communities about the dangers of extreme ideologies can dispel harmful rumors and myths that alienate already pressured communities. We have learned from the European experience how these alienated communities become a breeding ground for violent extremism and a safe haven for potential terrorists to hide among the population.

Granted, the U.S. does not have the same types of problems as England, France, Germany, or Israel. While the tactics terrorists employ are learned behaviors that migrate across national boundaries – through groups, training camps, and the Internet – the underlying motivations for

these violent acts are unique to the host countries. Consequently, the remedies (i.e., jailhouse de-radicalization in Malaysia, the Channel Project in northern England, and the BIRR Project in Australia) are often contextually bounded and dependent on the depth, strength, national allegiance and identity of the native Muslim community.

In Los Angeles, for example, there are many Muslim communities that do not share the same risk profile as those in the United Kingdom as they are much more integrated into the larger society. That said, the European example does provide U.S. law enforcement with a starting point when searching for early indicators of radicalization.

We have learned that Muslim communities in the U.S. are mistrustful of the mainstream media. Therefore, they may turn to other sources of information for news and socialization, such as the Internet. Unfortunately, despite all of the positive aspects of the Internet, it allows those individuals and groups with ideological agendas to easily make contact with like-minded individuals and access potentially destructive information.

As we move from the virtual to the physical, it is important to apply the hard-won lessons we have learned in combating gang crime to the problem of terrorism. Southern California was the birthplace of gang culture and in Los Angeles we are all too familiar with the threat of violent crime by street gangs. Regardless of how many police officers we deploy, we can only suppress specific incidents. While more police are part of the answer, the real solution lies in the community – with the strengthening of the family structure and the economic base; and the weakening of political power bases built on victimization and a cultural tolerance of violence. The problem of violent street gangs is based on deep community structures. However, so are the solution sets of youth-at-risk programs, parenting classes, economic infusion, job training, community activism against violence and religion-based interventions.

While it might seem counter-intuitive, the isolation of Muslim communities acts both as a wall and as a self-regulator. Similar to gangs, the signs of extremism are first seen on the most local levels: in the families, neighborhoods, schools, mosques, and work places. The wall built by the community is the barrier created to sustain cultural identity and values and protect against the pace of assimilation.

II. LAPD Strategies and Initiatives

One of the biggest challenges for law enforcement in this environment is separating political jihadists (i.e., those who intentionally plant seeds of division in an effort to alienate and isolate Muslim citizens from the rest of society) from legitimate actors. Teaching all communities about the dangers of extreme ideologies can dispel harmful rumors and myths that alienate already pressured communities. The LAPD has done much outreach in this area, both with Muslim and non-Muslim communities. For the 18 months, we have been involved in outreach and grassroots dialogue with Muslim communities, bringing the entire command staff to observe, learn, engage and, most importantly, listen. This has helped to build more robust trust networks at the divisional level of police service. One of our goals is to be viewed as trusted friends by Muslim communities in our city.

Our outreach to the non-Muslim community has combined education with prevention. We now have Terrorism Liaison Officers (TLOs) at all of our divisions and Fire Stations who serve as the principal points of contact for terrorism information and intelligence. These liaison officers educate Department personnel and the broader community about the indicators of violent extremism and have proven to be critical assets when it comes to raising the level of terrorism prevention and preparedness.

The education provided by the TLOs has been supplemented with training by outside experts. Within our ranks, we have worked to educate our officers in the Counter-Terrorism and Criminal Intelligence Bureau about Islam and the cultural sensitivities they should be aware of when they are in the field. Approaching Muslims with respect and integrity is a large piece of the counter-narrative that law enforcement can write for itself.

The LAPD must have the capability to hunt for signs of radicalization and terrorism activities on the Internet. We recently started a cyber investigations unit to do just that. The Internet is the virtual hangout for radicals and terrorists. It provides a plain-view means of identifying and gathering information on potential threats. Information gleaned from this open source, fed into the radicalization template, and combined with a thorough understanding of operational indicators, is critical to articulating suspicion and justifying the increased application of enforcement measures.

LAPD's Counter-Terrorism and Criminal Intelligence Bureau initiatives for both the present and future have aligned people, purpose, and strategy around the mission of building capacity to hunt and disrupt operational capability on the part of terrorists (recruiting, funding, planning, surveilling, and executing operations). However, just as important, we have aligned our resources to focus on the motivational side of the terrorist equation and have made great efforts and organizing, mobilizing and in partnership, raising the moderate Muslim voice to prevent the extremists from making inroads into this faith community. A few of these strategies are described below:

- Working in concert with our seven county regional and federal partners, we continue to build capacity to collect, fuse, analyze, and disseminate both strategic and operational intelligence. We are aligning our intelligence collection and dissemination process with an eye toward accountability and ensuring that our First Preventers have the information they need when they need it.
- Our Terrorism Liaison Officers are casting an ever-wider safety net to train more people in the city to be public data collectors and First Preventers.
- We have started a Muslim outreach program with our command staff to leverage resources, institutionalize the idea of developing the counter-narrative, and facilitate an educational process. In developing this counter-narrative, the goal is to inspire Muslim communities to responsibly partner with law enforcement to protect American values. We also aim to elevate the moderate Muslim voice and empower people to counter the extremist ideology with confidence. This enables community

leadership to assist law enforcement in identifying those individuals and groups who espouse extremism and work to divide Muslim communities from American society.

- We are working with a think tank to develop a training program for mid-level executives that will be tailored specifically to state and local law enforcers. It is our hope that this will develop into a model for a national counter-terrorism academy.
- We initiated the Regional Public Private Infrastructure Collaboration System – a tool that enhances communication between and within LAPD and the Private Sector.
- Our Archangel program is a Critical Infrastructure Protection System that includes a Protective Security Task Force.
- We are developing a Cyber Investigation Unit to hunt violent extremists on the Internet.
- Our Community Mapping project is described below in Section V.

III. A Different Problem

In contrast to much of Europe, which has suffered from a marked increase in violence and violent intentions – often by its own citizens, the problem we face in the U.S is mainly political. There are those among us, I call them political jihadists, who are attempting to create division, alienation, and a sense of persecution in Muslim communities in order to create a cause. They are the nemesis of community engagement. Their purpose is to create the conditions that facilitate the radicalization process for international political causes.

Law enforcement's *ultimate* goal is to engender the continued loyalty and good citizenship of American-Muslims – not merely disrupt terrorist activities. Let me be clear, I am not saying that law enforcement should relax its effort to hunt down and neutralize small numbers of “clusters” on the criminal side of the radicalization trajectory. That task remains, and must be done with precision and must also be carried out in the context of what is ultimately valuable. What good is it to disrupt a group planning a mall bombing if the enforcement method is so unreasonable that it is widely criticized and encourages many more to enter the radicalization process?

The point is not merely an academic one—it has operational consequence. In preserving good will and by in by Muslim communities, law enforcement is, in fact, advancing its intelligence agenda by fostering an environment that maximizes tips and leads surfacing from those same communities. The long-term solution to this radicalization problem will come from Muslim communities themselves.

The natural question is: What factors put a community at-risk? Taking a page from the European experience, diaspora communities are in transition from one culture to another, making its members particularly vulnerable to identity crises which may be very easily subverted by ideologues. As Eric Hoffer wrote in his book, “The True Believer: Thoughts on the Nature of

Mass Movements”: “Faith in a holy cause is to a considerable extent a substitute for the lost faith in ourselves.” If there is a real or perceived threat of discrimination between the new community and the host, then an “us against them” mentality may prevail making that final step towards radicalization that much easier. Some Muslim communities may view any local discrimination as linked to Muslim causes globally, and vice versa, any discrimination against the *Ummah* (the global Muslim community) may be felt locally.

The Pakistani-British community in the United Kingdom is a diaspora, which is significant, because it makes the 2nd and 3rd generations of the community particularly vulnerable to the social pressures of growing up in a country very different from their parents’ and grandparents’ homeland. As a diaspora community, they remain transnational, tending to maintain close family, social, and financial ties with Pakistan. Globalization allows a diaspora to maintain these transnational contacts via faster, cheaper air travel, global communications technology (Internet and cell phone), global mass media, and nearly instant transnational banking. If the first two risk factors are present, then one must ask, “Does the community also hail from an unstable homeland with Wahabbi-Salafi ties?” If so, that community, like the British-Pakistani Muslim community, might be at greater risk of incubating homegrown radicalization.

If social factors - such as enclaves where residents are culturally and linguistically isolated - contribute to radicalization, it is important for law enforcement to be aware of those potentially vulnerable communities. This is part of our next step. We want to map the locations of these closed, vulnerable communities, and in partnership with these communities, infuse social services that will help the people who live there while weaving these enclaves into the fabric of the larger society. While the role of the law enforcer is not one of religious scholar or social worker, there is the potential to build and strengthen bridges from communities to those resources. It is then we will know where to find our Pakistani, Iranian, Somali, Chechen, Jordanian, and North African communities and thus understand how better to support their integration into the greater society. It is then that local law enforcement becomes an enabler.

IV. Legitimacy and Constitutionality

It is our position that legitimacy and intelligence are equally important tools for U.S. law enforcement to use in counter-terrorism efforts. Legitimacy starts with an organizational knowledge and pride in operating constitutionally and within the law. The need for transparency – being perceived to be and authentically honoring this principle – in intelligence and counter-terrorism activities cannot be understated. Taking great care to ensure that intelligence and enforcement operations are narrowly targeted against terrorist cells determined to go operational is critical. Law enforcement and its advocates must also avoid name-calling exchanges with political jihadists, opting instead to engage them professionally on specific issues. Political jihadists will reveal themselves in these exchanges by being unreasonable and unable to articulate specific grievances, preferring instead to use personal attacks and blanket accusations. In doing so, they are failing in their purpose to attract converts.

Community policing initiatives in Muslim communities should aim to create a shared sense of threat: society as a whole fears the indiscriminate, mass violence we are seeing around the world. All forms of communication with the public (whether analytical reports or post-incident news conferences) should address this fear. In summary, law enforcement’s most pressing

challenge is to shield the public from this threat, while not advancing the purpose of political jihadists. It is a difficult balance to achieve, however, raising the moderate Muslim voice and creating the counter-narrative that offsets the fanatical trajectory of radicalization.

The LAPD has created the Counter-Terrorism and Criminal Intelligence Bureau with nearly 300 officers who are solely dedicated to counter-terrorism, criminal intelligence gathering, and community building. Policing terrorism must be a convergent strategy that enhances the fight against crime and disorder. In building the resistance to crime and disorder, we create hostile environments to terrorists.

V. Community Mapping

We need to understand the problem as it exists in Los Angeles before we roll out programs to mitigate radicalization. Historically, the temptation has been to turn to intervention programs before we have clearly identified problems within the community. In the past we have relied on interventions based on "experts," logic or previous programs that are either generic or insensitive to the constellation of issues. This has consistently produced unremarkable results. Public safety pays a high cost for this business practice. This is one of many reasons to support the rationale behind community mapping, a process that delivers a richer picture and road map that can guide future strategies.

In order to give our officers increased awareness of our local Muslim communities, the LAPD recently launched an initiative with an academic institution to conduct an extensive "community mapping" project. We are also soliciting input of local Muslim groups, so the process can be transparent and inclusive. While this project will lay out the geographic locations of the many different Muslim population groups around Los Angeles, we also intend to take a deeper look at their history, demographics, language, culture, ethnic breakdown, socio-economic status, and social interactions. It is our hope to identify communities, within the larger Muslim community, which may be susceptible to violent ideologically-based extremism and then use a full-spectrum approach guided by an intelligence-led strategy.

Community mapping is the start of a conversation, not just data sets: It is law enforcement identifying with its community and the community identifying with its families, neighborhoods, city, state, country and police. For the past 18 months, the LAPD's outreach and grassroots dialogue with Muslim communities has helped the entire command staff to observe, learn, engage and, most importantly, listen. This has helped to build more robust trust networks at the divisional level of the police service area.

Without a community mapping blueprint and methodical community engagement strategy, our outreach efforts will be sporadic. Our counter-narrative will be empty of meaning, leaving us talking about, rather than talking with, this community.

VI. Conclusion – The Evolving Threat

We need to show that our democratic principles built on the values, practices, and lives of American citizens are sacred and worthy of embracing. We need to show our belief in human dignity, the family and the value of the individual. We need to show how we honor the meaning of our lives by what we contribute to others' lives. We need to show that behind the badges of American law enforcement are caring Americans “doing” law enforcement. To do this we need to go into the community and get to know peoples' names. We need to walk into homes, neighborhoods, mosques, and businesses. We need to know how Islam expresses itself in Los Angeles if we expect to forge bonds of community support. The LAPD has been involved in this process and we are now ready to evolve our outreach to a more sophisticated and strategic level.

The U.S. faces a vicious, amorphous, and unfamiliar adversary on our land. The principal threats will be local, self-generating and self-directed. If there are direct connections with overseas groups, these are most likely to be initiated by the local actors. Cases in point include the 7/7 bombers, the Glasgow car bombers, and, more locally, Lodi in which local individuals and groups sought out training in Pakistan. This is not intended to dismiss threats that emerge from overseas locations, which should continue to be of concern. Rather, it is an estimate of relative density—locally generated threats will manifest themselves with greater frequency.

Ultimately, preventing extremism will be up to neighborhoods and communities, but thread by thread, relationship by relationship, the police can help build a network of services and relationships that will make it very hard for terrorism to take root. American Muslim neighborhoods and communities have a genuine responsibility in preventing any form of extremism and terrorism. If the broader communities are intolerant of such things, these ideologies cannot take root in its midst. I believe no amount of enforcement or intelligence can ultimately prevent extremism if the communities are not committed to working with law enforcement to prevent it.