

*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.<sup>1</sup> 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.<sup>2</sup> 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.

---

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

<sup>2</sup> 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.

<b>LEVELS OF INTELLIGENCE INVESTIGATION ACTIVITY</b>			
	<b>INITIAL LEAD</b>	<b>PRELIMINARY</b>	<b>OPEN INTELLIGENCE</b>
<b>Source of Information</b>	Other law enforcement agencies, private citizen, departmental employees	Same as Initial Lead	Same as Initial Lead
<b>Required Threshold for Opening Investigation</b>	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.
<b>Approval Level</b>	Detective III	Commanding Officer, MCD	Commanding Officer, MCD
<b>Investigative Techniques</b>	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.
<b>Time Limit for Completion</b>	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.<sup>3</sup> 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.

---

<sup>3</sup> 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.<sup>4</sup> 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.

---

<sup>4</sup> 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 calendar 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.