LOS ANGELES POLICE COMMISSION

SUSPICIOUS ACTIVITY REPORTING SYSTEM AUDIT

Conducted by

OFFICE OF THE INSPECTOR GENERAL

ALEXANDER A. BUSTAMANTE
Inspector General

March 12, 2013

OFFICE OF THE INSPECTOR GENERAL
SUSPICIOUS ACTIVITY REPORT AUDIT
2012

PURPOSE OF REVIEW

The Office of the Inspector General has completed its Suspicious Activity Report Audit (Audit). The purpose of this Audit was to test for compliance with Special Order No. 1, 2012, Reporting Incidents Potentially Related to Foreign or Domestic Terrorism – Revised and Renamed.

BACKGROUND

In March 2008, the Los Angeles Police Department (LAPD or Department) published Special Order No. 11, Reporting Incidents Potentially Related to Foreign or Domestic Terrorism, to address the gathering, reporting and analysis of information that could indicate activity or intentions related to foreign or domestic terrorism. In the Special Order, the Department wrote that law enforcement officers fill a critical position in the area of terrorism prevention and that law enforcement must carry out their counter-terrorism responsibilities within the broader context of their core duties. Under this philosophy, the Department established a policy for investigating and reporting crimes and non-criminal incidents of potential foreign or domestic terrorism. The Special Order went on to state that in the Department's effort to carry out its responsibility, the Department must do so in a manner that protects the information privacy and legal rights of Americans.

Special Order No. 11, 2008, established a Suspicious Activity Report (SAR) to document reported or observed activity or a criminal act which an officer believed had a nexus to foreign or domestic terrorism. The SAR information was recorded on the Department's Investigative Report form. Although the information reported in a SAR could result from observations of police officers or community members, a report was only prepared if the observations related to 1 of the 41 incidents defined in the Special Order as suspicious activity.

Once completed, the SAR was forwarded to the Area watch commander for review and approval. If the SAR sufficiently described 1 of the 41 suspicious activities, the watch commander approved the report and obtained a Division of Records (DR) number.[1] The original report was then sent to Major Crimes Division. Major Crimes Division was given the responsibility to manage the reports created by the Special Order. In May 2008, the Analysis Unit was established within Major Crimes Division to undertake that task. The Special Order specifically prohibited copies of a SAR from being maintained at the Area police stations.

The Department amended this policy in January 2012, with Special Order No. 1, Reporting Incidents Potentially Related to Foreign or Domestic Terrorism – Revised and Renamed. The Special Order resulted in two notable changes. First, the number of distinct activities or behaviors that define suspicious activity was reduced from 41 to 16.[2] The reduction allows the

[1] DR numbers are assigned from the Consolidated Crime and Arrest Database (CCAD).

[2] The 16 defined suspicious activities and/or behaviors are defined in the attached Addendum.

Department to better align its policies with federal guidelines.[3] Secondly, the Department records suspicious activity on a SAR instead of the more generic Investigative Report form.

The Special Order further redefines the reporting requirements of a SAR. A SAR should only be prepared when there are articulable facts and circumstances that support the suspicion that the behavior was reasonably indicative of suspicious activity associated with terrorism.[4] The Special Order specifically prohibits Department personnel from using an individual's race, color, religion, national origin, gender, age, physical or mental disability, marital status, sexual orientation, gender identity, gender expression, creed, ancestry or medical condition as factors that create suspicion.

Either an officer or a community member can initiate a SAR. When a community member witnesses what they believe to be suspicious activity, that individual can report that activity directly to the Area station, call the Department's hotline or submit information via the internet. In an effort to educate the public on suspicious activity reporting, the Department created a community awareness program called iWatch. This program is designed to educate community members on the behaviors and activities that may have connections to terrorism.

When a SAR is reported, the watch commander (WC) will make a determination on whether the information obtained warrants a SAR designation. If the WC determines that a SAR is appropriate, the case is immediately assigned a DR number. From this point forward, the SAR is tracked in the Department's database.[5] The database will capture all entries into the system, to include the date, time and location of the suspicious activity, the officer completing the report, the community member reporting the observation and the individual(s) engaged in the suspicious activity or behavior, if known.[6]

Most of the information entered into the DR database is automatically transferred to the Major Crimes Division's SAR database.[7] The personal information related to suspected individuals, however, is not automatically entered into the SAR database. The individual's personal information is not entered into the SAR database until a specialized unit, named the Analysis

[3] Federal guidelines refer to the Office of the Department of National Intelligence (ODNI). The Office of the Department of National Intelligence is a federal agency which oversees and directs the carry out of the National Intelligence Program for the collection, analysis, production and sharing of national intelligence.

[4] Reasonably indicative is defined as the totality of the circumstances in which creates in the mind of the reasonable observer an articulable concern that the observed behavior is terrorism-related. It also takes into account the training and experience of a reasonable law enforcement officer, in cases where an officer is the observer.

[5] The DR number database is the same that tracks crime and arrest reports.

[6] Special Order No. 1 defines an involved person as an individual that has been observed engaging in suspicious activity, when no definitive criminal activity is identified, thus precluding their identification as a suspect.

[7] SAR information is maintained in the Memex database. Memex Inc. is a worldwide provider of intelligence management and analysis solutions which provides the Major Crimes Division the ability to gather, analyze, track and disseminate intelligence information collected in the SARs.

Unit, has determined that the SAR satisfies the requirements of Special Order No. 1.[8] If the requirements are met, the Analysis Unit personnel will enter the descriptive information into the database and the information is then forwarded to the federal government where it may be shared with various intelligence agencies.[9]

If the requirements are not met, the LAPD does not share the data with any outside law enforcement or governmental agencies. The Department also removes the data from the Department's SAR database. The data, however, is still retained in the Department's DR database. The Records and Identification Division and the Major Crimes Division also maintain copies of these reports. The Department is currently recommending that the SARs reports, regardless whether the SAR met Department criteria, be retained for 10 years.

Community Involvement

During the planning phase of the Audit, the Office of the Inspector General met with various community members and groups to discuss their concerns with Special Order No. 1, 2012. During these discussions, the OIG learned that many community members were, among other things, interested in knowing under what circumstances individuals were contacted, how often such contacts were made, how these individuals were selected, and what the Department did with the information they gathered. The OIG attempted to incorporate many of these concerns into its audit plan and then began assessing the Special Order to determine whether the policy was being fairly and justly implemented.

The OIG examined the statistical information surrounding the Department's SARs program in an effort to identify patterns or trends in the issuance of SARs. Specifically, the OIG examined SARs within the four-month period of February 1 to May 31, 2012. During this period, the Department processed 78 SARs.[10]

The OIG determined that 36, or nearly half, of the 78 SARs were initiated in West Bureau. West Bureau includes Hollywood, Wilshire, West Los Angeles, Pacific and Olympic Areas. In contrast, Valley, Central and South Bureaus had 20, 16, and 6 SARs, respectively. After its review, the Analysis Unit concluded that 10 of the SARs failed to meet the established criteria as defined in Special Order No. 1, 2012 and were eliminated from further processing. The OIG verified that all data from these 10 SARs was removed from the SAR database.

---

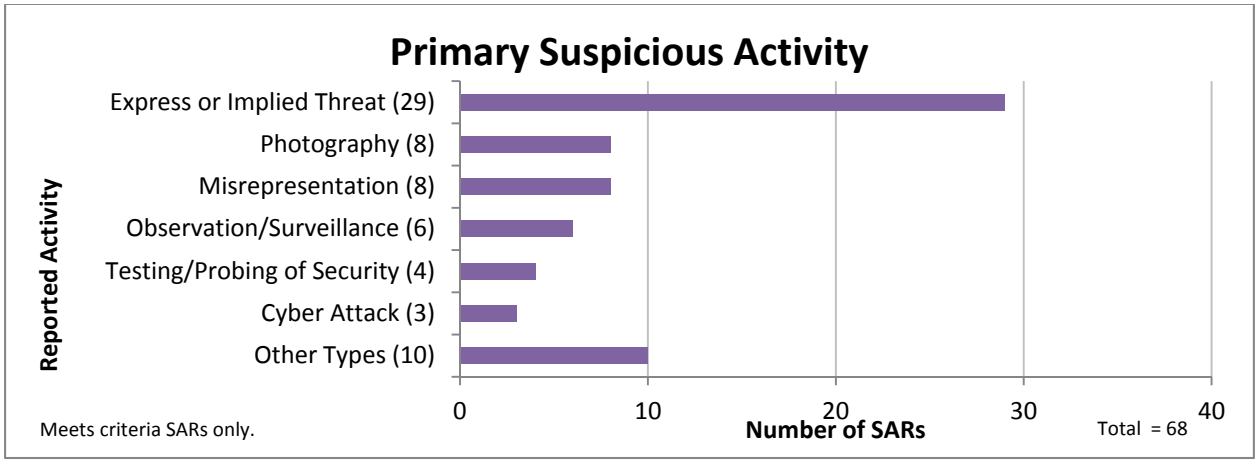
[8] Personal information used to identify an individual may include descriptors such as name, license plate, date of birth, moniker, address and driver license. These elements appear in the involved persons fields within the body of the SAR and are subject to privacy protection based on the ODNI Functional Standards.

[9] Federal government refers to the Joint Regional Intelligence Center. The Joint Regional Intelligence Center is a center for collaboration between federal, state and local law enforcement to integrate terrorism threat intelligence and dissemination of that information. SARs are accepted by the Joint Regional Intelligence Center if they meet the ODNI functional standards.

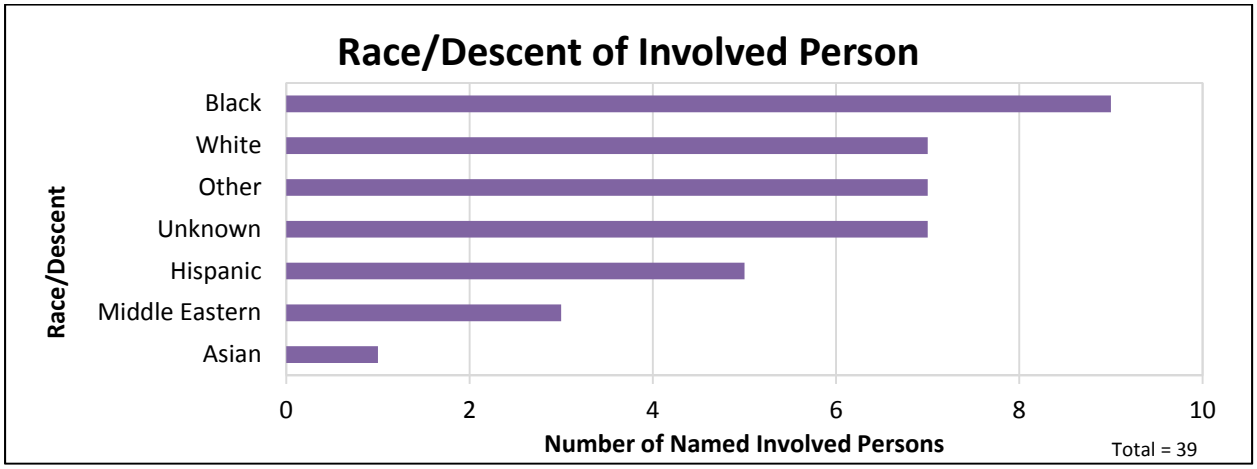
[10] As a SAR is tracked by the Department only after its approval by a watch commander and subsequent assignment of a DR number, the OIG was unable to determine the total number of suspicious activity calls received by the Department.

Each of the 68 remaining SARs was treated as meeting the criteria of suspicious activity, which resulted in the Department ultimately sharing the documented information with the Federal government. However, each SAR did not necessarily identify an involved person, whereas some SARs identified more than one individual. In all, 33 SARs had at least one named involved person with a total of 39 individuals named.

Although the Special Order identifies 16 defined activities and behaviors that may reveal a nexus to foreign or domestic terrorism, one category (an "expressed or implied threat") accounted for more than 40 percent of the reported incidents as depicted in the following chart:[11]



The SAR database contains involved person(s) data for each applicable SAR as described by the reporting officer or community member. A community member was the original reporting party for 27 of the 33 SARs containing named involved persons, 2 of which were received via the iWatch program. Based on the descriptions provided in the SARs, the following information was established:



[11] Political expression does not meet the ODNI functional criteria for a SAR and therefore, no SARs were generated based on those criteria.

Although 33 SARs contained named involved persons, officers had direct contact with an involved person in just 15 instances. Six officer contacts resulted from a traffic enforcement stop. Three of the contacts stemmed from consensual encounters, although not all of the reports clearly articulated the actions and conversations leading to the contact. The remaining contacts adequately described circumstances in which the officer had reasonable suspicion to initiate a contact with the individual.

Although the Audit selected and reviewed SARs generated within a specific four month period of 2012, some calendar year totals included:

- SARs: 322
- SARs Unfounded: 32[12]
- SARs investigated: 290
- Arrests for crimes associated with a SAR: 19[13]

To address the educational component necessary to keep officers apprised of current SAR policies and procedures, the Analysis Unit has established a SAR training program. To accomplish this training, an officer at each Area station has been appointed to work with the Analysis Unit. Together, training is provided at roll call and detective divisional training days as well as through Information Bulletins and training videos. The training is provided to officers, supervisors, watch commanders and commanding officers.

METHODOLOGY AND SCOPE

Special Order No. 1, 2012, was used as the standard for testing the SAR process for compliance. The OIG judgmentally selected the four-month period of February 1 to May 31, 2012, as the testing period.[14] During that period, the Department generated 78 SARs. The OIG included all 78 SARs in its testing sample. In addition to its testing, the OIG conducted interviews of Department personnel to obtain an understanding of the controls and related risks surrounding the SAR process. The Audit scope included two objectives with various tests to address each objective.

The OIG conducted this Audit in accordance with generally accepted government auditing standards. These standards require that the Audit is adequately planned, performed, and supervised, and that sufficient, appropriate evidence is examined to provide a reasonable basis for the results and conclusion.

[12] An Unfounded SAR is defined as: The crime or incident alleged in the original report did not occur; the same crime or incident has been reported more than once; or, the incident described in a SAR did not meet the ODNI Functional Standards guidelines.

[13] Arrests were related to criminal threats, bomb threats and explosives.

[14] The Commission approved a revision to Special Order No. 1, 2012 on August 28, 2012, (Special Order No. 17) causing the Department Manual to be revised (Manual Section Volume IV Section 271.46).

SUMMARY OF AUDIT RESULTS

Audit Objectives		Compliance Rates
Objective 1: Determine if each SAR was properly completed		
Test 1	Determine if each SAR was documented as approved by a supervisor.	100% (78/78)[15]
Test 2	Determine if each SAR was assigned a unique DR number.	100% (78/78)
Test 3	Determine if each SAR reported one of the defined suspicious activities.	100% (78/78)

DETAILED METHODOLOGY

OBJECTIVE 1: Determine if each SAR was properly completed.

All 78 SARs were reviewed to determine whether the report was signed as approved with a signature and serial number. To verify that each SAR was approved by a supervisor, the LAPD Deployment Roster was used to reconcile each supervisor's rank at the time of the approval. Each SAR was also reviewed to determine if it was documented with a unique DR number. For those SARs which indicated a related arrest or property seizure, the Arrest Report and/or Property Report was reviewed to ensure that the SAR DR number or information related to the SAR was not included on the associated reports. The SAR was reviewed to determine if there was sufficient information included on the form, such as location, time of day, behavior or activity reported or observed. The SAR was also reviewed to determine if, based on the totality of the evidence, the activity described was reasonably indicative of suspicious activity associated with terrorism. In addition, the OIG engaged in a number of discussions with the Analysis Unit staff regarding the rationale used to support their conclusions.

Objective 2: Determine if each SAR was adequately processed by the Analysis Unit		
Test 1	Determine if each SAR was logged into the SAR Tracking Log.	100% (25/25)[16]
Test 2	Determine if each SAR was date stamped with the date received by the Analysis Unit.	100% (78/78)
Test 3	Determine if each SAR disposition assigned by the Analysis Unit was supported by the evidence.	100% (78/78)
Test 4	Determine if the data from each Unfounded SAR was removed from the Analysis Unit's database.	100% (10/10)[17]

[15] Eleven of the 78 SARs were prepared by the Analysis Unit with 5 received from the Department hotline and 6 received from the iWatch program. The remaining 67 SARs were prepared by police officers.

[16] The OIG judgmentally selected 25 of the 78 SARs for this test.

OBJECTIVE 2: Determine if each SAR was adequately processed by the Analysis Unit.

The OIG judgmentally selected 25 SARs from the total population for testing the logging and tracking system. In each case, the SAR was traced to the Analysis Unit's Daily SARs Log to determine whether the SAR was properly logged. The Analysis Unit's most critical decision is the disposition it assigns to the SAR. The OIG reviewed all 78 SARs to determine whether the policy standards were equally applied and the final disposition was adequately supported by the evidence. The OIG compared the information on the SAR to the information in the SAR database. Additionally, the OIG interviewed the Analysis Unit's staff to determine if they properly considered the specific activity, content of the report, available Department and outside resource information, and the relative potential risk before rendering their disposition. Ultimately, 10 SARs received a disposition of Unfounded. The OIG searched the SAR database for each of the Unfounded SARs to determine if all information had been removed from the database.

MANAGEMENT RESPONSE

The commanding officer of Major Crimes Division expressed general agreement with the findings and recommendations.

RECOMMENDATIONS

The OIG recommends that the Department ensure that all SAR reports thoroughly describe the facts and circumstances surrounding any contact with an individual. The OIG also recommends that all Department personnel reviewing these SARs focus on the circumstances related to the contact to ensure that all contacts are constitutional.

The OIG recommends that the Department maintain all SARs in a secure location and restrict access to these reports. The Department should record each time these documents are viewed. This recording log should include the time and date the documents were accessed, the individuals viewing these documents, and a detailed reason for examining these documents. These controls should be maintained in such a manner as to allow for periodic auditing by the OIG and Department auditors.

CONCLUSION

The OIG found the Department to be in compliance with Special Order No. 1, 2012. Furthermore, the OIG concluded that the Analysis Unit properly assessed each SAR in the OIG's sample to determine if there was a potential nexus to terrorism before sharing the gathered information with any outside governmental entity. Of the 78 SARs reviewed, the Analysis Unit determined that 68 had a potential nexus to terrorism. The remaining 10 SARs, following additional review, did not technically meet the necessary criteria and the Analysis Unit was able to Unfound these reports. After reviewing each of these 78 SARs and performing our own analysis, the OIG concurred with each SAR disposition assigned by the Analysis Unit.

[17] The Analysis Unit assigned a disposition of Unfounded for ten SARs.

ADDENDUM

Special Order No. 1, 2012 identifies the following 16 distinct activities or behaviors as potentially having a nexus to terrorism. Although the information reported in a SAR may result from observations or investigation by police officers, or may be reported to them by a community member, the suspicious activities reported on a SAR are restricted to 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: Comprising 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.