

LOS ANGELES POLICE COMMISSION

**REVIEW OF
SUSPICIOUS ACTIVITY REPORTS,
FISCAL YEAR 2013/2014**



OFFICE OF THE INSPECTOR GENERAL

ALEXANDER A. BUSTAMANTE
Inspector General

January 23, 2015

TABLE OF CONTENTS

I. INTRODUCTION1

II. REVIEW OF SARs2

 Table No. 1 – Types of Officer Contacts with Involved Persons2

 Table No. 2 – Primary Activities Identified in Affirmed SARs.....3

 Chart No. 1 – Race/Ethnicity & Gender of Named IPs for SARs Sent to JRIC3

 Chart No. 2 – Race/Ethnicity & Gender of IPs for Unfounded SARs4

III. ISSUES4

 Six SARs Should Have Been Unfounded.....4

 Five SARs Had the Incorrect Activity Type Identified5

IV. PRIOR RECOMMENDATIONS5

 Recommendation No.15

 Recommendation No. 26

V. RECOMMENDATION6

VI. DEPARTMENT RESPONSE6

APPENDICES

APPENDIX A – 16 ACTIVITY TYPES IDENTIFIED IN SPECIAL ORDER NO. 17-2012a

APPENDIX B – GEOGRAPHIC DISTRIBUTION MAP OF THE 161 SARs SENT TO JRICb

REVIEW OF SUSPICIOUS ACTIVITY REPORTS FISCAL YEAR 2013/2014

I. INTRODUCTION

The United States Government in 2009 established the Nationwide Suspicious Activity Reporting (SAR) Initiative in response to the findings of the 9/11 Commission. The purpose of the SAR Initiative is to foster the sharing of SARs across all levels of government. In August 2012, the Los Angeles Police Department (Department) issued Special Order No. 17-2012 revising existing guidelines for the collection of SARs.¹ The Department guidelines are based on existing federal guidelines.²

Police officers or community members can initiate a SAR when they directly observe or otherwise become aware of a suspicious activity or behavior. A community member can report that activity or behavior directly to an officer in the field or at an Area station, submit information via the internet, or call the Department hotline.³ In an effort to educate the public on suspicious activity reporting, the Department created a community awareness program called iWatchLA.⁴ This program is designed to educate community members on the behaviors and activities that may have connections to terrorism.

In most cases, SARs are initiated by community members who contact their local Area station and notify a police officer of the suspicious activity or behavior. The officer then completes a report following the instructions of the Special Order. The Area watch commander (WC) then reviews the report to determine if the information obtained warrants a SAR designation. If the WC determines that a SAR is appropriate, the “paper” SAR is faxed or mailed to Major Crimes Division (MCD), with no copies retained at the Area.⁵

The MCD enters all SAR data into the Department’s Palantir system.⁶ The MCD then analyzes the SAR and determines whether to unfound or affirm the SAR. Two conditions must be present for MCD to affirm a SAR. First, the observed activity must be “reasonably indicative of intelligence gathering or pre-operational planning related to terrorism or other criminal activity.”⁷ Second, the activity must be one (or more) of 16 specific activities identified in the Special Order.⁸

¹ Department Special Order No. 17-2012, “Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism - Revised; and Suspicious Activity Report Notebook Divider, Form 18.30.03 - Revised” (Aug. 28, 2012), first published March 5, 2008, as Special Order No. 11, “Reporting Incidents Potentially Related to Foreign or Domestic Terrorism.”

² See Nationwide SAR Initiative at nsi.ncirc.gov.

³ The internet URL for reporting is http://www.lapdonline.org/iwatchla/content_basic_view/52267. The LAPD Hotline is 877-LAPD-247 (877-527-3247).

⁴ <http://lapdonline.org/iwatchla>.

⁵ MCD resides within the Department’s Counter-Terrorism and Special Operations Bureau.

⁶ Palantir is a computerized “platform,” or combination of hardware and software, that collects and organizes data. For additional information, see www.palantir.com/solutions/law-enforcement.

⁷ See Special Order (S.O.) No. 17-2012.

⁸ See Appendix A for definitions of the 16 activity types (based on activities identified by the National SAR Initiative).

All SARs which MCD affirms are digitally sent to the Joint Regional Intelligence Center (JRIC), which then shares the information with other law enforcement agencies.⁹ All SARs which MCD unfounds are purged from Palantir and are not digitally sent to JRIC.

Working copies of the affirmed paper SARs are secured in a locked file cabinet at MCD for two years. Then the working copies are sent to Iron Mountain off-site storage for three years, until destroyed. Originals of the affirmed paper SARs are sent monthly to Records and Identification Division (R&I), where they are secured in a locked file cabinet for two years. Then the originals are sent to Iron Mountain off-site storage for three years, until destroyed.

The unfounded paper SARs (both working copies and originals) are secured in a locked file cabinet at MCD for one year or until reviewed by the OIG, and then destroyed.¹⁰

II. REVIEW OF SARs

The OIG reviewed all 215 SARs collected by the Department during Fiscal Year 2013/14.¹¹ Of those 215 SARs, 175 (81%) were initiated by community members and 40 (19%) were initiated by officers. Also, of those 215 SARs, 50 (23%) resulted in officer contact with an involved person (IP).¹² Those 50 SARs are categorized in the table below by the type of officer contact.

Table No. 1 – Types of Officer Contacts with Involved Persons

Type of Officer Contact with IP	No. of SARs	% of Total
Traffic Stop/Detention ¹³	20	40%
Arrest ¹³	11	22%
Consensual Encounter	7	14%
Pedestrian Stop/Detention ¹³	5	10%
Officer Response to Radio Call	3	6%
Officer Response to Traffic Collision	2	4%
Detention for Mental Evaluation Hold	<u>2</u>	<u>4%</u>
Total	<u>50</u>	<u>100%</u>

The OIG reviewed each of these 50 officer-contact SARs and identified no constitutionally-related issues.

⁹ JRIC is collaboration between federal, state, and local law enforcement and public safety agencies. JRIC collects, analyzes, and disseminates threat intelligence. The JRIC Norwalk, CA facility serves Los Angeles County and six surrounding counties. For additional information, see <https://www.jric.org>.

¹⁰ This procedure, to destroy unfounded paper SARs after one year or until reviewed by the OIG, was established after the prior OIG review.

¹¹ FY 2013/14 is July 1, 2013, to June 30, 2014.

¹² In 10 instances, an officer had contact with an IP after the community member notified police of the suspicious activity.

¹³ The suspicious activity was observed or surmised during the detention or arrest but was not the reason for the detention or arrest. As an example, an officer made a traffic stop for a Vehicle Code violation and then observed something suspicious inside the vehicle. As another example, a person was arrested for trespassing on private property, and their reason for being on the property was considered suspicious.

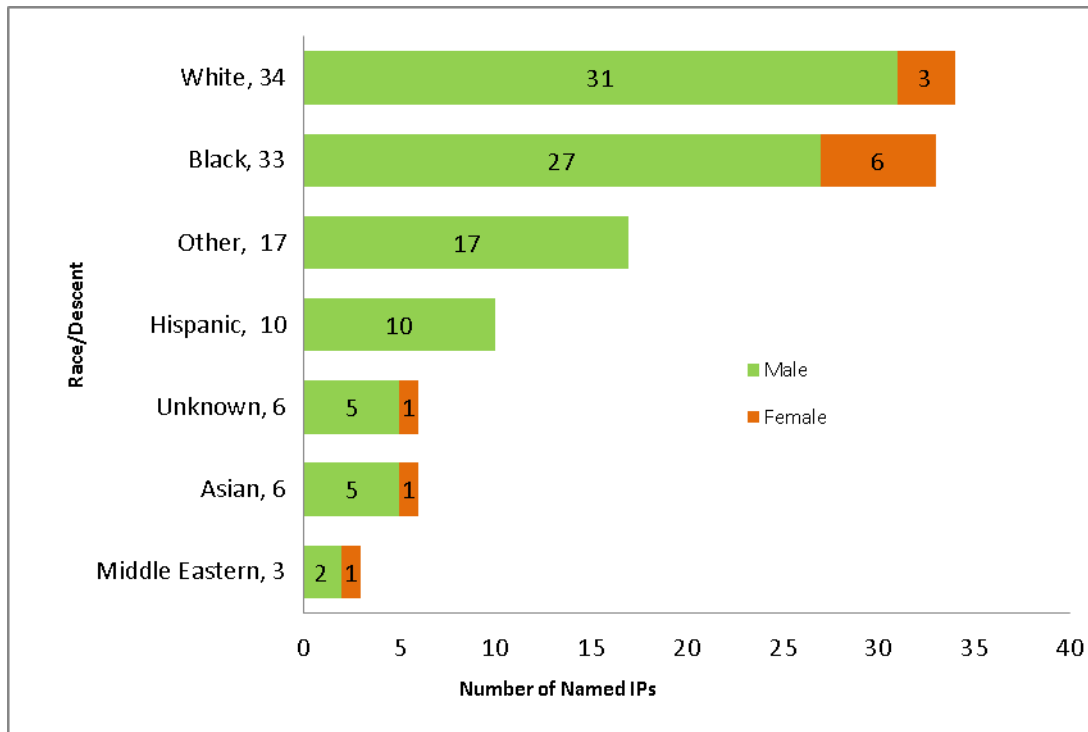
The MCD sent 161 affirmed SARs to JRIC and unfounded 54 SARs.¹⁴ The 161 affirmed SARs are categorized in the table below by primary activity type.

Table No. 2 – Primary Activities Identified in Affirmed SARs

Primary Activity	No. of SARs	% of Total
Expressed or Implied Threat	46	29%
Misrepresentation	26	16%
Observation/Surveillance	21	13%
Photography	20	12%
Testing/Probing of Security	13	8%
Breach/Attempted Intrusion	10	6%
Other Activity	<u>25</u>	<u>16%</u>
Total	<u>161</u>	<u>100%</u>

Of the 161 affirmed SARs sent to JRIC, 99 included information on 109 named involved persons, categorized in the chart below by race/ethnicity and gender.

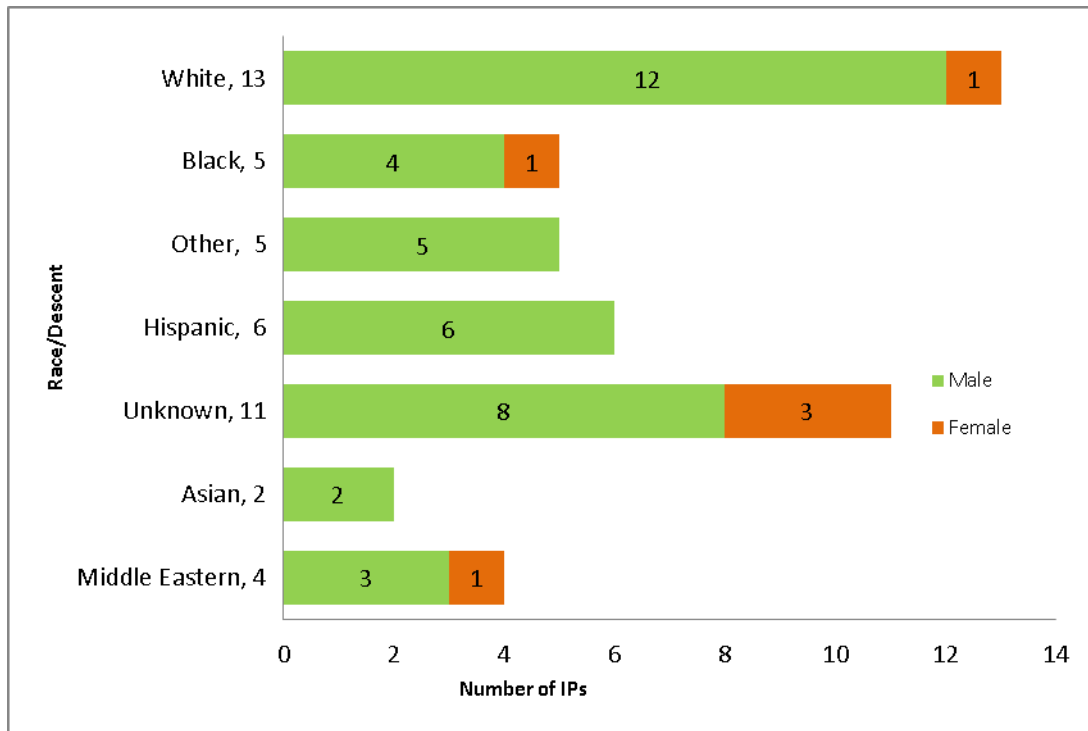
Chart No. 1 – Race/Ethnicity & Gender of Named IPs for SARs Sent to JRIC



¹⁴ See Appendix B for a geographic distribution (“pin”) map of the 161 SARs sent to JRIC.

Of the 54 unfounded SARs, 41 had 46 IPs categorized in the chart below by race/ethnicity and gender.¹⁵

Chart No. 2 – Race/Ethnicity & Gender of IPs for Unfounded SARs



III. ISSUES

Six SARs Should Have Been Unfounded

The OIG found no issues with 209 (97%) of the 215 SARs either affirmed or unfounded. For only 6 of the 161 SARs affirmed, the OIG believes the SAR should have been unfounded. In each of these 6 cases, the OIG concurred with MCD that the activity was of concern but disagreed as to one specific aspect of each case. These 6 SARs are briefly summarized below:

Three SARs resulted from traffic stops for Vehicle Code violations where the IP drivers identified themselves as members of possible suspected terrorist groups.¹⁶ In each stop, the IP initially attempted to present a non-legitimate form of identification but also subsequently provided valid identification (e.g., California Driver License). The MCD affirmed each SAR as a “Misrepresentation.” Because the IP did present valid identification, the OIG believes there was no actual misrepresentation, even though the initial presentation of non-legitimate identification would be of concern to a police officer.¹⁷

¹⁵ The OIG verified that the personal identifying information of all 46 IPs was purged from Palantir.

¹⁶ Two drivers were described on the SAR as “Male Black” and one as “Male White.”

¹⁷ Misrepresentation is “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),” (Special Order 17-2012).

Two SARs resulted from traffic stops for Vehicle Code violations where the IP drivers were found to be on the Terrorist Watchlist.^{18,19} The officers created SARs which MCD affirmed and forwarded to JRIC. The OIG agreed that being named on the Watchlist would be a concern to a police officer but is not one of the specific 16 categories required for a SAR to be affirmed.

For one SAR, a citizen reported that an unnamed IP espoused a violent extremist philosophy and support of terrorist attacks reported in the news, but the IP did not make any specific threats.²⁰ The citizen reported the SAR, which MCD affirmed and forwarded to JRIC. The OIG noted that espousing violent extremist philosophy or generalized support of terrorism is not one of the specific 16 categories required for a SAR to be affirmed.²¹

Five SARs Had the Incorrect Activity Type Identified

As a lesser procedural issue, the OIG determined that 5 (3%) of the 161 SARs MCD sent to JRIC had the incorrect activity type identified. That is, while the OIG agreed that the behavior or activity was correctly affirmed as a SAR, the activity was better classified as one of the other 15 activities rather than the original activity chosen.

IV. PRIOR RECOMMENDATIONS

On March 12, 2013, the OIG presented its first report on the Department SAR process to the Board of Police Commissioners. That report included two recommendations, which are recounted here to verify what action the Department took in response.

Recommendation No. 1

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.

Status: Closed. The OIG generally noticed more detail in the narratives for the FY 2013/14 SARs and more articulation as to why or how officer contact was made with involved persons. The narratives articulated that any detentions or arrests were for the underlying criminal activity (e.g., traffic code violation or trespassing) and not for the suspicious [non-criminal] activity.

¹⁸ Both drivers were described on the SAR as “Male Other.”

¹⁹ The Terrorist Screening Center of the National Security Branch of the Federal Bureau of Investigation maintains the Watchlist, which is “a single database of identifying information about those known or reasonably suspected of being involved in terrorist activity.” For additional information, see www.fbi.gov/about-us/nsb/tsc.

²⁰ The unnamed IP was described on the SAR as “Male Other.”

²¹ The Special Order notes that activities “generally protected by the First Amendment to the United States Constitution . . . should not be reported in a SAR.” In this case, the IP did not make a spoken threat “reasonably indicative of intelligence gathering or pre-operational planning related to terrorism or other criminal activity.”

Recommendation No. 2

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.

Status: Closed. The OIG found adequate security over the paper SARs. As previously stated, the affirmed paper SARs are secured in locked file cabinets at both MCD (working copies) and R&I (originals) for two years, until sent to Iron Mountain and later destroyed. The unfounded paper SARs are secured in a locked file cabinet at MCD for one year or until reviewed by the OIG and then destroyed. The MCD management attested that the OIG auditors are the only outsiders who have accessed and examined the paper SARs. Management also attested that, internally, the paper SARs at both MCD and R&I have only been accessed and examined by five MCD officers: the captain and lieutenant, the two detectives assigned to the SAR unit, and the compliance officer.

V. RECOMMENDATION

The OIG recommends that collaboration and review occur to ensure that MCD's improvements to and revisions of the SAR process continue. In this report, the OIG noted improvements to the process, which serve to enhance constitutional privacy protections while promoting the goal of coordinating information about potential terrorism-related activity.

VI. DEPARTMENT RESPONSE

The Commanding Officer (C/O) of MCD concurred with the recommendations by the Office of the Inspector General. In furtherance of the implementation of the recommendations, the C/O addressed each below reported issue and the related action the Department will take.

In response to the SARs that should have been unfounded due to misrepresentation and espousing violent extremist philosophy, MCD has unfounded the SARs and has notified the JRIC. Major Crimes Division has also implemented additional oversight and training to Department personnel in the deficient areas to ensure compliance with Special Order No. 17-2012.

In response to the two SARs relating to the Terrorist Screening Center WatchList hits, MCD has provided additional oversight and training to Department personnel. The Department has also developed a Department Notice, dated November 12, 2014, to address TSC matters.

APPENDIX A - 16 ACTIVITY TYPES IDENTIFIED IN SPECIAL ORDER NO. 17-2012

Criminal Activity and Potential Terrorism Nexus Activity (7)

- **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/Diversions.** 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; or,
- **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.

Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During an Investigation (9)

- **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 9 behaviors/activities are generally protected by the First Amendment to the United States Constitution and should not be reported in a SAR, absent articulable facts and circumstances that support suspicion that the behavior observed is not innocent, but rather reasonably indicative of criminal activity associated with terrorism, including evidence of pre-operational planning related to terrorism. Race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion (although these factors may be used as specific-involved person descriptors).

APPENDIX B – GEOGRAPHIC DISTRIBUTION MAP OF THE 161 SARs SENT TO JRIC

