INTRADEPARTMENTAL CORRESPONDENCE

June 11, 2019 **BPC# 19-0157**
1.0

TO: The Honorable Board of Police Commissioners

FROM: Inspector General, Police Commission

SUBJECT: REVIEW OF SUSPICIOUS ACTIVITY REPORTS 2016 – 2017

RECOMMENDED ACTION

REVIEW and APPROVE the Office of the Inspector General's Review of Suspicious Activity Reports 2016 – 2017.

DISCUSSION

The Office of the Inspector General (OIG) is responsible for conducting annual reviews of the Department's Suspicious Activity Report (SAR) program. The OIG reviewed a total of 348 SARs from calendar years 2016 and 2017and determined that, based on the information provided, about 98 percent of SAR classifications appeared to comply with current Department policy. The small number of cases wherein the OIG did identify concerns related to classification or other issues are discussed in this report. In analyzing the SARs and related policies, the OIG further determined that the Department's overall SAR process could be improved by updating current policy to reflect changes made at the federal level in 2015, as well as by better defining procedures regarding the dissemination of SAR-related information to outside entities.

E-Copy – Original Signature on File with the Police Commission

MARK P. SMITH
Inspector General
Police Commission

Attachment

LOS ANGELES POLICE COMMISSION

REVIEW OF SUSPICIOUS ACTIVITY REPORTS 2016 – 2017

Conducted by the

OFFICE OF THE INSPECTOR GENERAL

MARK P. SMITH
Inspector General

June 11, 2019

TABLE OF CONTENTS

I. INTRODUCTION AND EXECUTIVE SUMMARY 1

II. SAR POLICY 1

III. DEPARTMENT SAR PROCESSING 2

IV. STATISTICAL OVERVIEW 3

A. SARs by Location of Occurrence and LAPD Classification 3

B. Reported Activities and Behaviors 4

C. Descent of Involved Persons 5

D. Officer-Initiated SARs and Officer Contact Types 8

V. OIG REVIEW OF 2016 – 2017 SUSPICIOUS ACTIVITY REPORTS 8

A. Classification of SARs 8

B. Unfounded SARs Sent to JRIC Through Other Means 11

C. Removal of Identifying Information for Unfounded SARs 12

D. Basis for Contact with the Police 12

VI. STANDARDS FOR SUSPICIOUS ACTIVITIES AND BEHAVIORS 12

VII. DEPARTMENT RESPONSE 13

VIII. RECOMMENDATIONS 13

IX. APPENDIX i

A. Special Order No. 17 – 2012 i

B. NSI Suspicious Activity Reporting Indicators and Behaviors, February 2016 xii

OFFICE OF THE INSPECTOR GENERAL
REVIEW OF SUSPICIOUS ACTIVITY REPORTS 2016 – 2017

I. INTRODUCTION AND EXECUTIVE SUMMARY

In 2009, the United States Government established the Nationwide SAR Initiative (NSI) in response to the findings of the 9/11 Commission. The NSI fosters the sharing of information across multiple levels of government to prevent terrorism and other criminal activity.[1] The Los Angeles Police Department (LAPD or Department) began collecting Suspicious Activity Reports (SARs) in 2008 to document reported or observed activity that was believed by officers to have a nexus to foreign or domestic terrorism.[2] In August 2012, the Department issued Special Order 17 – a revised SAR policy, which included a refined list of the activities/behaviors that constitute suspicious activity.[3,4]

The Office of the Inspector General (OIG) is responsible for conducting annual reviews of the Department's SAR program. The OIG reviewed a total of 348 SARs from calendar years 2016 and 2017 and determined that, based on the information provided, about 98 percent of SAR classifications appeared to comply with current Department policy. The small number of cases wherein the OIG did identify concerns related to classification or other issues are discussed in this report. In analyzing the SARs and related policies, the OIG further determined that the Department's overall SAR process could be improved by updating current policy to reflect changes made at the federal level in 2015, as well as by better defining procedures regarding the dissemination of SAR-related information to outside entities.

II. SAR POLICY

Special Order 17 revised the Department's practices to be consistent with the federal Information Sharing Environment (ISE) Functional Standard published in 2009.[5] It specifies that SARs are to be completed when Department officers directly observe, or receive reports of, activities or behaviors that are "reasonably indicative of pre-operational planning related to terrorism or other

---

[1] The Nationwide Suspicious Activity Reporting Initiative is a joint collaborative effort by the U.S. Department of Homeland Security; the Federal Bureau of Investigation; and state, local, tribal, and territorial law enforcement partners. This initiative provides law enforcement with a tool to help prevent terrorism and other related criminal activity by establishing a national capacity for gathering, documenting, processing, analyzing, and sharing Suspicious Activity Report information. For more information, *see* https://nsi.ncirc.gov.

[2] For further background information on the Department's past SAR protocols, see "Suspicious Activity Reporting System Audit," Office of the Inspector General, March 12, 2013. https://docs.wixstatic.com/ugd/b2dd23_a000774e4074ac5da6af41f276f3d4b4.pdf.

[3] 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," Los Angeles Police Department, August 28, 2012. Codified as Department Manual 4/271.45, "Terrorism Liaison Officer (TLO)'s Responsibilities."

[4] The changes detailed in Special Order 17 were based on The Intelligence Reform and Terrorism Prevention Act of 2004 and the National Strategy for Information Sharing in 2007.

[5] "Information Sharing Environment - Suspicious Activity Report (ISE-SAR) Functional Standard, Version 1.5," Program Manager for the Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, 2009.

criminal activity."[6] These activities or behaviors must fall into one of the 16 designated categories listed in the special order.[7]

The list of activities/behaviors provided in Special Order 17 is separated into two groups, with the first group being criminal activity or activity with a potential nexus to terrorism, and the second group being activity that may not be criminal in nature. The special order warns that some of the activities observed by or reported to officers are generally protected by the First Amendment. As such, they 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." This may include, for example, "evidence of pre-operational planning related to terrorism."

The policy further states that a SAR should not consider the race, ethnicity, national origin, or religious affiliation of an Involved Person (IP) as a factor creating suspicion.[8] It also reminds officers of constitutional and case law relating to search and seizure, and it indicates that officers may not detain a person if they do not have reasonable suspicion of criminal activity or probable cause to make an arrest.

III. DEPARTMENT SAR PROCESSING

A SAR can be initiated by police officers or community members when they observe or become aware of activity that they perceive to be suspicious and potentially related to terrorism. Community members initiate most SARs by reporting the suspicious activity to a police officer in the field or at an Area station, but the Department also receives such reports online and through a telephone hotline as a part of the iWatchLA program.[9]

Upon observing activity believed to be suspicious, or when receiving information from a community member, a police officer may conduct a preliminary investigation where appropriate. If the information is deemed to fall within SAR guidelines, the officer then completes a SAR and forwards it to the Area watch commander for review. Once approved, the SAR is forwarded to Major Crimes Division (MCD), with no copies retained at the area station.[10] Department

---

[6] The Department and federal guidelines also refer to this as potentially having a "nexus to terrorism."

[7] LAPD Manual 4/271.45, "Terrorism Liaison Officer (TLO)'s Responsibilities."

[8] An Involved Person is an individual that allegedly has been observed engaging in suspicious activity when no definitive criminal activity can be identified, thus precluding identification as a "suspect." *See* LAPD Manual 4/271.45, "Terrorism Liaison Officer (TLO)'s Responsibilities,"*supra* note 10.

[9] iWatchLA "educates the public about behaviors and activities that may have a connection to terrorism." iWatchLA is available through any internet browser, as well as through mobile applications for both Android and Apple operating systems. For more information, *see* http://www.lapdonline.org/iwatchla.

[10] MCD is within the Counter-Terrorism and Special Operations Bureau, Office of Special Operations, LAPD. A Division of Records (DR) Number and incident number will also be assigned to each SAR in the Consolidated Crime and Arrest Database (CCAD).

personnel can obtain guidance from MCD on completing SARs 24 hours per day, seven days per week, via on-duty personnel or an on-call supervisor.

Upon receiving a SAR, MCD personnel enter the relevant reported information into the Department's Palantir database.[11] The report is analyzed pursuant to the standards described in Special Order 17 to decide whether it will be unfounded or affirmed. If, in the judgment of the SAR Unit, the information provided in the SAR is consistent with one of the order's 16 specified activities/behaviors and is reasonably indicative of terrorism or other criminal activity, the SAR is affirmed; otherwise, the SAR is unfounded.

In cases where the SAR is affirmed, MCD digitally sends the report and any corresponding documentation to the Joint Regional Intelligence Center (JRIC), which has the final authority in accepting or rejecting a SAR.[12] If accepted, JRIC assigns the incident to a specific working group that will follow up on the details provided. In some cases, JRIC accepts LAPD-affirmed SARs on an "Information Only" basis, which indicates that the information will be retained, but that there will not necessarily be immediate follow-up. In either situation, information from accepted SARs is shared with other law enforcement agencies nationwide via the federally-operated Information Sharing Environment (ISE).

If a SAR is unfounded by LAPD, it is typically not sent to JRIC, and any Involved Person's information is to be deleted from Palantir and CCAD. However, Palantir retains other pertinent information related to the SAR, such as location, date of occurrence, and case synopsis, for five years. Occasionally, information and details about an unfounded SAR are forwarded to other Departmental units for further investigation if it is deemed necessary based on the underlying action or potential crime described in the SAR.[13]

IV. STATISTICAL OVERVIEW

A. SARs by Location of Occurrence and LAPD Classification

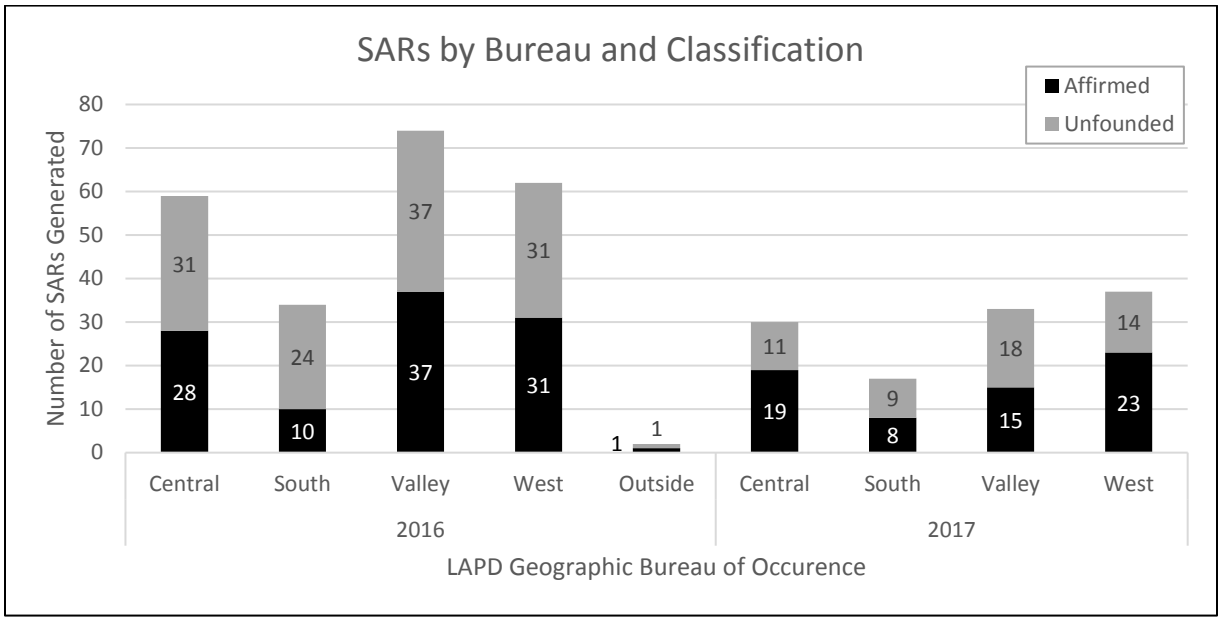
The OIG reviewed a total of 348 SARs generated by the Department during calendar years 2016 and 2017, which included 231 and 117 SARs for those years, respectively. Of those, 172 (about

[11] Palantir is an online platform, accessible via the Department's intranet, which provides integrated access to information stored in multiple law enforcement databases. Although every sworn employee has access to basic Palantir functionality, access to SARs is restricted. Authorization to view SARs in Palantir is limited to employees of MCD and select employees given temporary access, such as OIG personnel performing this review. Temporary access expires once the need for access has concluded.

[12] JRIC is a multi-agency collaboration of federal, state, and local law enforcement agencies formed to collect, analyze, and disseminate threat-related information. The Norwalk JRIC facility deals with threat intelligence for Los Angeles County and six surrounding counties, and it is also capable of disseminating information to agencies outside of its primary operation zone. For additional information on JRIC, *see* https://www.jric.org.

[13] Affirmed SARs are to be maintained for 5 years, in accordance with the Department's document retention policy, while unfounded SARs are secured in a locked file cabinet at MCD for one year, or until reviewed by the OIG, at which point they are to be destroyed.

49 percent) were affirmed and 176 (about 51 percent) were unfounded. The breakdown of SARs by Bureau and classification can be seen in the following table.



The OIG noted a significant (49 percent) decline in the number of SARs reported from 2016 to 2017. In conversations with the Department, this reduction was attributed, in part, to the training of personnel on the proper circumstances and incidents that require a SAR to be filled out. As a possible related result, the OIG's analysis also noted a slight increase in the proportion of SARs that were affirmed from 2016 to 2017 (from 46 percent to 56 percent). The OIG also noted that, during this same time period, the JRIC acceptance rate for SARs affirmed by the LAPD decreased slightly from 57 percent to 48 percent.[14]

B. Reported Activities and Behaviors

The primary activities/behaviors reported in each affirmed SAR were captured by the OIG and are listed in the following tables. The most common activities/behaviors in both years, as documented on the SAR, were Expressed or Implied Threat, Photography, and Observation/Surveillance.

[14] Two additional 2016 SARs that were initially affirmed but later unfounded by the LAPD were also accepted by JRIC prior to being reversed.

Primary Activities/Behaviors Identified in Affirmed SARs 2016 – 2017					
2016			**2017**		
Activity/Behavior Type	**Number and Percent**		**Activity/Behavior Type**	**Number and Percent**	
Expressed or Implied Threat	53	50%	Expressed or Implied Threat	30	46%
Photography	21	20%	Observation/Surveillance	12	18%
Misrepresentation	8	7%	Photography	8	12%
Materials Acquisition/Storage	6	6%	Eliciting Information	4	6%
Observation/Surveillance	5	6%	Testing or Probing of Security	2	3%
Testing or Probing of Security	5	5%	Breach/Attempted Intrusion	2	3%
Theft/Loss/Diversion	2	2%	Recruiting	1	2%
Eliciting Information	2	2%	Misrepresentation	1	2%
Sabotage/Tampering/Vandalism	1	1%	Sabotage/Tampering/Vandalism	1	2%
Cyber Attack	1	1%	Acquisition of Expertise	1	2%
Aviation Activity	1	1%	Weapons Discovery	1	2%
Acquisition of Expertise	1	1%	Theft/Loss/Diversion	1	2%
Weapons Discovery	1	1%	Aviation Activity	1	2%
Total	**107**	**100%[15]**	**Total**	**65**	**100%[16]**

C. Descent of Involved Persons

As previously noted, Special Order 17 specifies that race, ethnicity, national origin, or religious affiliation should not be considered as factors that create suspicion, although these factors may be used in describing an Involved Person who is the subject of a SAR. The following tables provide the breakdown of the Descent listed for the primary Involved Person on each SAR, the gender documented for that person, and whether the SAR was accepted by JRIC (for affirmed SARs only). It is important to note that the race/ethnicity categorizations associated with Involved Persons, which are used by the Department to populate the Descent field, are in many cases based on the perceived descriptions reported to the Department by community members or on the perception of officers themselves.

[15] Due to rounding, percentages shown may not add up to 100.

[16] Due to rounding, percentages shown may not add up to 100.

2016 SARs by Primary Involved Person Descent, Gender, and Outcome							
Reported Descent	Total SARs	Reported Gender			LAPD Classification		JRIC Result
		Male	Female	Unknown	Affirmed	Unfounded	Accepted[17]
Other	61	56	5	0	27	34	20
White	39	37	2	0	20	19	13
Hispanic	33	33	0	0	14	19	3
Black	25	23	2	0	13	12	6
Asian	5	5	0	0	4	1	2
Middle Eastern	5	5	0	0	4	1	2
Persian	1	1	0	0	0	1	0
Afghan	1	1	0	0	1	0	1
Unknown	61	21	6	34	24	37	16
Total	**231**	**182**	**15**	**34**	**107**	**124**	**63**

2017 SARs by Primary Involved Person Descent, Gender, and Outcome							
Reported Descent	Total SARs	Reported Gender			LAPD Classification		JRIC Result
		Male	Female	Unknown	Affirmed	Unfounded	Accepted[18]
Other	28	26	2	0	17	11	10
White	26	24	2	0	12	14	6
Hispanic	17	14	3	0	4	13	1
Black	10	9	1	0	6	4	3
Asian	1	1	0	0	1	0	0
Middle Eastern	1	1	0	0	1	0	1
Unknown	34	10	0	24	24	10	11
Total	**117**	**85**	**8**	**24**	**65**	**52**	**32**

The OIG found that only 48 percent of the above SARs, including 47 percent of SARs that were affirmed, contained names or other information that could be used to identify the Involved Person. The following table indicates the Descent and outcome for Involved Persons whose name or other identifying information was captured in the SAR.

[17] This calculation includes SARs accepted by JRIC as "Information Only," as well as two unfounded cases that were initially affirmed and sent to JRIC prior to being reversed.

[18] This calculation includes SARs accepted by JRIC as "Information Only."

All Named or Otherwise Identified IPs by Descent and Outcome[19]						
Reported Descent	**2016**			**2017**		
	Unfounded	**Affirmed**	**Accepted by JRIC[20]**	**Unfounded**	**Affirmed**	**Accepted by JRIC[21]**
Other	31	23	17	2	7	4
White	14	9	5	10	6	3
Hispanic	11	13	3	7	3	0
Black	6	10	5	4	5	2
Asian	3	3	2	0	1	0
Middle Eastern	0	1	0	0	0	0
Afghan	0	1	1	0	0	0
Persian	1	0	0	0	0	0
Unknown	11	4	4	3	1	0
Total	**77**	**64**	**37**	**26**	**23**	**9**

The OIG noted that a substantial portion of SARs – about 26 percent in 2016 and 24 percent in 2017 – listed the primary IP as "Other." Many of these SARs, however, contained additional details or descriptors about the IP in the narrative or associated notes. Using the notes, the OIG found that about half (53 percent) of the reports that classified the primary IP as "Other" explicitly referenced the person as being of Middle Eastern descent or originating from a specific Middle Eastern country.[22] Thirteen percent of the "Other" cases included one of the following descriptors: Indian/South Asian, Armenian, Turkish, Pakistani, Ethiopian, Bangladeshi, Sri Lankan, Ukrainian, or Mediterranean. The remaining 34 percent of "Other" SARs did not contain explicit descriptions of the IP's descent.

Given community concerns that SARs may be used to target people based on their racial/ethnic or religious background, the OIG believes that it would be beneficial for the Department to more effectively track, to the extent possible, the descent of IPs classified as "Other." This is particularly relevant where, as here, the "Other" category represents the largest group of IPs by number (excluding IPs whose Descent is listed as "Unknown"). While demographic data should not be used as a factor creating suspicion, the Department may want to consider whether its

[19] This table includes 23 secondary IPs, as some SARs have more than one identifiable IP.

[20] This includes information from one SAR that was sent to, and accepted by, JRIC prior to being reversed.

[21] This includes SARs accepted by JRIC as "Information Only."

[22] These notes are in many cases based on the perceived descriptions reported to the Department by community members, or on the perception of officers themselves.

Descent categories should be broadened to facilitate more precise statistical record-keeping and greater accountability of its SAR program.[23]

D. Officer-Initiated SARs and Officer Contact Types

Of the 231 SARs in 2016, 39 (17 percent) were initiated by officers, and a total of 56 (24 percent) involved police contact with the Involved Person(s). In 2017, 16 of the 117 SARs were officer-initiated (14 percent), with a total of 18 incidents involving contact between the police and the Involved Person(s) (15 percent). The following table details the types of contacts that officers had with Involved Persons for both years.

Type of Officer Contacts with Involved Person(s) in 2016 and 2017			
2016		**2017**	
Type of Contact with IP	**No. of Contacts**	**Type of Contact with IP**	**No. of Contacts**
Arrest	15	Detention Following Radio Call	6
Investigation Pursuant to Radio Call	10	Arrest	5
Consensual Encounter	8	Traffic Stop	4
Detention Following Radio Call	8	Consensual Encounter	2
Detention for Medical Evaluation Hold	5	Detention Following Traffic Stop	1
Detention Following Pedestrian Stop	3		
Traffic Stop	3		
Follow-up Investigation	2		
Police Station Walk-In	1		
Citation Following Radio Call	1		
Total	**56**	**Total**	**18**

V. OIG REVIEW OF 2016 – 2017 SUSPICIOUS ACTIVITY REPORTS

A. Classification of SARs

A primary focus of the OIG SAR review, in addition to ensuring compliance with procedural standards, was to determine whether affirmed SARs clearly adhered to the standards related to activities/behaviors set forth in Special Order 17. In order for the activities/behaviors described in the SARs to be affirmed, there must be "articulable facts and circumstances supporting the

[23] For instance, regulations associated with the California Racial and Identity Profiling Act of 2015 (RIPA), which govern the Department's collection of stop data, include the following categories in the list of races/ethnicities tracked: "Asian," "Black/African American," Hispanic/Latino(a)," "Middle Eastern or South Asian," "Native American," "Pacific Islander," and "White." The OIG also found that the United States Census has been researching changes to its current set of race/ethnicity options, including the addition of a "Middle Eastern or North African" response category. *See* "2015 National Content Test Race and Ethnicity Analysis Report," U.S. Department of Commerce, Economics and Statistics Administration, U.S. Census Bureau, February 28, 2017.

allegation that the behavior observed is not innocent and is reasonably indicative of criminal activity associated with terrorism."[24]

Based on the information provided, the OIG determined that almost all of the Department's SAR classifications – about 98 percent – complied with the SAR policy. As described below, the OIG did identify concerns about the decision to affirm seven SARs, including six SARs from 2016 and one from 2017. Two of these were accepted by JRIC, four were declined, and one was affirmed but never sent to JRIC.

1. *Photography and Video Recording in Public Places*

Two affirmed SARs questioned by the OIG described the Involved Person taking pictures or recording video in a public place. In each case, the report also included additional factors about the person's behavior that were considered by officers to be suspicious. Even considering these factors, however, the OIG did not concur that the person's activity was reasonably indicative of pre-operational planning related to terrorism or other criminal activity. Additionally, in one of these cases, further investigation by the Department confirmed that an Involved Person worked in a vocation that likely explained the photography. Although this last case was not ultimately sent to JRIC, it was not clear to the OIG why its classification was not changed to unfounded, as occurred in other cases.

An additional two cases also involved photography or video recording in public places, specifically of police stations or police buildings, by one or more Involved Persons who are often referred to as "First Amendment Auditors." Each of these two incidents included the same Involved Person. As stated in a 2014 Department notice, the public has a right to photograph and videotape government buildings, including police stations, provided the activity is done for lawful purposes.[25] The notice also indicates that officers may investigate and report those who engage in behavior that would support a SAR. In these instances, however, the OIG did not concur that the additional facts described in the associated reports were reasonably indicative of pre-operational planning related to terrorism or other criminal activity.

The Department has explained that it was not familiar with the emerging trend involving First Amendment Auditors at the time these SARs were affirmed, and that the IP's activity therefore appeared suspicious. As such, all of the above cases occurred in 2016, with no similar cases being affirmed in 2017.

In researching this issue, the OIG also found that the language related to photography in the current federal Functional Standard for SARs was revised in 2015 and is more restrictive than its

[24] LAPD Manual 4/271.45, "Terrorism Liaison Officer (TLO)'s Responsibilities."

[25] "Rights of Persons to Photograph and Videotape Officers in Public," Office of Operations Notice, September 9, 2014.

previous version; it is also more restrictive than the language contained in LAPD policy.[26] For example, LAPD's current SAR language related to photography describes someone "taking pictures […] in a manner that would arouse suspicion in a reasonable person." In contrast, the revised Standard describes "taking pictures […] in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person." As noted on page 12, the OIG recommends that the LAPD update its policy to be consistent with the revised guidelines.

2. *Other Classification Issues*

The OIG also identified questions about three additional affirmed SARs. In two of these cases, based on the information provided, the IP's behavior did not appear to fall into one of the 16 behavior categories listed in Special Order 17.[27] In the first case, the IP provided official identification to confirm a lodging reservation that indicated they were not the same person who had initiated the reservation. The SAR did not, however, describe any attempt by the IP to present a falsified document or to misrepresent their own identity or affiliation to cover possible illicit activity, as is addressed by Special Order 17. In the second case, it appeared that a cyber attack or website hack involving a business entity had occurred. The limited information provided in the SAR, however, was insufficient to indicate that the IPs could reasonably be connected with the cyber attack.

The final case involved the discovery of potential bomb-making material found in the trunk of the Involved Person's vehicle. Following an investigation, however, it was determined that the items found were not bomb-making materials and did not pose a threat. As such, it was not clear why this SAR was not subsequently unfounded, as had occurred in other cases.

3. *Documentation of Rationale*

The OIG found that notes from SAR Unit personnel are typically documented in Palantir, describing the reasons for which a SAR was affirmed or unfounded, and also describing what preliminary investigatory work has been performed. This information was extremely helpful in understanding the basis for each classification decision. In some cases, however, the OIG found the notes to be less descriptive than in others, making it difficult to fully understand the relationship between the described activity/behavior in the SAR and the Special Order 17 criteria.

The OIG also noted that MCD performs regular internal audits of all SARs to ensure that they are properly processed and classified, which helps to maintain the integrity of the reporting

[26] "Information Sharing Environment – Suspicious Activity Report (ISE-SAR) Functional Standard, Version 1.5.5," Program Manager for the Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, 2015.

[27] In both cases, the OIG also found that other facts provided in the SAR did not reasonably indicate that the Involved Persons' activities had a potential nexus to terrorism.

system. This process occasionally results in overturning a preliminary decision to affirm or unfound a SAR, but the OIG found that corresponding Palantir notes did not always adequately describe the specific reasons for the change. For example, in two of the affirmed cases listed in the previous section, the SAR had originally been unfounded but was later affirmed due to an internal audit. In these cases, although the notes contained a rationale for unfounding the case, no similar rationale was provided for overturning that decision.[28]

The OIG recommends that SAR-related notes in Palantir include a clear rationale for all classification or reclassification decisions, including any additional detail used to affirm or unfound a SAR. In cases that are ultimately unfounded, the notes should also continue to verify that personal identifying information was scrubbed or purged from the system and that JRIC was notified of the final decision.

B. Unfounded SARs Sent to JRIC Through Other Means

During its review, the OIG discovered that 13 SARs in 2016 and 6 SARs in 2017 were classified as unfounded by the Department, but that the details and information contained in each of the reports was sent to JRIC through its Tips & Leads program.[29,30] Department personnel indicated that this practice was limited to those situations wherein Special Order 17 criteria were not met, but it was nonetheless determined that the details of an incident were concerning and should be transmitted to JRIC for further analysis. The OIG verified that, in these cases, identifying information and other details were scrubbed from LAPD databases, as is required for any SAR that is unfounded.

It should be noted that, according to federal guidelines, the SAR process "does not supersede other information or intelligence gathering, or sharing authority," and that multiple federal agencies have "the authority to collect tips and leads." The guidelines further indicate that only tips and leads that meet the guidelines set forth for SARs will be broadly shared with participants of the National SAR Initiative through the Information Sharing Environment. Terrorism-related leads that do not meet this standard, however, may nonetheless require investigative follow-up or other action.[31]

In reviewing these cases further, the OIG noted that some of the unfounded SARs contained information potentially related to terrorism, such as a person declaring their support or allegiance for a terrorist organization or referencing statements about an attack on a location or dignitary.

---

[28] In cases where a SAR is unfounded after initially being sent to JRIC, LAPD personnel contact JRIC to inform them of this fact.

[29] A total of 14 of the 19 unfounded SARs sent to JRIC contained identifying information about the Involved Person.

[30] The OIG noted one additional unfounded SAR for which identifying information about the IP was sent to another law enforcement agency.

[31] Information Sharing Environment - Suspicious Activity Report (ISE-SAR) Functional Standard, Version 1.5.5, Program Manager for the Information Sharing Environment (PM-ISE), Office of the Director of National Intelligence, 2015, pages 16-17.

They also included instances in which the activity documented appeared to potentially fall into a SAR category, such as "Express or Implied Threats" or "Acquisition of Expertise," but the report had limited detail, was stale, or could not be corroborated. In other cases, however, the basis for sending the information to JRIC as being terrorism-related was not as clear.

To the extent that the Department finds it appropriate to share intelligence gleaned from unfounded SARs with JRIC or other entities, the OIG recommends that it develop a clear set of written parameters and an approval process to ensure that such decisions do not undercut the protections built into the SAR policy.

C. Removal of Identifying Information for Unfounded SARs

The OIG sought to ensure that all unfounded SARs were disposed of as required by law and that all corresponding private information was eliminated from any Department databases. One of the OIG's primary concerns during this review involved the collection, dissemination, and expected purging of Involved Persons' identifying information. As noted above, roughly 48 percent (167 of 348) of the SARs had some type of personal identifying information associated with one or more IPs. Due to the sensitive nature of this information, the OIG reviewed the Palantir database for each of the 348 SARs to confirm that identifying information was purged for all unfounded SARs. In doing so, the OIG determined that two unfounded SAR records still contained some personal identifying information. The OIG notified the Department, which took immediate measures to have the information permanently removed from Palantir.

D. Basis for Contact with the Police

The OIG reviewed each SAR for any potential issues related to the basis for a stop or search. In general, based on the information provided in the SAR, the LAPD contacts with Involved Persons appeared to be either consensual or supported by reasonable suspicion or probable cause. Likewise, the vast majority of searches were documented as being consensual or supported by reasonable suspicion or probable cause. The OIG did identify concerns about one case, however, which involved the inappropriate detention and search of an individual who was filming and taking pictures outside of a police station. In further researching this case, the OIG discovered that a complaint had been filed and that the subsequent investigation appropriately resulted in sustained allegations against two officers related to these concerns.

This incident was captured on Body-Worn Video (BWV), which proved very helpful in reviewing both the SAR and the associated encounter with the police. In all, 34 SAR-related contacts were captured on BWV or other video. The OIG recommends that MCD be required to review any video associated with a SAR as part of its review and classification process.

VI. STANDARDS FOR SUSPICIOUS ACTIVITIES AND BEHAVIORS

As noted above, Special Order 17 explicitly revised Department SAR procedures "to be consistent with Office of the Director for National Intelligence, Information Sharing Environment (ISE) Functional Standards." At that time, the most recent version of the ISE

Functional Standard had been published in 2009. The ISE Functional Standard was revised in 2015, providing further clarification for the types of actions and behaviors that would properly be categorized as suspicious. These new definitions have been distributed by the Department internally and, according to SAR Unit personnel, already factor into their decision-making. The OIG recommends that the Department update its written policy to conform to the current Functional Standard.[32]

VII. DEPARTMENT RESPONSE

The OIG met with Department representatives to present its general findings and discuss specific examples and concerns. Although its analysis differed from the OIG's in some instances, the Department understood the concerns presented and was receptive to the findings of the report, as well as to the proposed recommendations listed in the next section. The OIG believes that the implementation of the proposed recommendations will be effective in addressing the concerns identified in this report.

VIII. RECOMMENDATIONS

Based on the findings set forth in this report, the OIG recommends the Commission direct the Department to do the following:

A. Revise Special Order 17 to incorporate updated language regarding suspicious activity behaviors and indicators set forth by the 2015 iteration of the ISE Functional Standard.

B. Require that Palantir analyst notes clearly state the rationale for affirming or unfounding each SAR, and require that the notes explain the rationale for any reversal of an original classification.

C. Consider options to more effectively categorize the racial/ethnic background of Involved Persons currently listed in the Descent category as "Other."

D. Develop parameters regarding the sharing of information gleaned from any unfounded SAR with JRIC or other outside agencies.

E. Review all video and audio recordings associated with a SAR as part of the classification process.

[32] SAR Unit personnel also suggested to the OIG that it would be advisable to: a) streamline procedures for ensuring timely delivery of SARs to MCD; and b) require officers to contact the SAR Unit for advice prior to completing a SAR.

IX. APPENDIX

A. Special Order No. 17 – 2012

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 17 **August 28, 2012**

APPROVED BY THE BOARD OF POLICE COMMISSIONERS ON AUGUST 28, 2012

SUBJECT: **REPORTING SUSPICIOUS ACTIVITY POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM - REVISED; AND SUSPICIOUS ACTIVITY REPORT NOTEBOOK DIVIDER, FORM 18.30.03 - REVISED**

PURPOSE: This Order revises the procedures for reporting suspicious activity potentially related to foreign or domestic terrorism to be consistent with the Office of the Director of National Intelligence, Information Sharing Environment Functional Standards Suspicious Activity Reporting. Officers are reminded of the Fourth Amendment to the United States Constitution as it pertains to search and seizure, and the United States Supreme Court Case *Terry vs. Ohio* as it pertains to stop and frisk. Furthermore, the Office of the Inspector General will review the Suspicious Activity Report process on an annual basis as part of their audit/inspection responsibilities.

PROCEDURE: Attached are the revised Department Manual Section 1/590, renamed as *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism;* Section 4/271.46, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism;* and the Suspicious Activity Report (SAR) Notebook Divider, Form 18.30.03, with revisions in italics. Manual Section 4/271.46 is revised to provide relevant definitions and clarifies the employee's responsibilities regarding the investigation and reporting of suspicious activity.

FORM AVAILABILITY: The Suspicious Activity Report Notebook Divider is available in LAPD E-Forms on the Department's Local Area Network (LAN). All other versions of the SAR Notebook Divider shall be marked "obsolete" and placed into the divisional recycling bin.

AMENDMENTS: This Order amends Sections 1/590 and 4/271.46 of the Department Manual.

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

CHARLIE BECK
Chief of Police

Attachments

DISTRIBUTION "D"

DEPARTMENT MANUAL
VOLUME I
Revised by Special Order No. 17, 2012

590. REPORTING *SUSPICIOUS ACTIVITY* POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM. 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. 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].

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

271.46 REPORTING SUSPICIOUS ACTIVITY POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM.

DEFINITIONS.

Suspicious Activity. *Suspicious Activity is defined as observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.*

Terrorism. *Terrorism is defined as the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. This is consistent with the Code of Federal Regulations (28 C.F.R. Section 0.85). This definition includes individuals and groups who plan, threaten, finance, aid/abet, and attempt or perform unlawful acts in furtherance of terrorist activity.*

Suspicious Activity Report. A Suspicious Activity Report (SAR), Form 03.24.00, *is an official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. The SAR* is a stand-alone report. The information reported in a SAR may result from observations or investigations by police officers, or may be reported to them by private sources.

These terrorism-related behaviors may indicate intelligence gathering or pre-operational planning related to terrorist activities or other criminal activity. These activities and behaviors include:

Criminal Activity and Potential Terrorism Nexus Activity.

- **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; *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.

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

Potential Criminal or Non-Criminal Activity Requiring Additional Fact Information During an Investigation.

- **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 *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).

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

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

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.

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

Employee's Responsibilities. Any Department employee receiving any information regarding suspicious activity and/or observing any suspicious activity is to investigate and take appropriate action, *including* 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.

Activities that are generally protected by the First Amendment should not be reported as a SAR, unless additional facts and circumstances can be clearly articulated that support an officer's or agency's determination that the behavior observed is reasonably indicative of criminal activity associated with terrorism or other criminal activity.

Officers are reminded of constitutional and case law as they pertain to search and seizure, and to stop and frisk. Officers, who have neither reasonable suspicion to detain nor probable cause to arrest, cannot legally prevent an individual from walking away.

***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. The individual is free to leave at any time during a consensual encounter unless there is reasonable suspicion to detain or probable cause to arrest.*

***Lawful Detention**. A lawful 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.*

***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.*

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

- **If the suspicious activity observed (e.g., suspicious behaviors or activities only) is <u>not</u> 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 *is to* be listed within the "Potential Target" section of the SAR. Otherwise the "City of Los Angeles" *is to* 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 *is to be* completed. The Property Report *is to* bear a separate DR and incident number from the SAR, along with the following:**

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

    - **The Property Report DR number *is to* 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 *is to* 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 *are to* be maintained at the Area**.

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

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

- **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 *are to* 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 *are to* 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 *are to* 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 was completed, DR No.__." The involved person's name(s) from the SAR *are* not *to* be documented on the aforementioned report or any other related reports, e.g., IR, Arrest, etc.

Hazardous Devices Materials Section, Emergency Services Division – Responsibility. *Personnel assigned to the Explosive Unit (Bomb Squad), Hazardous Materials Unit, or Los Angeles Police Department Bomb Detection Canine (K-9) Section are to 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.*

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

Watch Commander's Responsibilities. Upon notification that officers have received information regarding suspicious activity, the watch commander *is to*:

- 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 for completeness; and,
- Ensure 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 *is* not *to* be documented on the aforementioned reports or any other related reports, e.g., IR, Arrest, etc.

Major Crimes Division's *Responsibilities*. Upon receiving a telephonic notification of suspicious activity, MCD personnel *will*, 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 *are to* 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**.

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 *are to*:

- Assign DR number(s) for the SAR 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, *MCD*, 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 *are to* be maintained at the Area.**

DEPARTMENT MANUAL
VOLUME IV
Revised by Special Order No. 17, 2012

Area Detective's Responsibilities. *For* 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 *are to:*

- Immediately notify MCD and forward the SAR to MCD (**No copies of the SAR *are to* 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**.

Counter-Terrorism and Special Operations Bureau - Responsibility. *Counter-Terrorism and Special Operations Bureau 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.*

SUSPICIOUS ACTIVITY REPORT
These guidelines should be followed for investigations of Suspicious Activity.

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 activities or intentions related to either foreign or domestic terrorism, in a manner that protects the information, privacy and legal rights of Americans.

DEFINITIONS:

SUSPICIOUS ACTIVITY
Suspicious Activity *is defined as* observed *behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity.*

TERRORISM
Terrorism is defined as the unlawful use of force and violence against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof, in furtherance of political or social objectives. This is consistent with the Code of Federal Regulations (28 C.F.R. Section 0.85). This definition includes individuals and groups who plan, threaten, finance, aid/abet, and attempt or perform unlawful acts in furtherance of terrorist activity.

SUSPICIOUS ACTIVITY REPORT
A Suspicious Activity Report (SAR), Form 03.24.00, *is an official documentation of observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity. The SAR* is a stand-alone report. The information reported in a SAR may result from observations or investigations by police officers, or may be reported to them by private sources.

Note: A SAR shall only be completed for those activities and behaviors specifically listed or defined under "Reportable Suspicious Activities" (see page 2).

INVOLVED PERSON
An involved person (IP) is an individual *who* 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, *including* 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;
☐ 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 *is to* be listed within the "Potential Target" section of the SAR. Otherwise the "City of Los Angeles" *is to* 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 *is to* be completed. The Property Report *is to* bear a separate DR and incident number from the SAR, along with the following:**

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

☐ **The Property Report DR number *is to* 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 *is to* 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 *are to* 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 *are to* 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.

SUSPICIOUS ACTIVITY REPORT
These guidelines should be followed for investigations of Suspicious Activity.

☐ 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 *are to* 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 *are to* 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 was completed, DR No. __." The involved person's name(s) from the SAR *are* not *to* be documented on the aforementioned report or any other related reports, e.g., IR, Arrest, etc.

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 *is* not *to* 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.

REPORTABLE SUSPICIOUS ACTIVITIES:

These terrorism-related behaviors may indicate intelligence gathering or pre-operational planning related to terrorist activities or other criminal activity. These activities and behaviors include:

Criminal Activity and Potential Terrorism Nexus Activity

- **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; *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

- **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 *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).

SOURCE: Department Manual Section 1/590, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism* and Section 4/271.46, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism.*

B. NSI Suspicious Activity Reporting Indicators and Behaviors, February 2016

Suspicious Activity Reporting
Indicators and Behaviors

Tools for Analysts and Investigators

Behaviors	Descriptions
Defined Criminal Activity and Potential Terrorism Nexus Activity	
Breach/Attempted Intrusion	Unauthorized personnel attempting to enter or actually entering a restricted area, secured protected site, or nonpublic area. Impersonation of authorized personnel (e.g., police/security officers, janitor, or other personnel).
Misrepresentation	Presenting false information or misusing insignia, documents, and/or identification to misrepresent one's affiliation as a means of concealing possible illegal activity.
Theft/Loss/Diversion	Stealing or diverting something associated with a facility/infrastructure or secured protected site (e.g., badges, uniforms, identification, emergency vehicles, technology, or documents {classified or unclassified}), which are proprietary to the facility/infrastructure or secured protected site.
Sabotage/Tampering/ Vandalism	Damaging, manipulating, defacing, or destroying part of a facility/infrastructure or secured protected site.
Cyberattack	Compromising or attempting to compromise or disrupt an organization's information technology infrastructure.
Expressed or Implied Threat	Communicating a spoken or written threat to commit a crime that will result in death or bodily injury to another person or persons or to damage or compromise a facility/infrastructure or secured protected site.
Aviation Activity	Learning to operate, or operating an aircraft, or interfering with the operation of an aircraft in a manner that poses a threat of harm to people or property and that would arouse suspicion of terrorism or other criminality in a reasonable person. Such activity may or may not be a violation of Federal Aviation Regulations.
Potential Criminal or Non-Criminal Activities Requiring Additional Information During Vetting ***Note: When the behavior describes activities that are not inherently criminal and may be constitutionally protected, the vetting agency should carefully assess the information and gather as much additional information as necessary to document facts and circumstances that clearly support documenting the information as an ISE-SAR.***	
Eliciting Information	Questioning individuals or otherwise soliciting information at a level beyond mere curiosity about a public or private event or particular facets of a facility's or building's purpose, operations, security procedures, etc., in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Testing or Probing of Security	Deliberate interactions with, or challenges to, installations, personnel, or systems that reveal physical, personnel, or cybersecurity capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Recruiting/Financing	Providing direct financial support to operations teams and contacts or building operations teams and contacts; compiling personnel data, banking data, or travel data in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Photography	Taking pictures or video of persons, facilities, buildings, or infrastructure in an unusual or surreptitious manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include taking pictures or video of infrequently used access points, the superstructure of a bridge, personnel performing security functions (e.g., patrols, badge/vehicle checking), security-related equipment (e.g., perimeter fencing, security cameras), etc.
Observation/ Surveillance	Demonstrating unusual or prolonged interest in facilities, buildings, or infrastructure beyond mere casual (e.g., tourists) or professional (e.g., engineers) interest and in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person. Examples include observation through binoculars, taking notes, attempting to mark off or measure distances, etc.
Materials Acquisition/ Storage	Acquisition and/or storage of unusual quantities of materials such as cell phones, pagers, radio control toy servos or controllers; fuel, chemicals, or toxic materials; and timers or other triggering devices, in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Acquisition of Expertise	Attempts to obtain or conduct training or otherwise obtain knowledge or skills in security concepts, military weapons or tactics, or other unusual capabilities in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.
Weapons Collection/ Discovery	Collection or discovery of unusual amounts or types of weapons, including explosives, chemicals, and other destructive materials, or evidence, detonations or other residue, wounds, or chemical burns, that would arouse suspicion of terrorism or other criminality in a reasonable person.
Sector-Specific Incident	Actions associated with a characteristic of unique concern to specific sectors (e.g., the public health sector), with regard to their personnel, facilities, systems, or functions in a manner that would arouse suspicion of terrorism or other criminality in a reasonable person.

http://nsi.ncirc.gov

rev. 02/16