LOS ANGELES POLICE COMMISSION

REVIEW OF SUSPICIOUS ACTIVITY REPORTS, 2015

Conducted by the

OFFICE OF THE INSPECTOR GENERAL

ALEXANDER A. BUSTAMANTE
Inspector General

September 7, 2016

TABLE OF CONTENTS

APPENDIX

OFFICE OF THE INSPECTOR GENERAL
REVIEW OF SUSPICIOUS ACTIVITY REPORTS, 2015

I. INTRODUCTION

The United States Government in 2009 established the Nationwide Suspicious Activity Reporting Initiative in response to the findings of the 9/11 Commission. The Initiative fosters information sharing across multiple levels of government to prevent terrorism and other criminal activity.[1] In August 2012, the Los Angeles Police Department (Department or LAPD) issued revised guidelines for the collection of Suspicious Activity Reports (SARs)[2] based upon federal guidelines adopted in 2004 and 2007.[3] The Office of the Inspector General (OIG) conducts regular reviews of the Department's SARs.[4]

Police officers or community members can initiate a SAR when they observe or become aware of activity that appears 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. The Department also provides a hotline,[5] and iWatchLA, which provides community education about suspicious activity reporting.[6]

Upon observing suspicious activity or receiving information from a community member, a police officer completes a SAR following Department policy guidelines. The officer then forwards the SAR to the Area watch commander for review and, once approved, the SAR is forwarded to Major Crimes Division (MCD)[7] with no copies retained at the Area station. Department personnel can obtain guidance from MCD on completing SARs, 24 hours a day, 7 days a week, via on-duty personnel or an on-call supervisor.[8]

In comparison to LAPD, the Los Angeles County Sheriff's Department, the Long Beach Police Department, and the Glendale Police Department do not have a special unit to process and analyze SARs. Those agencies rely on watch commanders to cull suspicious information from crime and incident reports and forward the information to the Joint Regional Intelligence Center (JRIC).

---

[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] Department Special Order No. 17, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism - Revised; and Suspicious Activity Report Notebook Divider, Form 18.30.03 – Revised*, August 28, 2012, codified as Department Manual Volume 4, Section 271.46.

[3] The Intelligence Reform and Terrorism Prevention Act of 2004 and the National Strategy for Information Sharing in 2007.

[4] This review and report was completed by the OIG's Audit & Complaint Section.

[5] The LAPD hotline is 877-LAPD-247 (877-527-3247).

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

[7] MCD is within the Counter-Terrorism and Special Operations Bureau, Office of Special Operations, LAPD.

[8] During major holidays or after large terrorist incidents, the number of on-call supervisors is temporarily increased.

II. DEPARTMENT SAR PROCESSING

Upon receiving a SAR, MCD personnel enter all of the report information into the Department's Palantir database.[9] Personnel from MCD analyze the SAR and determine whether to unfound or affirm it. Two conditions must exist for a SAR to be affirmed: 1) the observed activity or behavior must be "reasonably indicative of intelligence gathering or pre-operational planning related to terrorism or other criminal activity,"[10] and 2) the activity/behavior must be one or more of the 16 specific activities/behaviors identified in Department policy.[11] The MCD digitally sends all affirmed SARs to the JRIC,[12] which has the final authority in accepting or rejecting a SAR. The JRIC shares the accepted SAR information with other law enforcement agencies nationwide.

The MCD does not send unfounded SARs to JRIC. If a SAR is unfounded, any Involved Person(s)[13] information is deleted from the Palantir system. However, the Palantir system retains other pertinent information, such as location, date of occurrence, and case synopsis for five years. Additionally, an unfounded SAR can be forwarded to another Department entity for further investigation.[14]

Working copies of the affirmed paper SARs are secured in a locked file cabinet at MCD for two years. The working copies are then sent to off-site storage for three years until destroyed. Originals of the affirmed papers SARs are sent monthly to Records and Identification Division (R&I), where they are secured in a locked file cabinet for two years.[15] The originals are then sent to off-site storage for three years, until destroyed.

---

[9] Palantir is a "platform" or portal, accessible via the intranet, which provides access to multiple law enforcement databases (e.g., DMV, DABIS, CWS, DOJ, etc.). Every sworn employee has Palantir access but must have specific permission to gain access to certain databases, such as SARs. For more information about Palantir generally, *see* www.palantir.com.

[10] Department Manual, Volume 4, Section 271.46, *Reporting Suspicious Activity Potentially Related to Foreign or Domestic Terrorism.*

[11] *Ibid.* The 16 specific activities/behaviors were developed by the Nationwide SAR Initiative. *See* Appendix for definitions.

[12] JRIC is a multi-agency collaboration of federal, state, and local law enforcement agencies to collect, analyze, and disseminate threat-related information. Five MCD officers are assigned to JRIC. The Norwalk JRIC facility not only deals with threat intelligence for Los Angeles County and the six surrounding counties but 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] An Involved Person is a named individual that has been observed engaging in suspicious activity when no definitive criminal activity can be identified, thus precluding identification as a "suspect." *See* Section 271.46, *supra* note 10.

[14] The unfounded SAR must contain information that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. Additionally, the Anti-Terrorism Intelligence Section can conduct limited investigations on information that does not constitute reasonable suspicion. For more information, *see* Office of the Inspector General, *Anti-Terrorism Intelligence Section Audit, Fiscal Year 2012/2013,* January 29, 2014, *available at* http://www.oig.lacity.org/#!audit-reports/c78i.

[15] The OIG determined that four R&I employees and four MCD employees have access to the paper SARs.

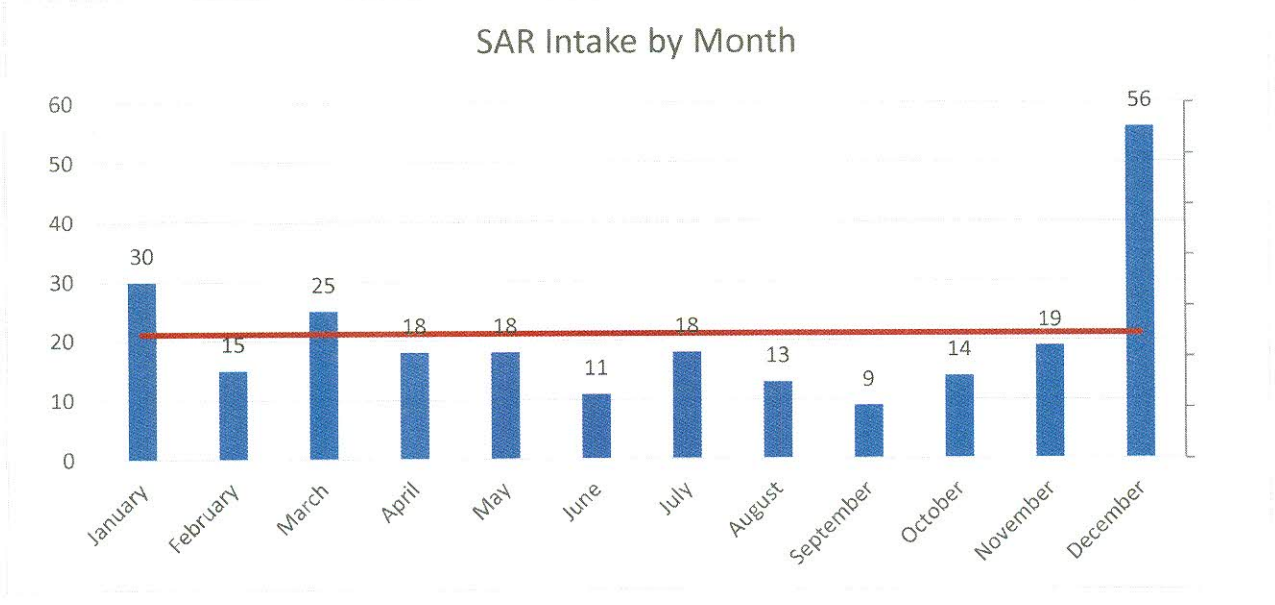
During the review, the OIG learned that SARs were also maintained digitally within the Integrated Crime and Arrest Records System (ICARS). Each SAR has a Division of Records (DR) number. As a matter of Department practice, all working DRs are scanned into ICARS. All SARs were also scanned into ICARS for indefinite retention. [16] When the OIG identified this issue, MCD's Commanding Officer immediately worked with R&I Command to end the practice of scanning SARs into ICARS.[17]

III. OIG REVIEW OF SARs

The OIG reviewed all 246 SARs collected by the Department during calendar 2015. In conducting the review, the OIG ensured that all affirmed SARs identified at least 1 of the 16 terrorism-related activities/behaviors.

The average monthly SAR intake at MCD was 21. The MCD received 19 SARs during November 2015, 13 of which were reported after the terrorist attack in Paris, France, on November 13. December 2015 had the highest number of reported SARs (56), possibly due to the terrorist attack that occurred in San Bernardino, California, on December 2. The monthly SAR intake, which includes both affirmed and unfounded, is depicted in the following chart.[18]

Chart No. 1 – SAR Intake by Month



The following table identifies the geographic Department bureau where each of the SARs was received. Five SARs indicated a location outside of City boundaries.

[16] The Department does not have policy regarding the retention timeframe for digital report copies. As of this review, MCD will be using the same retention policy for digital copies as they do for original reports.

[17] The MCD Commanding Officer also removed all MCD personnel access to SARs in ICARS.

[18] For a graphic depiction of SAR distribution, *see* the pin map in the Appendix, page c.

Table No. 1 – SAR Location of Occurrence by Bureau

Bureau	Number of SARs	Rate
West	83	34%
Valley	59	24%
Central	54	22%
South	45	18%
Outside	5	2%
Total	**246**	**100%**

The MCD unfounded 139 SARs and sent 107 affirmed SARs to JRIC. Some of the 107 affirmed SARs had more than one activity/behavior type reported, resulting in a total number of 138 activities/behaviors. The 107 affirmed SARs are categorized in the table below by the 16 activity/behavior types.

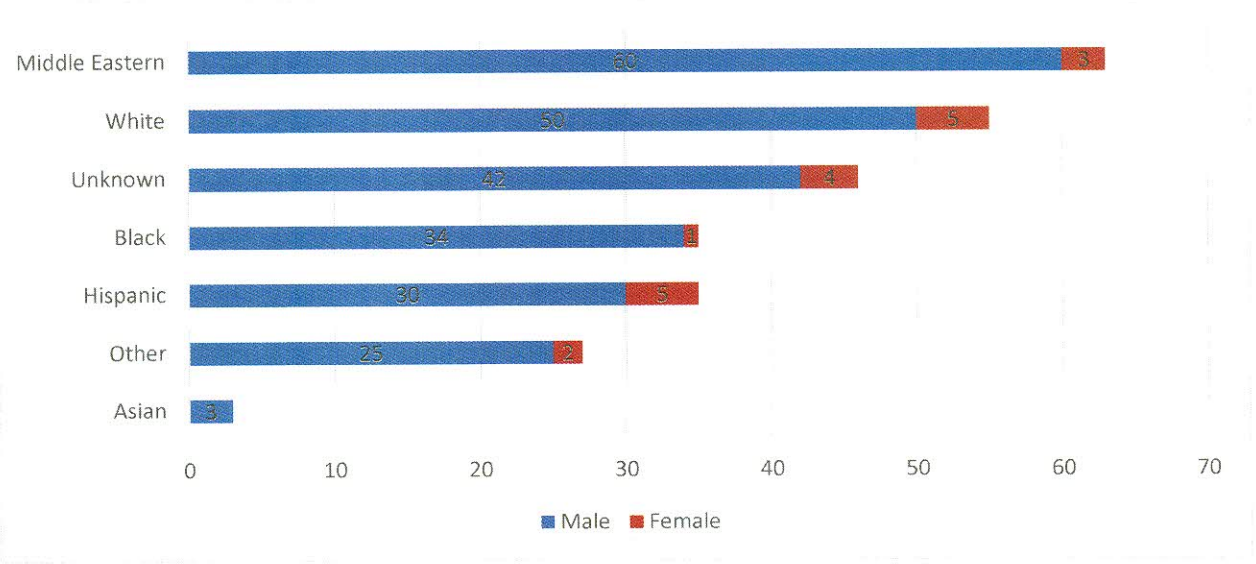
Table No. 2 – Activities/Behaviors Identified in Affirmed SARs

Activity/Behavior Type[19]	No. of Activities/ Behaviors	Occurrence Rate
Expressed or Implied Threat	49	35%
Photography	30	22%
Observation/Surveillance	13	9%
Testing or Probing of Security	11	8%
Recruiting	7	5%
Breach/Attempted Intrusion	5	4%
Materials Acquisition/Storage	5	4%
Acquisition of Expertise	5	4%
Misrepresentation	4	3%
Theft/Loss/Diversion	4	3%
Sabotage/Tampering/Vandalism	3	2%
Aviation Activity	2	1%
Total	**138**	**100%**

Of the 246 total SARs that MCD received, only 156 SARs had information describing individuals. The 156 SARs included information identifying 264 Involved Persons. The chart below shows the 264 Involved Persons by race and gender.

[19] Four of the 16 activities/behaviors were not reported in any of the 107 affirmed SARs: Cyber Attack, Eliciting Information, Weapons Discovery, or Sector-Specific Incident.

Chart No. 2 – SARs by Involved Person Race and Gender



IV. OFFICER-INITIATED SARS

Of the 246 SARs, 168 (68%) were initiated by community members and 78 (32%) by officers. Of those 78 officer–initiated SARs, 44 (56%) resulted in contact with Involved Persons. The OIG reviewed each of the 44 officer-contact SARs to search for any constitutionally-related issues (i.e., unlawful detention or arrest) or evidence of biased policing. Although the OIG requested clarification for a small number of SARs, there were no constitutional issues or biased policing concerns identified. None of the 44 contacts were initiated based on the behavior or activity subsequently reported on the associated SAR. The 44 SARs resulted in contacts with 57 Involved Persons. The table below shows the types of officer-initiated contacts with the 57 Involved Persons.

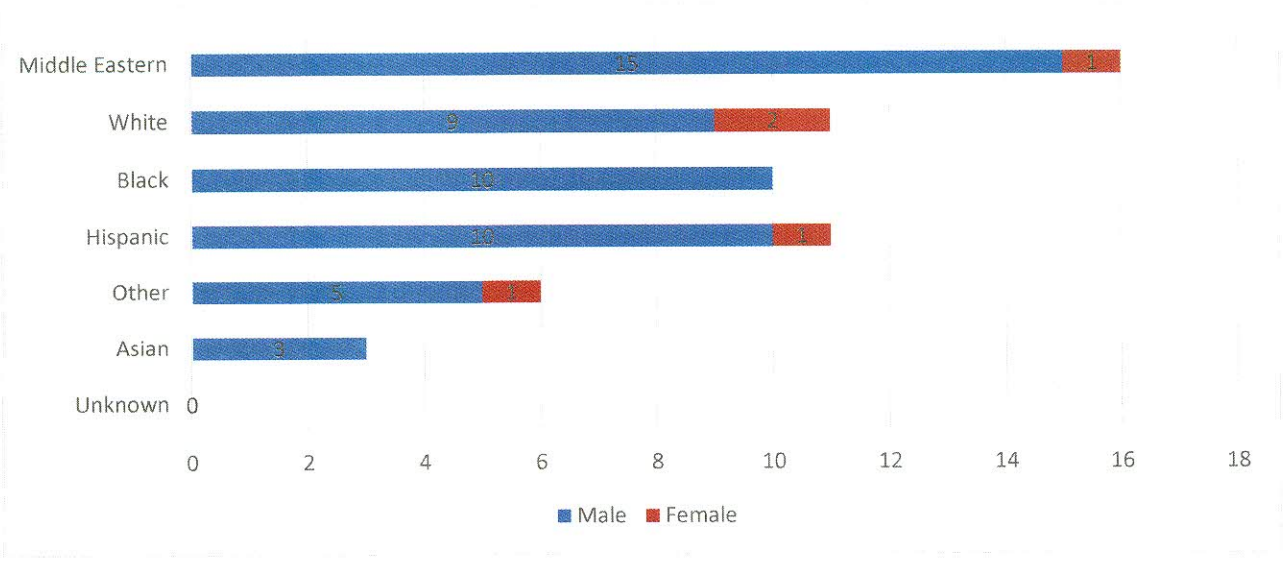
Table No. 3 – Type of Officer Initiated Contacts with Involved Person(s)

Type of Contact	No. of Persons	Occurrence Rate
Detention[20]	29	51%
Arrest	18	32%
Consensual	10	17%
Total	**57**	**100%**

The following chart shows the race and gender of these 57 Involved Persons.

[20] Detention includes placement of individuals under the California Welfare and Institutions Code, Section 5150.

Chart No. 3 – Officer Initiated Contacts: Race and Gender of Involved Persons



V. COMPLIANCE RATE

The previous OIG review[21] indicated that MCD attained a 97% rate of compliance with Department SAR policy for both affirmed and unfounded SARs. This current review determined that MCD attained a 100% compliance rate for all 246 SARs. The OIG concluded that all 139 SARs that MCD unfounded had no nexus to terrorism. The OIG also concluded that all 107 affirmed SARs that MCD sent to JRIC included at least 1 of the 16 terrorism-related activities/behaviors, so potentially had a nexus to terrorism.

VI. ISSUE & RECOMMENDATION: UNFOUNDED OFFICER-GENERATED SARS

The OIG noted that Terrorism Liaison Officers[22] (TLOs) are assigned to each geographic Area station.[23] The MCD provides updated terrorism information to the TLOs, who in turn provide roll call training to Area officers and supervisors. However, MCD indicated that while TLOs provide updates during roll calls and other meetings, they are not used as an Area-level resource as part of the SAR reporting process.

In this review, the OIG found that 36 percent of officer-generated SARs were ultimately unfounded by MCD. Those SARs were either based upon spontaneous angry, verbal threats made against an officer at the time of arrest with no potential nexus to terrorism or did not

---

[21] Office of the Inspector General, *Review of Suspicious Activity Reports, Fiscal Year 2013/2014*, January 23, 2015, http://www.oig.lacity.org/#!audit-and-complaint-reports/hi4dl.

[22] TLOs are sworn personnel of various ranks trained by MCD on identifying suspicious activity. TLOs are also responsible for disseminating new information to area officers and supervisors.

[23] Special Order No. 26, *Terrorism Liaison Officer Program – Revised*, June 8, 2009.

include any the aforementioned 16 terrorism-related activities/behaviors. In an effort to reduce the number of unfounded officer-generated SARs, the OIG recommends that TLO duties be expanded to include their use as an information and training resource for field officers and supervisors.

VII. DEPARTMENT RESPONSE

The commanding officer of Major Crimes Division agrees with the findings and recommendations.

APPENDIX

DEPARTMENT MANUAL § 4/271.46: 16 TERRORISM-RELATED ACTIVITIES/BEHAVIORS

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/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**:[24] 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)

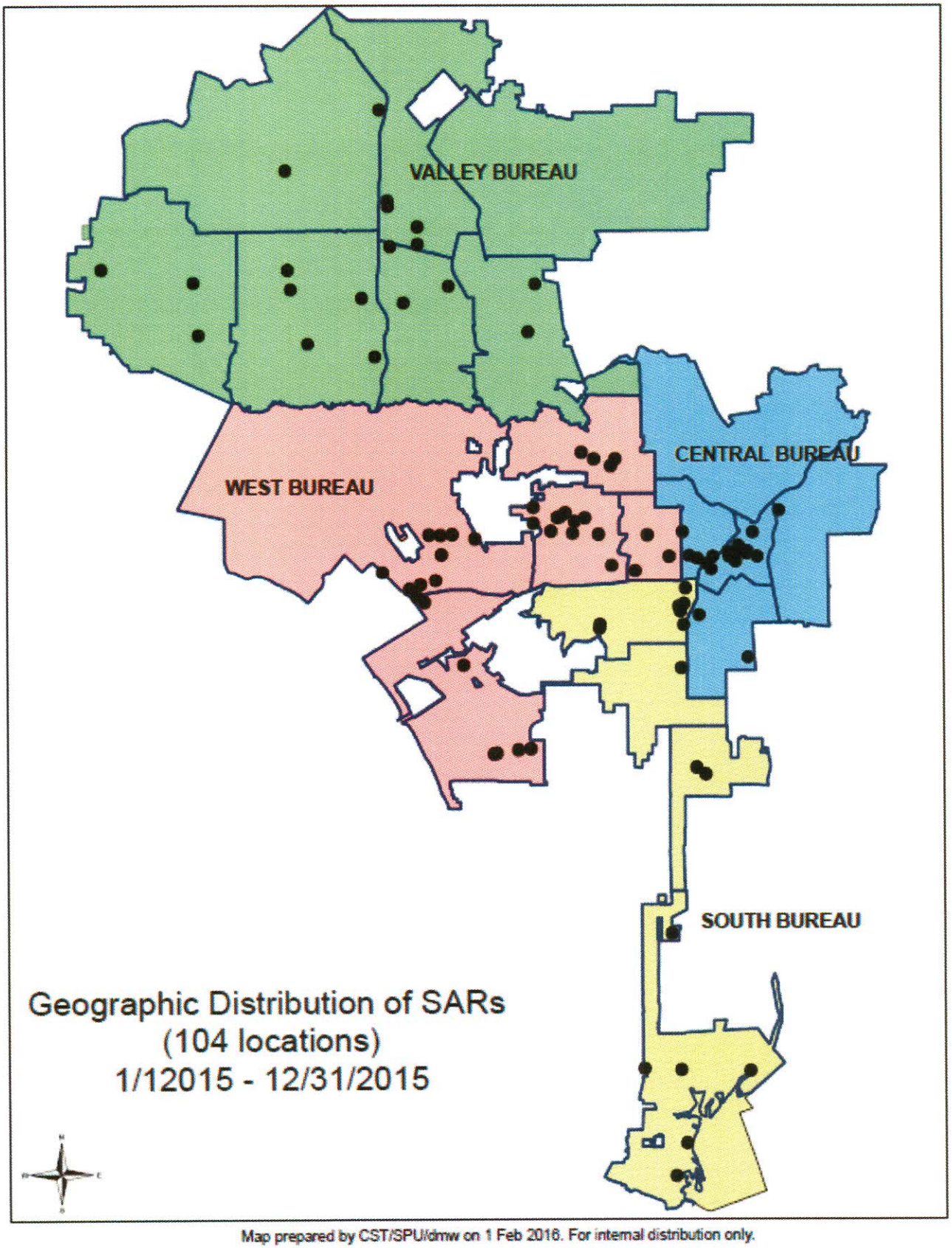
- **Eliciting Information**: Questioning individuals at a level beyond mere curiosity about particular facets of a facility's or building's purpose, operations, security procedures, etc., that would arouse suspicion in a reasonable person;
- **Testing or Probing of Security**: Deliberate interactions 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)

[24] The Federal Government has added "person(s)" to this definition. However, the Department Manual has not been updated and therefore does not incorporate this addition.

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 nine activities/behaviors 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).



Map prepared by CST/SPU/dmw on 1 Feb 2016. For internal distribution only.