United States
Department of Justice

Findings and Recommendations of the

Suspicious Activity Report (SAR)

Support and Implementation Project

October 2008

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

United States
Department of Justice

Findings and Recommendations of the

Suspicious Activity Report (SAR)

Support and Implementation Project

October 2008

Acknowledgements

The *Suspicious Activity Report (SAR) Support and Implementation Project* appreciates the support and guidance of the project sponsors: the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); the Major Cities Chiefs Association (MCCA); DOJ's Global Justice Information Sharing Initiative (Global); the Criminal Intelligence Coordinating Council (CICC); the U.S. Department of Homeland Security (DHS); and the Federal Bureau of Investigation (FBI). Representatives of these organizations were vital in the development of the findings and recommendations for the reporting of suspicious activity.

The SAR Support and Implementation Project team and participants involved numerous law enforcement experts from local, state, tribal, and federal agencies whose knowledge and dedication to the project are reflected within this document. The project's site visit team and the executive steering committee's insight helped guide the project through to its completion. A complete listing of all project team members and participants is contained in Appendix A.

Special appreciation goes to the Los Angeles, California, Police Department for spearheading the SAR Initiative and bringing it to the national forefront. Without the leadership and commitment of Chief William Bratton, Deputy Chief Michael Downing, and Commander Joan McNamara, this project would not be as advanced as it is today. Particular thanks are extended to Chief R. Gil Kerlikowske, Chief of Police, Seattle Police Department, and President of the MCCA, for his guidance throughout this project. The forward thinking from the senior leadership involved was instrumental in the development of these findings and recommendations.

This report would not have been possible without the effort of the Office of the Program Manager, Information Sharing Environment (PM-ISE) and its commitment to the sharing of criminal and terrorist information among local, state, tribal, and federal law enforcement agencies. A special thank-you is given to Ambassador Thomas E. ("Ted") McNamara, Program Manager; Ms. Susan B. Reingold, Deputy Program Manager; and Mr. John Cohen, Senior Advisor, for their dedication to this important nationwide initiative.

This project was supported by Grant No. 2007-NC-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative and the Program Manager, Information Sharing Environment. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice or the Program Manager, Information Sharing Environment.

Table of Contents

Executive Summary

The development of the recommendations for the reporting of suspicious activity is the direct result of the hard work and ingenuity of many local, state, tribal, and federal law enforcement representatives who believe national guidelines for suspicious activity reporting will help protect the citizens of the United States and aid in the prevention of another terrorist attack occurring on American soil. First and foremost, it should be noted that local law enforcement entities carry out counterterrorism-related activities within the context of their core mission of protecting local communities from crime and violence. Accordingly, it is essential that local law enforcement officers receive training to recognize those behaviors and incidents indicative of criminal activity associated with the planning and carrying out of a terrorist attack. Furthermore, it is important that local law enforcement entities incorporate the documenting, processing, analyzing, and sharing of information related to such activities into existing processes and systems used to better protect communities from criminal activity.

The Suspicious Activity Report (SAR) process, as defined in this paper, focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime and establishing a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism. Implementation of the SAR process can be accomplished within the agency's existing framework to gather, process, analyze, and report behaviors and events that are indicative of criminal activity. Just as the *National Criminal Intelligence Sharing Plan*,[1] the *Fusion Center Guidelines*,[2] and the *National Strategy for Information Sharing*[3] are key tools for law enforcement, the *Findings and Recommendations of the SAR Support and Implementation Project* will be another resource that agencies can employ to support their crime-fighting and public safety efforts.

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency. This report and its recommendations are important for establishing national guidelines that will allow for the timely sharing of SAR information; however, it is understood that every jurisdiction will have to develop policies and procedures that take into account the unique circumstances and relationships within that community. In accordance with the *National Criminal Intelligence Sharing Plan* and the *National Strategy for Information Sharing* (NSIS), the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); the Major Cities Chiefs Association (MCCA); DOJ's Global Justice Information Sharing Initiative (Global); the Criminal Intelligence Coordinating Council (CICC); the U.S. Department of Homeland Security (DHS); and

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the all-crimes approach to gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency.

1 www.it.ojp.gov/documents/National_Criminal_Intelligence_Sharing_Plan.pdf.
2 www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.
3 www.whitehouse.gov/nsc/infosharing/index.html.

the Federal Bureau of Investigation (FBI) have developed these recommendations to be used by law enforcement agencies to improve the identification and reporting of suspicious activity and the sharing of that information with fusion centers and Joint Terrorism Task Forces (JTTF).

In the spring of 2008, site visits to four major law enforcement agencies were conducted by subject-matter experts. During the site visits (Los Angeles, California; Chicago, Illinois; Boston, Massachusetts; and Miami-Dade, Florida, Police Departments), a number of findings were identified in order to develop a standardized approach to the reporting of suspicious activity in the United States.

Major Findings

1. **Executive Leadership**
   - Leadership must recognize the importance of implementing a SAR process.
2. **Privacy and Civil Liberties Protections**
   - Implement an agency privacy policy.
3. **Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity (SAR Process)**
   - Identify existing SAR processes and determine what SAR processes need to be developed.
   - Incorporate national guidelines into standard operating procedures.
4. **Standard Reporting Format and Data Collection Codes**
   - Institutionalize the SAR process within the agency.
5. **Training and Community Outreach**
   - Train all agency personnnel on the SAR process.
   - Educate the community on the SAR process.
6. **Technology**
   - Partner with others, and connect to information sharing networks.

Major Findings

Executive Leadership

1. Strong executive leadership is an essential element leading to the success of any SAR program.

2. Agencies should educate and gain the support of policymakers.

Privacy and Civil Liberties Protections

1. Local law enforcement entities should incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public.

2. Agencies should evaluate and update, if necessary, their privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of information regarding terrorism-related criminal activity are specifically addressed.

3. The policy should be transparent and communicated with the public, community organizations, and other groups as appropriate.

Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity (SAR process)

1. The SAR process is critical to preventing crimes, including those associated with domestic and international terrorism.

2. Local law enforcement entities should incorporate the gathering, documenting, processing, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence.

3. Local law enforcement agencies or agencies with original jurisdiction are the initial collection points and investigative leads for all suspicious activity data. Suspicious activity submissions should not bypass the local law enforcement agency and the standard 911 reporting systems.

4. When an agency receives information that impacts another jurisdiction, it is the responsibility of the receiving agency to immediately notify the impacted agency and discuss coordination, deconfliction, investigation, and vetting procedures with the impacted agency. Once vetted, further dissemination of the information will be the responsibility of the impacted agency.

5. A defined process is needed by the originating agency to ensure that suspicious activity reporting is made available to fusion centers and local Joint Terrorism Task Forces (JTTF) in a timely manner.

6. An ongoing emphasis should be placed on defining and communicating trends in terrorism activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.

Standard Reporting Format and Data Collection Codes

1. There is a need for a common national methodology for the sharing of suspicious activity data in order to discern patterns across the country.

2. Utilizing a standard reporting format and common national data collection codes is essential to identifying local, regional, and national crime trends.

Training and Community Outreach

1. Training is a key component of the SAR process—all relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.

2. Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.

Technology

1. Technology and use of common national standards enhance the capability to quickly and accurately analyze suspicious activity data in support of controlling and preventing criminal activity.

2. Agencies should explore the concepts and use of virtual fusion centers that are accessible to all law enforcement personnel via a Web-enabled interface.

Considerations for Further Actions on the National Level

- Develop a set of common national data collection codes in order to allow for common analysis of data across jurisdictions.

  a. Formulate a working group to consolidate and standardize the suspicious activity to be reported and shared. Currently, a number of agencies have identified certain activities to be reported and assigned codes for those activities. In addition, the *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)* Version 1.0 (ISE-SAR Functional Standard) and the DOJ Information Exchange Package Document (IEPD) identify activities to document and share. In order to have a consistent methodology to share SAR data, these activities and codes need to be standardized.

- The findings and recommendations developed in this report are supported by the Major Cities Chiefs Association; however, the report is not a template solely for major cities. Smaller agencies and jurisdictions can also utilize this report in establishing a SAR process. For agencies that do not currently have a method to document, process, analyze, and share suspicious activity, training and technical assistance should be provided.

- Update the common definition for *suspicious activity*. The ISE-SAR Functional Standard defines suspicious activity as "observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention."[4]

  a. Consideration should be given to update the definition to include "observed incident or behavior."

  b. Additionally, while the ISE-SAR Functional Standard provides a comprehensive list of examples of suspicious activity, the definition lists only two categories: intelligence gathering and preoperational planning. Although most SARs may fall into these categories, not all will. For example, the suspicious activity may be an actual attack or other crime. It may be a report of a suspicious association or material that supports activity. Because of these limitations, consideration should be given to expanding the definition: "Reported or observed activity and/or

4 *Information Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)* Version 1.0, p. 6. For additional information, go to www.ise.gov/pages/ctiss.html.

behavior that, based on an officers training and experience, is believed to be indicative of criminal activity associated with terrorism."

- Emphasis should be placed on the analytical component of the SAR process. Analysis is vital to the success of the SAR process to ensure that the information gathered is properly vetted and analyzed to determine its credibility. Information that is shared should document the current status of the SAR to indicate factors such as whether an investigation was opened, whether the SAR was referred to another agency, or whether it was unresolved, before it is shared with other agencies.

- Develop a common national methodology to share SAR data in a timely manner. This methodology should articulate how SAR information will be shared with other law enforcement agencies, both horizontally and vertically, and how privacy and civil liberties policies of the originating agencies will be protected.

- Agencies should leverage the ISE Privacy Guidelines, Global privacy products, and tenets of 28 Code of Federal Regulations (CFR) Part 23 to evaluate, update, or develop privacy and civil liberties protection policies. Law enforcement agencies across the nation operate under privacy and information-handling frameworks that are governed by state law, local ordinances, judicial decrees, and federal regulation. Some jurisdictions may have more restrictive privacy procedures than others; however, there is a need for common procedures and standards to facilitate data sharing while protecting privacy and civil liberties. During the site visits, each agency described slightly different decision-making processes that would determine at what point SAR information actually becomes intelligence and subsequently subject to 28 CFR Part 23 requirements. The determination of when a SAR becomes controlled by the tenets of 28 CFR Part 23 needs to be clearly defined by the agency.

- Develop a standardized training program in order to provide consistent nationwide SAR training. Although there are a number of training programs regarding terrorism awareness, there should be a common understanding of what is needed to appropriately gather, process, report, analyze, and share suspicious activity. A standardized training program would also address the use of the common national data collection codes and methodology, as well as provide an understanding of the importance of protecting privacy and civil liberties.

  a. It is critical that a national training protocol be developed for the sharing of SAR data, and it is the responsibility of each agency to train on its collection process.

Introduction

Local law enforcement agencies are critical to efforts to protect our local communities from another terrorist attack. Fundamental to local efforts to detect and mitigate potential terrorist threats is ensuring that frontline personnel are trained to recognize and document behaviors and incidents indicative of criminal activity associated with domestic and international terrorism. Daily, there are more than 17,000 local law enforcement agencies in the United States that document information regarding suspicious criminal activity, including that related to terrorism. In the absence of national guidance, individual jurisdictions have independently developed intradepartmental policies and procedures for gathering and documenting Suspicious Activity Reports (SARs); however, the lack of standardization has restricted the efficient analysis and sharing of this information on a regional and/or national basis.

The ISE-SAR Functional Standard defines a Suspicious Activity Report (SAR) as "official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention."

The SAR process is the gathering, processing, reporting, analyzing, and sharing of suspicious activity.

The purpose of the *Findings and Recommendations of the SAR Support and Implementation Project* is to describe the gathering, processing, reporting, analyzing, and sharing of suspicious activity (SAR process) by the local police agency. This report and its recommendations are important for establishing national guidelines that will facilitate the improved sharing of SAR information. While these recommendations are intended to bring about standardization of the SAR process, every jurisdiction should develop policies and procedures that take into account the unique circumstances and relationships within that community.

The ISE-SAR Functional Standard defines a Suspicious Activity Report as "official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention."[5] The SAR process focuses on what law enforcement agencies have been doing for years—gathering information and establishing a process

5 Ibid., p. 3. For additional information, go to www.ise.gov/pages/ctiss.html.

whereby information can be shared to detect and prevent criminal and terrorist activity. Standardizing the SAR process will assist local law enforcement agencies in incorporating efforts involving the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious behaviors and incidents into the processes and systems used to manage other crime-related information and criminal intelligence. As part of this effort, law enforcement agencies should encourage the principles of intelligence-led policing (ILP) to involve and interact with other agencies in the reporting of suspicious activity to identify and prevent criminal and terrorist activity.

The *Findings and Recommendations of the SAR Support and Implementation Project* report was developed to provide recommendations to the Criminal Intelligence Coordinating Council (CICC)[6] from the Major Cities Chiefs Association (MCCA).[7] To develop these findings and recommendations, site visits were conducted at police departments in Los Angeles, California; Chicago, Illinois; Boston, Massachusetts; and Miami-Dade, Florida, to observe and document their SAR practices and processes. The site visit teams were selected by the sponsoring agencies—the Bureau of Justice Assistance (BJA), U.S. Department of Justice (DOJ); MCCA; DOJ's Global Justice Information Sharing Initiative (Global); CICC; the U.S. Department of Homeland Security (DHS), and the Federal Bureau of Investigation (FBI). After the site visits, the *Findings and Recommendations of the SAR Support and Implementation Project* report was developed by the SAR Executive Steering Committee, which was composed of local, state, and federal agencies representing the CICC, the Global Advisory Committee (GAC),[8] and the MCCA. Promising practices from these site visits were identified and are detailed throughout this report. In June 2008, the *Findings and Recommendations of the SAR Support and Implementation Project* was presented for review to the MCCA, which is composed of the 64 largest police departments in the United States and Canada, and was unanimously approved. It was presented to and unanimously approved by the CICC in September 2008 and the GAC in October 2008.

Through this effort, several key areas regarding the implementation of the SAR process were identified: Executive Leadership; Privacy and Civil Liberties Protections; Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity; Standard Reporting Format and Data Collection Codes; Training and Community Outreach; and Technology. This report examines each of these issues, provides information on the findings, and presents SAR process implementation recommendations. Following the issue-specific findings and recommendations, the report examines promising practices identified from the site visits.

6 For more information on the CICC, visit www.iir.com/global/council.htm.
7 For more information on the MCCA, visit www.majorcitieschiefs.org/.
8 For more information on the GAC, visit www.iir.com/global/committee.htm.

Section One:
Executive Leadership

Issue-Specific Findings

- **Strong executive leadership is an essential element leading to the success of any SAR program.**
- **Agencies should educate and gain the support of policymakers.**

The efficient documentation and analysis of suspicious activity by local law enforcement agencies is an important process that could potentially lead to the prevention of crime, including that involving individuals or groups motivated to commit acts of violence and other crime due to political ideology. Therefore, it is imperative that the Chief Executive understand the importance of the SAR process and the protection of privacy and civil liberties. Incorporating terrorism-related SARs into the processes and systems used by local entities to identify and mitigate emerging crime problems is an achievable goal for all agencies, regardless of agency size or jurisdiction served. In order to implement this program, Chief Executives must lead by example—clearly integrating the SAR process into their strategic, operational, and tactical decisions—thereby demonstrating their confidence in the approach and providing evidence of how the reporting of suspicious activity using a documented process helps to achieve the agencies' goals.

The Chief Executive must be an effective spokesperson to champion the SAR program. Chief Executives must ensure that line officers and other first responders understand their significant role and responsibility in the collection of suspicious activity. It is equally important that the Chief Executive communicate the goals and objectives of the SAR program with other stakeholders, such as external government agencies, appropriate private sector partners, security officials, and the general public. Providing this communication serves to inform the stakeholders of how the agency is identifying suspicious activity and how that activity is used to make the community safer.

Intelligence-led policing (ILP) is a process for enhancing law enforcement agency effectiveness toward reducing crimes, protecting community assets, and preparing for responses. ILP provides law enforcement agencies with an organizational framework to gather and use multisource information and intelligence to make timely and targeted strategic, operational, and tactical decisions. Chief Executives should understand the importance of ILP and its foundational approach to the SAR process. The data derived from the SAR program feeds directly into and supports the agency's ILP approach.

It is essential that the suspicious activity reporting processes within law enforcement agencies be transparent to the public. The agencies' policies, practices, and safeguards should be made known in such a way as to alleviate any public apprehension concerning police activities and attempts to detect and deter terrorist and other criminal activity. The Chief Executive plays the lead role in developing this transparency.

SAR Process Implementation Recommendations

- The Chief Executive must spearhead the efforts to gather, process, report, analyze, and share suspicious activity:
  - Institutionalize the gathering of suspicious activities and information at the street level, and standardize the reporting of such data so that it may be shared with other appropriate agencies.

- Educate and gain the support of the policymakers:
  - Legislature
  - Mayor
  - City Council
  - County Commissioners
  - Police Commissions
- Recognize and take steps to overcome any potential impediments or barriers to information sharing.
- Foster a culture that stresses the importance of sharing SAR information both horizontally and vertically.
- Incorporate counterterrorism efforts into an all-crimes approach for collecting suspicious activity.
- Apply the principles of ILP to the SAR process.

- The Chief Executive must issue an order directing the gathering, processing, reporting, analyzing, and sharing of suspicious activity.
  - The order should be directed to all members at all levels of the agency.
  - The order should address the use of a mechanism to provide feedback to the original submitter of the information.
  - Privacy and civil liberties protection concerns should be integrated into the order.
  - The order should address the evaluation of all members of the agency to ensure they are compliant with the SAR process.
- Accountability for consistent gathering, processing, reporting, analyzing, and sharing of SAR data should be developed at all levels of the organization.
- Accountability can be achieved through evaluations, COMPSTAT-type operations, performance metrics, and other accountability mechanisms.
  - The Chief Executive should leverage national SAR coordination efforts in order to counter and respond to threats that may affect his or her community.

Promising Practices Identified During the Site Visits

The site visits provided several promising practices related to the role of the Chief Executive. These include:

- Execution of an order mandating the reporting of suspicious activity from all officers. This ensures that all members of the agency are involved in the SAR process.
- Development of a robust communication campaign to promote the SAR program within the agency and outside the agency with the external community stakeholders.
- Emphasizing the importance of sharing information versus stockpiling it. Accepting the mind-set that information must be shared in order to make the program successful is an essential philosophy that all Chief Executives must adopt.
- Utilizing SAR programs to enhance ILP activities, providing an integration of the two concepts and a seamless approach to identifying and addressing jurisdiction risks and threats.
- Utilizing the *Information Exchange Package Document for the Suspicious Activity Report (SAR) for Local and State Entities IEPD* v1.01[9] and the I*nformation Sharing Environment (ISE) Functional Standard (FS) Suspicious Activity Reporting (SAR)* Version 1.0 to share SARs developed by local agencies with fusion centers, JTTFs, and other appropriate agencies. The Chief Executive will need to manage the development of the internal information technology systems to comply appropriately.

9 For more information, visit www.niem.gtri.gatech.edu/niemtools/iepdt/display/container.iepd?ref=woqtAeBWVYM%3D#.

Section Two:
Privacy and Civil Liberties Protections

Issue-Specific Findings

- **Local law enforcement entities should incorporate the gathering, processing, reporting, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public.**
- **Agencies should evaluate and update, if necessary, their privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of information regarding terrorism-related criminal activity are specifically addressed.**
- **The policy should be transparent and communicated with the public, community organizations, and other groups as appropriate.**

In order to balance law enforcement's ability to share information with the rights of citizens, appropriate privacy and civil liberties policies must be utilized.[10] Agencies should establish their SAR process in a manner that is consistent with existing privacy and civil liberties policies. A strong privacy and civil liberties policy will not only protect the rights of the citizens but also protect the agency.

SAR Process Implementation Recommendations

- In recognition of their state laws and local ordinances, agencies should promote a policy of openness and transparency when communicating with the public regarding their SAR process.
- When developing an order to mandate the SAR process, agencies should clearly articulate when 28 CFR Part 23 should be applied.
- Consistent with federal, state, and local statutory and regulatory requirements, agencies should ensure that key privacy-related issues—such as accuracy, redress, and purging—are addressed in their existing privacy and civil liberties policy.
- When developing the SAR process, agencies should review and consider their jurisdictional and state laws and local ordinances regarding the retention, disposition, and release of information.

10 *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New Era*, p. 41. For more information regarding the *Fusion Center Guidelines*, visit www.it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

- Random audits of the quality and substance of reports should be conducted in order to ensure that the integrity of the program is maintained and that appropriate respect and attention are given to reasonable suspicion and other civil rights issues.

Promising Practices Identified During the Site Visits

The site visits provided several promising practices related to privacy protection. These include:

- Utilizing interagency privacy agreements and standardized vetting mechanisms.
- Mandating supervisory review of SARs to ensure that all of the information has been properly reviewed and evaluated.
- Utilizing legal/privacy advisors in the development of the SAR process.

Section Three:
Gathering, Processing, Reporting, Analyzing, and Sharing of Suspicious Activity

Issue-Specific Findings

- **The SAR process is critical to preventing crimes, including those associated with domestic and international terrorism.**
- **Local law enforcement entities should incorporate the gathering, documenting, processing, analyzing, and sharing of terrorism-related suspicious activities and incidents into existing processes and systems used to manage other crime-related information and criminal intelligence.**
- **Local law enforcement agencies or agencies with original jurisdiction are the initial collection points and investigative leads for all suspicious activity data. Suspicious activity submissions should not bypass the local law enforcement agency and the standard 911 reporting systems.**
- **When an agency receives information that impacts another jurisdiction, it is the responsibility of the receiving agency to immediately notify the impacted agency and discuss coordination, deconfliction, investigation, and vetting procedures with the impacted agency. Once vetted, further dissemination of the information will be the responsibility of the impacted agency.**
- **A defined process is needed by the originating agency to ensure that suspicious activity reporting is made available to fusion centers and local Joint Terrorism Task Forces (JTTF) in a timely manner.**
- **An ongoing emphasis should be placed on defining and communicating trends in terrorism activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.**

As detailed in the ISE-SAR Functional Standard, the ability to collect and process suspicious activity requires agencies to implement five key components: information acquisition, organizational processing, integration and consolidation, data retrieval and distribution, and feedback.[11] The information acquisition component includes the gathering and documentation of all suspicious activity. After the information is acquired and documented, it is then validated through organizational processing, in which data is reviewed and vetted by a

11 Additional information regarding the ISE-SAR Functional Standard can be found at www.ise.gov/pages/ctiss.html.

trained supervisor.[12] Once the information is validated as a terrorism-related SAR, it will be made available to both the fusion center and the local JTTF in a timely manner.

SAR Process Implementation Recommendations

- All agencies, regardless of size, have a responsibility to develop and implement a process for gathering, processing, reporting, analyzing, and sharing suspicious activity information within their jurisdiction.
- The agency SAR process and policies should detail the specific suspicious activities to report and should include:
  - A clear scope of when suspicious activity should be reported.
  - How other crimes with a possible nexus to terrorism activity should be reported.
  - A clear description of how the agency processes the suspicious information. This description should address the following questions:
    - How should the submitting officer document the information?
    - How is the information reviewed by the chain of command?
    - What SAR-related data should be made available to the fusion center and JTTF?
    - Who should analyze SAR data?
    - At what point in the process does the information become a SAR?
    - What method is used for routing the SAR to other appropriate agencies/organizations?
    - What methodology is used to provide feedback to the original collector/submitter of the SAR data?
- In order to leverage resources and avoid duplicative efforts, agencies should utilize existing information technology, common systems, and information sharing relationships so that SAR information can be shared more broadly and effectively.
- Agencies should consider a modification of their current reports—basic incident report, offense report, information report, or field interview report—to include fields to capture SAR data in a simplified reporting process.
  - Consider adding a checkbox that will flag the report as containing suspicious activity to ensure evaluation and appropriate routing within the agency.
- The coding of SARs should be done at a central point within the agency by subject-matter experts trained in identifying terrorism precursor activities.
  - Enable line officers to provide a summary-level description of the activity in their reports.
- All SARs should receive an initial vetting within 24 hours, and recommendations should be made regarding whether to respond, refer, or take other action.
  - Local agencies should utilize fusion center resources for the evaluation of SARs if internal resources are not available.
- The SAR process should include a comprehensive analytic component.
  - Analysis is vital to the success of the SAR process, and emphasis should be placed on the analytical component.
  - Agencies should utilize fusion center analytic resources if internal resources are not available.
  - Through training, agency analysts should receive a clear understanding of their roles and responsibilities regarding the SAR process.
- Upon completion of local agency vetting and when a nexus to terrorism has been identified, agencies should immediately engage their counterterrorism assets to include investigators, analysts, and intelligence units. Terrorism-related SARs must be

12 The evaluation of the collected suspicious activity data is essential to understanding the full importance and value of the data. Reports identified as containing suspicious activity should be immediately provided to the supervisor for further evaluation and action.

made available to the local JTTF and fusion center in a timely manner to support further investigative action and/or regional analysis.

- Agencies should coordinate with appropriate entities to ensure that SARs are made available to and from appropriate agencies/organizations:
  - The FBI JTTF: located at 106 locations across the United States, the JTTFs' mission is to detect, disrupt, and dismantle terrorist cells and networks in the United States and prevent acts of terrorism by individuals acting alone.
  - FBI Field Intelligence Group (FIG)
  - State and major urban area fusion centers
  - FBI InfraGard
  - DHS Information Sharing and Analysis Center (ISAC)
  - Terrorism Early Warning (TEW) Group
  - Other intake points/jurisdictional-specific programs; i.e., tip lines, the Internet, "Text-a-Tip"
  - Other regional or local intelligence centers with a need and/or right to know
  - Other homeland security units
- Information that is shared should document the current status of the SAR to indicate factors such as whether an investigation was opened, whether the SAR was referred to another agency, or whether it was unresolved, before it is shared with other agencies.
- Once a SAR has been evaluated, feedback should be provided to the original submitter via the liaison officer or other established mechanism.

Promising Practices Identified During the Site Visits

The site visits provided several promising practices related to the gathering, processing, reporting, analyzing, and sharing of suspicious activity. These include:

- Modifying existing reports—offense, incident, information, or field interview reports—to accommodate the reporting of suspicious activity. This provides for rapid institutionalization and requires little additional reporting by the officer. Including a SAR checkbox directs the report to the evaluation process.
- Developing an "E-Tips" system for external stakeholders—such as citizens, private industry, and other nongovernmental security agencies—to provide the ability to report suspicious activity information back to the law enforcement agency via the Internet for further evaluation.
- Utilizing technology to notify affected parties of a potential risk or threat. Providing a rapid response to mitigate potential incidents highlights the importance of how suspicious activities are processed and disseminated within the agency.
- Utilizing a separate repository system for SAR assessments and providing a full-time officer to review the system output.
- Developing of a process to make SARs that are related to terrorism available to the JTTF, fusion centers, or other law enforcement agencies with a demonstrated right or need to know.
- Utilizing an offense, incident, information, field interview, or general incident report to collect suspicious activities rather than creating a new form.
- Utilizing a SAR evaluation team as an effective strategy for vetting incoming information.
- Evaluating the use of field interview reports to collect SAR data. These reports must be timely in order to be useful to the SAR process.

Section Four:
Standard Reporting Format and Data Collection Codes

Issue-Specific Findings

- **There is a need for a common national methodology for the sharing of suspicious activity data in order to discern patterns across the country.**
- **Utilizing a standard reporting format and common national data collection codes is essential to identifying local, regional, and national crime trends.**

A standard reporting format is a key element of the effective implementation of a SAR program. A standardized report provides a mechanism for the efficient transition of the suspicious activity from the line-level officer to the agency management. This process will ensure that the suspicious activity is being collected and reported correctly and will regulate the reporting procedures across the agency.

Additionally, in order to identify local, regional, and national trends in crime and terrorist precursor activity, a common national set of data collection codes needs to be adopted to ensure seamless sharing and analysis of suspicious activity. This national standard of codes will ensure that patterns of criminal behavior are identified and handled properly. The establishment of these codes needs to be the result of evaluation and determination that the activities to be collected are likely precursors of terrorist activity.

The Los Angeles Police Department (LAPD) has developed data collection codes for the reporting of suspicious activity. These codes provide the method for documenting behavioral indicators that have a potential nexus to terrorism. LAPD uses the codes to train its personnel in the recognition of suspicious activity. The process is continuing to mature as LAPD conducts research to develop patterns and determine frequency of use with the codes. A sample of LAPD's data collection codes is located in Appendix C of this document.

SAR Process Implementation Recommendations

- Ensure that the SAR reporting mechanism is streamlined and efficient.
- Adhere to national standards when creating a reporting process:
  - Use commonly accepted data collection codes when developing reports.
  - Develop a sharing process that complies with the ISE-SAR Functional Standard.[13]
  - Follow the *Information Exchange Package Document for the Suspicious Activity Report (SAR) for Local and State Entities IEPD v1.01*[14] for reporting.
  - Utilize the National Information Exchange Model (NIEM)[15] data standards.
- Use a standard reporting format and data collection codes to efficiently identify the indicators of terrorist precursor activities.

13 For additional information regarding the ISE-SAR Functional Standard, visit www.ise.gov/pages/ctiss.html.

14 For additional information regarding the *Information Exchange Package Document for the Suspicious Activity Report (SAR) for Local and State Entities IEPD, v1.01*, visit www.niem.gtri.gatech.edu/niemtools/iepdt/display/container.iepd?ref=woqtAeBWVYM%3D#.

15 For additional information regarding NIEM, visit www.niem.gov.

- SAR policies and systems should provide for a review of the coding in order to allow for expansion or redaction dependent upon lessons learned and emerging national and international trends and tactics in terrorism.

- Audits should be completed to ensure appropriate screening and accurate coding of completed reports and associated entry into statistical systems.

Promising Practice Identified During the Site Visits

The site visits provided a promising practice related to the use of standard reporting formats and the use of criteria codes:

- Suspicious activity can provide a link to precursor terrorist activity. Agency evaluation of the suspicious activity collection process can demonstrate that the collection of this information is consistent with the protection and safety of the community.

Section Five:
Training and Community Outreach

Issue-Specific Findings

- **Training is a key component of the SAR process—all relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.**
- **Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.**

Training is a vital component of the implementation of a SAR process within an agency. SAR training must be provided throughout the department to ensure that the SAR process is institutionalized within the agency. In addition to in-service and roll-call training, distance learning or e-training capabilities are becoming a readily available option to law enforcement agencies. E-training can facilitate SAR training to personnel with schedules that do not permit them to attend traditional classroom training and will help ensure that everyone within the law enforcement agency is trained. External stakeholders should be trained and alerted regarding the concept of suspicious activity and where/when to report it. Educating the entire spectrum of stakeholders regarding the SAR process will help ensure that suspicious activity is properly reported and addressed accordingly.

SAR Process Implementation Recommendations

- Agencies must implement a training program that reaches all levels of law enforcement personnel so that they can recognize the behaviors and incidents that represent terrorism-related suspicious activity.
  - Training for both law enforcement and the public should be conducted in a phased approach. It should be updated regularly and provided on an ongoing basis. Training should include:
    - The SAR program and basic reporting.
    - Detailed training on the recognition of reportable behaviors.
  - Training must be provided to in-service law enforcement personnel and basic recruits on the SAR process. Training should include but not be limited to the following:
    - Recruits or cadets
    - Dispatch center personnel
    - Analysts
    - Records clerks or records management system (RMS) personnel
    - Patrol officers/deputies
    - Line supervisors
    - Executive and command-level personnel
    - Governance board members
    - Other stakeholders as appropriate
  - Training should:
    - Emphasize that all personnel, regardless of position, have an important role in the

collection, processing, analysis, and reporting of SAR data.

- Emphasize that SAR reporting is based on observable/articulable behaviors and not individual characteristics such as race, culture, religion, or political associations.
- Include the protection of privacy and civil liberties.
- Instruct personnel on how to use new reports and/or technology.

◊ Agencies should use cases and other examples to illustrate the usefulness of suspicious activity reporting as a tool to mitigate criminal activity associated with terrorism.

◊ Agencies should consider the use of one-page training bulletins to help identify the current and emerging trends of the SAR process.

◊ When resources are available, agencies should consider the use of e-training to reach out to individuals and ensure that agency personnel are trained in the SAR process.

♦ Law enforcement agencies should develop a liaison officer program to help ensure that terrorism-related suspicious activity is being gathered and reported to the proper personnel, local JTTFs, and fusion center.

◊ Liaison officers may be utilized as "train the trainer" assets and assist in standardizing and reinforcing the SAR policy throughout an agency. They frequently provide a more local or immediate resource to many frontline officers and units (especially in larger agencies).

◊ The liaison officer program will help expand and augment the SAR process and ensure that feedback is being provided to the original submitter.

◊ The liaison officer program will help foster trust between law enforcement agencies and the public and private sector.

♦ Agencies should provide feedback for training programs and updates through the auditing of completed reports to identify common errors, omissions, and training/knowledge gaps.

♦ Agencies should develop outreach material for other first responders, the public, and the private sector to educate them on the recognition and reporting of behaviors and incidents indicative of criminal activity associated with international and domestic terrorism. Outreach material could include but is not limited to the following:

◊ Internet-based newsletters

◊ E-mail notification to targeted stakeholders

◊ Officer-to-citizen interaction programs

◊ Media commercials outlining the program goals and how stakeholders can help

◊ Community awareness/training classes

◊ Informational fliers

◊ Distribution of CDs and DVDs related to the reporting of suspicious activity

◊ Distribution of a redacted daily report to appropriate stakeholders

◊ BJA's Communities Against Terrorism (CAT) CD

Promising Practices Identified During the Site Visits

The site visits provided several promising practices related to the importance of training. These include:

♦ Employing terrorism awareness training to inform officers and other stakeholders on what to look for regarding suspicious activity and how to report this activity.

♦ Utilizing Internet-based newsletters to communicate with other stakeholders, such as the business community and private security contacts.

♦ Utilizing liaison officer programs to provide direct liaison with other community partners, such as fire departments, university police, and area probation/parole partners.

♦ Utilizing community outreach and awareness programs to provide agencies with feedback and information from the community.

♦ Utilizing a daily report with redacted sensitive information to communicate information to the private sector.

♦ Utilizing the Communities Against Terrorism (CAT) Program developed by BJA, Office of Justice Programs, DOJ. This program provides agencies with ready-made materials to assist public and private sector organizations with the identification and reporting of suspicious activity.

Section Six: Technology

Issue-Specific Findings

- **Technology and use of common national standards enhance the capability to quickly and accurately analyze the suspicious activity data in support of controlling and preventing criminal activity.**
- **Agencies should explore the concepts and use of virtual fusion centers that are accessible to all law enforcement personnel via a Web-enabled interface.**

Technology is an important component in the reporting of suspicious activity. It can dramatically aid in the gathering, processing, reporting, analyzing, and sharing of information. The use of technology should be customized for each agency depending on size and jurisdiction served. Agencies should consider incorporating the SAR program into existing administrative, reporting, and criminal intelligence processes and systems. It is also important to consider new technology to provide important analytical and geospatial visualization tools to support intelligence-led policing decisions. While these technologies support a variety of all-crimes analysis objectives, they are an important resource in determining whether a SAR indicates a potential nexus with past or suspected terrorist activities.

Predominant among the emerging technologies is the deployment of systems that allow for the analysis of information (incident reports, field interviews, and tips) currently stored in numerous legacy systems and identification of links and relationships that were not previously evident.

SAR Process Implementation Recommendations

- Agencies should adopt national information sharing standards to enhance their capability to quickly and accurately analyze stored information, such as:
  - ISE-SAR Functional Standard
  - State and Local Agency IEPD for SAR reporting
  - National Information Exchange Model (NIEM)
  - Records Management System (RMS) and Computer Aided Dispatch (CAD) functional standards
- Agencies should strive to use an electronic reporting system for field incident reports, including the reporting of SARs. This will improve the timeliness of the activity reporting process.
  - It is critical that agencies have a defined process of sharing SAR information with fusion centers and JTTFs.
  - Agencies must strive to implement a technical solution for the routing of SARs to a central analytical or processing location within the agency or directly to fusion centers when the agency does not have the capacity to accomplish this.
- Agencies should build upon existing systems and methods such as:
  - Offense reports
  - Incident reports
  - Information reports
  - Field interview reports

- General incident reports
- Incident reports

- Agencies should implement mapping tools to provide a better understanding of suspicious activities occurring in their jurisdiction.

- Audits should be conducted to ensure the validity of statistical reports—via comparisons in radio calls and specialized unit notifications—and contribute to the refinement process for statistical and analytical products.

- A secure electronic communications network—such as the Regional Information Sharing Systems®, Law Enforcement Online, Nlets—The International Justice and Public Safety Network, the Homeland Security Information Network, or any secured criminal justice network—should be utilized to share the SAR information with other jurisdictions.

Promising Practices Identified During the Site Visits

The site visits provided several promising practices related to the development and use of technology. These include:

- Utilizing a "hot spot" mapping process to identify patterns and areas of needed resources.

- Implementing systems to combine data from disparate systems to allow for a more complete analysis of the data.

- Deploying mapping tools to allow for a complete understanding of suspicious activity and its relationship to critical infrastructure.

- Modifying existing information technology products to accommodate the SAR process.

- Utilization of a virtual fusion center as a platform for regional partners to share information and establish alerts when a new SAR is entered.

Site Visit Overviews

This is a review of the technology that is deployed by the agencies that were visited during this project.

Chicago Police Department

The centerpiece of the Chicago Police Department (CPD) Information Technology (IT) infrastructure is the Citizen Law Enforcement Analysis and Reporting (CLEAR) system. The CLEAR database, initially deployed in April 2000, is the foundation for a growing set of integrated CLEAR applications used by CPD officers and civilians, plus an exponentially expanding base of users outside the city limit. Thousands of queries are issued daily against the system since CLEAR is an integral IT component supporting all law enforcement and investigative functions.

In April of 2007, CPD opened its Crime Prevention & Information Center (CPIC), which has taken CLEAR's power to a new level. The CPIC's "all-crimes" concept design has literally changed the investigative culture of the Chicago Police Department. The Detective Division's entire staff of around-the-clock crime analysts has returned to the field due to the high-powered, real-time support of the CPIC. The CPIC has federated countless data sources and fused them together with geospatial mapping, gunfire detection technology, live CAD feeds, and even violence predictor programs. This wave of investigative support begins as 911 call takers start their process and is literally triggered before calls are dispatched to police on the street. This same technology supports terrorism-related investigations by the JTTF.

The state of Illinois has recognized Chicago's technological advancements and has decided to join the CLEAR community in order to provide a uniform incident reporting system and facilitate information sharing in the entire state. This additional component, called I-CLEAR (for Illinois-CLEAR) has been operational since 2006. In the summer of 2008, development began on R-CLEAR (for Regional-CLEAR), a federally grant-funded expansion of I-CLEAR. This will extend CLEAR access across multiple state borders and provide a regional information sharing environment.

Los Angeles Police Department

As the third-largest police department in the United States, the Los Angeles Police Department (LAPD) has dedicated significant resources and senior management focus to the identification and tracking of suspicious activities within the city and beyond. Like Chicago, Boston, and Miami-Dade, LAPD has developed a very close working relationship with the local JTTF.

This close relationship extends to the sharing of IT resources in the Joint Regional Intelligence Center (JRIC). At the present time, all crime and incident data, including potential SARs, is first collected and processed through LAPD's Consolidated Crime Analysis Database (CCAD) system, which was first deployed in 1995 at LAPD as the primary database for collection of initial crime data. The CCAD system has been refined to facilitate the collection of SARs. In addition to the historical crime data warehousing, CCAD is now also used to route potential SARs from frontline police officers and specialized units through the Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) incident review process. The subsequent review process by Major Crimes Division (MCD), CTCIB, includes a thorough classification of the SAR incident based on specific criteria codes recently introduced by LAPD and the basis of a key recommendation in this report. CCAD data also serves as one of the key internal data sources supporting LAPD's comprehensive COMPSTAT reporting system. It is important to note that

CCAD is utilized to store only preliminary information collected at the time the suspicious activity is initially reported, as well as the associated SAR coding—the CCAD system is siloed and contains no developmental information or intelligence.

At the time a SAR report is completed by officers, a review by first-line supervision determines whether immediate notification to MCD counterterrorism investigators is warranted. Further review of the SAR by MCD investigators is conducted within 24 hours, followed by entry into a separate Tips and Leads database with a direct interface to the regional fusion center (JRIC), providing them with real-time access to the SARs as they are entered. Within the JRIC, a review is conducted to determine whether the report meets predetermined criteria for assignment to the JTTF, at which time the information is provided in hard copy. At the moment, there is no electronic interface between CCAD and the JRIC case management system or between both systems and the FBI Guardian system used by the JTTF.

One of LAPD's strengths is the deployment of a sophisticated COMPSTAT application that essentially drives LAPD's intelligence-led policing model and allows resources to be allocated based on near real-time assessment of crime trends and patterns. Based on the classification of SAR codes and resulting geospatial visualization of potential SAR incidents, LAPD is the nation's leader in applying COMPSTAT technology to terrorism SAR investigations.

Boston Police Department

The Boston Police Department's Regional Intelligence Center (BRIC) was formed shortly after the 2004 Democratic Convention to take on an all-crimes mission. Like many organizations, the BRIC was saddled with an old records management system with limited analytical capabilities. As a solution, the BRIC implemented an in-house-designed data warehouse solution and built interfaces to the popular ESRI GIS software application. Each night, all incident data, including potential SAR reports, is loaded into the warehouse. BRIC analysts then search the warehouse for new incident records that may support ongoing investigations that include general crimes, gang violence and, of course, terrorist activities. Using the geospatial tools, analysts also track crime patterns and trends on map background and use these tools in daily briefings and investigative reports.

Once the BRIC determines that incident data (terrorism or criminal indicators) is important to an intelligence case, data from the data warehouse and/or RMS is exported to an intelligence case management system that has also been procured by the Massachusetts State Police for use in the state fusion center. Future plans include connecting the two systems to permit data exchange. At the moment, the BRIC has no electronic exchange process with the JTTF or eGuardian. In addition, Massachusetts rolled out the State-Wide Information Sharing System (SWISS) in July 2008. SWISS is designed to serve as both a statewide incident management resource as well as a connection point for the FBI Law Enforcement National Data Exchange system.

Miami-Dade Police Department

The Miami-Dade Police Department's Homeland Security Bureau (HSB) was recently designated by the U.S. Department of Homeland Security as the Miami-Dade Fusion Center. The IT infrastructure of the HSB, which was established in late 2005 with an all-crimes focus, represents a composite of systems and technologies in place at the other three sites. HSB relies upon all-crime incident data stored in an aging CAD/RMS. Upon first-line supervisor review, Offense Incident Report (OIR) data is input into the Crime Analysis System (CAS). CAS was built in-house seven to eight years ago and is well used by HSB investigators and analysts. Recently, however, HSB learned that it must replace CAS and has decided to implement a large data warehouse capability to both support more effective analysis as well as support extensive COMPSTAT functionality. Once incident data (terrorism SAR or criminal) achieves an intelligence threshold based on HSB guidelines, incident/case data from CAS is entered into an intelligence system. At the present time, the criminal intelligence system has no electronic interface to the JTTF, but the system is integrated into the JTTF and the FIG. However, the Southeast Florida Region, which is composed of 109 local law enforcement agencies, recently deployed an electronic solution to fill the gaps. The Southeast Florida Virtual Fusion Center enables the electronic sharing of information, including SARs, to all law enforcement partners and the Florida Fusion Center.

As a separate effort, Florida is in the process of implementing the Florida Law Enforcement Exchange (FLEX) system to centrally access all incident data. FLEX is designed to connect systems in each of the seven regions throughout the state. Miami-Dade expects to support a FLEX interface to its (to be developed) data warehouse in a year or two. With the deployment of the FLEX system, Florida is setting the stage for future information sharing of not only incident data but terrorism SAR data as well.

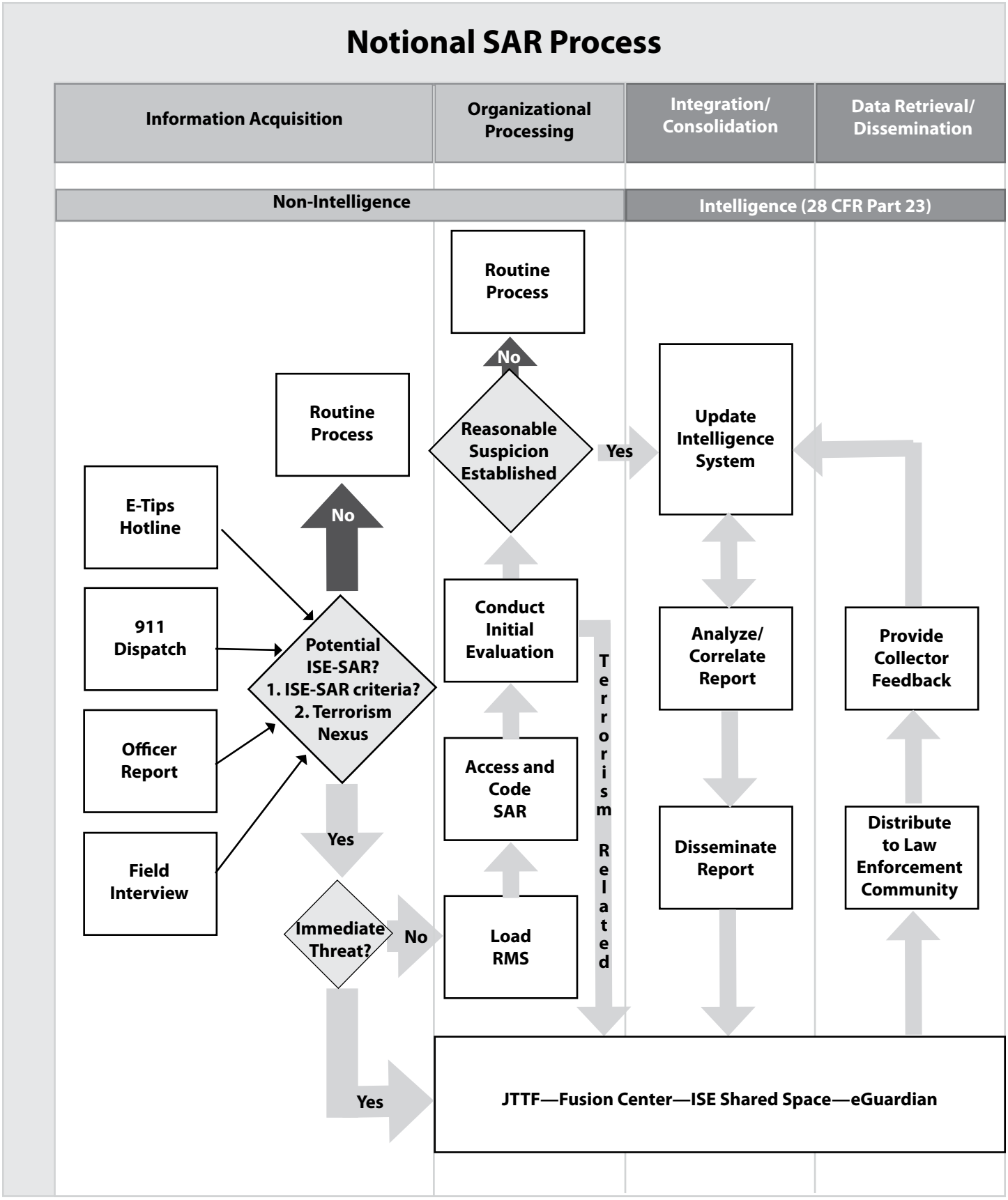
Notional SAR Flowchart

On the following page is a diagram, the Notional SAR Process, which represents a composite view of the processes used today by the four police departments identified in the study or discussed as a future direction for SAR reporting. As shown, SARs potentially pass through four general stages as defined in the ISE-SAR Functional Standard:

- **Information Acquisition** (how the information is originally collected, observed, or submitted)
- **Organizational Processing** (the series of manual and automated steps and decision points followed by the agency to evaluate the SAR information)
- **Integration and Consolidation** (the point at which SAR information transitions to intelligence and is then subject to 28 CFR Part 23 regulations)
- **Data Retrieval and Dissemination** (the process of making the intelligence available to other agencies and obtaining feedback on investigative outcomes)

Each agency employed different intake and preliminary review procedures to determine whether a report actually had a "potential" connection with terrorist activity subject to special treatment. In addition, as illustrated on the large horizontal box at the bottom of the diagram, each agency varied in the determination of when or if SARs are passed or made available to an external agency or system such as a JTTF or fusion center. More important, each agency described slightly different decision processes that would determine when SAR information actually became intelligence and subsequently subject to 28 CFR Part 23 requirements.

While the diagram illustrates some basic stages of a SAR processing cycle, the purpose of creating the activities or decision points shown was not to describe any particular agency's process but to highlight the primary steps that, as a group, all of the agencies followed to one degree or another.


Notional SAR Process
Information Acquisition
Organizational Processing
Integration/ Consolidation
Data Retrieval/ Dissemination
Non-Intelligence
Intelligence (28 CFR Part 23)
Routine Process
No
Routine Process
Reasonable Suspicion Established
Yes
Update Intelligence System
E-Tips Hotline
No
911 Dispatch
Potential ISE-SAR? 1. ISE-SAR criteria? 2. Terrorism Nexus
Conduct Initial Evaluation
Analyze/ Correlate Report
Provide Collector Feedback
Officer Report
Access and Code SAR
Terrorism Related
Field Interview
Yes
Disseminate Report
Distribute to Law Enforcement Community
Immediate Threat?
No
Load RMS
Yes
JTTF—Fusion Center—ISE Shared Space—eGuardian

Appendix A:
Project Team Members and Participants

U.S. Department of Justice's (DOJ) Bureau of Justice Assistance (BJA)—in partnership with the Global Justice Information Sharing Initiative (Global) Criminal Intelligence Coordinating Council (CICC), the U.S. Department of Homeland Security (DHS), and the Major Cities Chiefs Association (MCCA)—would like to thank the Los Angeles, Chicago, Boston, and Miami-Dade Police Departments for allowing the site team to visit and observe how their agencies handle suspicious activity. Recognition also needs to be made to the site team and executive steering committee members, whose support was instrumental in the development and vetting of the *Findings and Recommendations of the Suspicious Activity Reporting (SAR) Support and Implementation Project*. Everyone's assistance and dedication to this effort have contributed to the success of the SAR Support and Implementation Project.

Participating Agencies and Representatives

Los Angeles Police Department

Chief William Bratton
Officer Jim Buck
Sergeant Dino Caldera
Ms. Elizabeth Carrillo
Deputy Chief Michael Downing
Detective Jeff Godown
Reserve Officer Renee Greif
Detective Andy Grimes
Captain Joel Justice
Commander Joan T. McNamara
Lieutenant Shannon K. Paulson
Detective Stan Salas

Chicago Police Department

Mr. Terry Collins
Sergeant Paul Derosa
Lieutenant Daniel Godsel
Mr. James Hickey
Ms. Catherine Kolb
Commander Jonathan Lewin
Lieutenant James Marino
Lieutenant David McNaughton
Sergeant Mike Murphy
Lieutenant Leo Panepinto
Lieutenant Ronald Pontecore
Commander Ralph Price
Captain Martin Ryczek
Commander David A. Sobczyk
Assistant Deputy Superintendent Matthew Tobias
Superintendent of Police Jody P. Weis

Boston Police Department

Sergeant Detective Dan Coleman
Police Commissioner Edward Davis
Mr. Richard Laird
Deputy Superintendent Earl O. Perkins
Director Carl Walter

Miami-Dade Police Department

Ms. Lourdes De La Nuez
Sergeant Luis Fuste
Officer Jonathan Morris
Mr. John Murphy (Broward County, Florida, Sheriff's Office)
Mr. W. Scott Nugent (Palm Beach County, Florida, Sheriff's Office)
Sergeant Amado Ojeda
Director Robert L. Parker
Major Michael Ronczkowski
Chief Ricky Smith

Site Visit Team

Mr. Steven Ambrosini
Director of Operations
IJIS Institute

Mr. Robert P. Boehmer
Director
Institute for Public Safety Partnerships
University of Illinois at Chicago
Chair, GAC

Mr. Andrew Brock
Intelligence Officer
State and Local Fusion Center Program Office, DHS

Mr. Robert Cummings
Executive Vice President
Institute for Intergovernmental Research (IIR)

Mr. Thomas Frazier
Executive Director, MCCA

Mr. Stuart Frome
Section Chief
Office of Intelligence and Analysis, DHS

Mr. Ronald Leavell
Lieutenant
Washington State Fusion Center
Seattle, Washington, Police Department
Representing the MCCA

Mr. David Lewis
Senior Policy Advisor
Information Technology Office, Policy Division, BJA

Mr. Norman Lindsay
Deputy
Criminal Information Sharing and Analysis
Investigative Division
Hennepin County, Minnesota, Sheriff's Office
Representing the Major County Sheriffs' Association (MCSA)

Mr. Matthew Mattson
Research Associate, IIR

Ms. Suzette McLeod
Assistant Director
Project Management Services
IJIS Institute

Mr. Thomas J. O'Reilly
Senior Policy Advisor, BJA

Mr. Philip Ramer
Senior Research Associate, IIR

Mr. Donald Sutherland
Project Manager
Technical Assistance
IJIS Institute

Mr. Michael Tomczak
Representing the MCCA

Mr. James Welton
Lieutenant
Aurora, Colorado, Police Department
Representing the CICC

Mr. William A. Hipsley
Deputy Director
Information Analysis
California Office of Homeland Security

Mr. Paul Wormeli
Executive Director
IJIS Institute

Executive Steering Committee

Mr. Melvin Blizzard
Executive Director
Washington, DC, Regional Threat and Analysis Center

Mr. Ronald Brooks
Director
Northern California High Intensity Drug Trafficking Area
Regional Terrorism Threat Assessment Center
Vice Chair, CICC

Ms. Deborah Draxler
Branch Chief
Information Sharing and Collaboration
Office of Intelligence and Analysis, DHS

Mr. Thomas Frazier
Executive Director, MCCA

Mr. Thomas Galati
Deputy Chief
New York City Police Department

Mr. Richard Holland
Captain, Houston, Texas, Police Department

Mr. Clark Kimerer
Deputy Chief, Chief of Operations
Seattle, Washington, Police Department
MCCA

Ms. Joan McNamara
Commander, Assistant Commanding Officer, Counter-Terrorism and Criminal Intelligence Bureau
Los Angeles, California, Police Department

Mr. Daniel Oates
Chief of Police, Aurora, Colorado, Police Department, CICC

Mr. Thomas J. O'Reilly
Senior Policy Advisor, BJA

Mr. Russell M. Porter
Director, Intelligence Fusion Center,
Iowa Department of Public Safety
Chair, CICC

Mr. Robert Riegle
Director, State and Local Program Office
Office of Intelligence and Analysis, DHS

Mr. Richard Stanek
Sheriff, Hennepin County, Minnesota, Sheriff's Office, MCSA

Ms. Kathleen Suey
Deputy, Homeland Security Division
Las Vegas, Nevada, Metropolitan Police Department

Mr. Larry Trent
Director, Illinois State Police

Mr. Paul Wormeli
Executive Director
IJIS Institute

Appendix B:
Los Angeles Police Department Special Order Regarding SAR

OFFICE OF THE CHIEF OF POLICE

SPECIAL ORDER NO. 11
March 5, 2008

SUBJECT: REPORTING INCIDENTS POTENTIALLY RELATED TO FOREIGN OR DOMESTIC TERRORISM

PURPOSE:

Current anti-terrorism philosophy embraces the concept that America's 800,000 law enforcement officers fill a critical position in the area of terrorism prevention. Law enforcement authorities must carry out their counter-terrorism responsibilities within the broader context of their core mission of providing emergency and non-emergency services in order to prevent crime, violence and disorder. In support of this, the Department's Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) is engaging in an effort to more thoroughly gather, analyze and disseminate information and observations, of either a criminal or suspicious nature, which may prove critical to the intelligence cycle.

This Order establishes Department policy for investigating and reporting crimes and non-criminal incidents that represent indicators of potential foreign or domestic terrorism, and incorporates within the Department Manual a procedure for gathering and maintaining information contained in such reports.

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 activity 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).

PROCEDURE:

I. DEFINITIONS.

A. **Suspicious Activity Report.** A Suspicious Activity Report (SAR) is a report used to document any reported or observed activity, or any criminal act or attempted criminal act, which an officer believes may reveal a nexus to foreign or domestic terrorism. The information reported in a SAR may be the result of observations or investigations by police officers, or may be reported to them by private parties. Incidents which shall be reported on a SAR are as follows:

- Engages in suspected pre-operational surveillance (uses binoculars or cameras, takes measurements, draws diagrams, etc.).
- Appears to engage in counter-surveillance efforts (doubles back, changes appearance, evasive driving, etc.).
- Engages security personnel in questions focusing on sensitive subjects (security information, hours of operation, shift changes, what security cameras film, etc.).
- Takes measurements (counts footsteps, measures building entrances or perimeters, distances between security locations, distances between cameras, etc.).
- Takes pictures or video footage (with no

apparent esthetic value, i.e., camera angles, security equipment, security personnel, traffic lights, building entrances, etc.).

- Draws diagrams or takes notes (building plans, location of security cameras or security personnel, security shift changes, notes of weak security points, etc.).
- Abandons suspicious package or item (suitcase, backpack, bag, box, package, etc.).
- Abandons vehicle (in a secured or restricted location, i.e., the front of a government building, airport, sports venue, etc.).
- Attempts to enter secured or sensitive premises or area without authorization (i.e., "official personnel," closed off areas of airport, harbor, secured areas at significant events such as appearances by politicians, etc.).
- Engages in test of existing security measures (i.e., "dry run," security breach of perimeter fencing, security doors, etc., creating false alarms in order to observe reactions, etc.).
- Attempts to smuggle contraband through access control point (airport screening centers, security entrance points at courts of law, sports games, entertainment venues, etc.).
- Makes or attempts to make suspicious purchases, such as large amounts of otherwise legal materials (i.e., pool chemicals, fuel, fertilizer, potential explosive device components, etc.).
- Attempts to acquire sensitive or restricted items or information (plans, schedules, passwords, etc.).
- Attempts to acquire illegal or illicit explosives or precursor agents.
- Attempts to acquire illegal or illicit chemical agent (nerve agent, blood agent, blister agent, etc.).
- Attempts to acquire illegal or illicit biological agent (anthrax, ricin, Eboli, smallpox, etc.).
- Attempts to acquire illegal or illicit radiological material (uranium, plutonium, hospital x-ray discards, etc.).
- In possession, or utilizes, explosives (for illegal purposes).
- In possession, or utilizes, chemical agent (for illegal purposes, i.e., dry ice bomb, chlorine, phosgene, WMD attack, etc.).
- In possession, or utilizes, biological agent (for illegal purposes, i.e., terrorist device, WMD or a tool of terrorism, etc.).
- In possession, or utilizes, radiological material (for illegal purposes, i.e., as a weapon, etc.).
- Acquires or attempts to acquire uniforms without a legitimate cause (service personnel, government uniforms, etc.).
- Acquires or attempts to acquire official or official-appearing vehicle without a legitimate cause (i.e., emergency or government vehicle, etc.).
- Pursues specific training or education which indicate suspicious motives (flight training, weapons training, etc.).
- Stockpiles unexplained large amounts of currency.
- In possession of multiple passports, identifications or travel documents issued to the same person.
- Espouses extremist views (verbalizes support of terrorism, incites or recruits others to engage in terrorist activity, etc.).
- Brags about affiliation or membership with extremist organization ("white power," militias, KKK, etc.).
- Engages in suspected coded conversations or transmissions (e-mail, radio, telephone, etc., i.e., information found during a private business audit is reported to police).
- Displays overt support of known terrorist networks (posters of terrorist leaders, etc.).
- Utilizes, or is in possession of, hoax/facsimile explosive device.
- Utilizes, or is in possession of, hoax/facsimile dispersal device.
- In possession of, or solicits, sensitive event schedules (i.e., Staples Center, Convention Center).
- In possession of, or solicits, VIP Appearance or Travel Schedules.
- In possession of, or solicits, security schedules.
- In possession of, or solicits, blueprints to sensitive locations.
- In possession of, or solicits, evacuation plans.
- In possession of, or solicits, security plans.
- In possession of, or solicits, weapons or ammunition.
- In possession of, or solicits, other sensitive materials (passwords, access codes, secret government information, etc.).
- In possession of coded or ciphered literature or correspondence.

B. Involved Party (IP). An involved party (IP) is an individual that has been observed engaging in suspicious activity of this nature, when no definitive criminal activity can be identified, thus precluding their identification as a suspect.

II. REPORTING AND INVESTIGATING.

A. Employees—Responsibilities. Any Department employee receiving any information regarding suspicious activity of this nature shall:

- Investigate and take appropriate action, to include 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 or origin.

- If the activity observed is not directly related to a reportable crime, officers shall record the information collected from the person reporting, or their own observations, on an Investigative Report (IR), Form 03.01.00, titled "Suspicious Activity" in accordance with the following guidelines:

  - If the person reporting (R) is willing to be contacted by investigators, they shall be listed within the Involved Persons portion of the IR. Officers shall consider utilizing a "Request for Confidentiality of Information," Form 03.02.00, to ensure confidentiality. If absolutely necessary, officers can enter "Anonymous" for person reporting. Any desire by a person reporting to remain anonymous does not exempt officers from the requirement to complete an IR.
  - If the potential target of the activity can be identified, such as a government building or official being surveilled, that location or individual shall be listed within the "Victim" portion of the IR. Otherwise the "City of Los Angeles" shall be listed as the victim.
  - If the information includes an involved party (IP), officers shall identify or fully describe IPs within the narrative (page 2) of their report, along with any vehicle descriptions or other pertinent information.
  - If the information is related to a regular criminal investigation (such as a bomb threat, criminal threats, trespassing, etc.), the officers shall complete the criminal investigation, make any appropriate arrests, and complete any related reports. The officers shall include any additional information that provides the nexus to terrorism within the narrative of the crime or arrest report.

- Should officers come across information that indicates possible terrorism-related activity while investigating an unrelated crime or incident (e.g., such as officers conducting a domestic violence investigation observe possible surveillance photographs and a map of the region surrounding a government facility), or should they conduct an impound or found property investigation which is suspicious in nature, the officers shall make no mention of this potential terrorism-related material or activity within the impound, property, crime or arrest report. Under these circumstances, the officers shall complete a separate SAR in addition to the crime or arrest report, and shall note the criminal investigation, impound or found property investigation as their source of their activity.
- Officers shall note on the left margin of any arrest facesheet or IR that the report is to be sent to CTCIB, Major Crimes Division.

  Note: The Investigative Report is currently being revised to include "SAR" and "Original to CTCIB, Major Crimes Division" boxes to be checked when appropriate. The revised IR will also include additional entries for involved parties and involved vehicles.
- Notify Major Crimes Division (contact Real-Time Analysis and Critical Response [RACR] Division for off-hours notification) for guidance or if the report involves an arrest or a crime with follow-up potential.
- Notify the Watch Commander, Area of occurrence.
- Upon approval by the Watch Commander, ensure the Area Records Unit is made aware of the report, immediately assigns a DR number and forwards the original report to MCD.

  Note: Nothing in this Order alters existing policies regarding notifications to

required specialized units such as Bomb Squad, Hazardous Materials Unit, Criminal Conspiracy Section or RACR Division.

B. Hazardous Materials and Devices Section, Emergency Services Division—Responsibility. Personnel assigned to the Bomb Squad, Hazardous Materials/ Environmental Crimes, or Airport K-9 Bomb Detection Unit shall 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.

C. Watch Commanders—Responsibilities. Upon notification that officers have received information regarding suspicious activity, the Watch Commander shall:

- Ensure the information supports the completion of a SAR report and that no greater law enforcement response or notifications to MCD are currently needed;
- Review the report for completeness; and
- Ensure the Area Records Unit immediately assigns a DR Number and forwards the original report to MCD.

D. Major Crimes Division—Responsibility. Upon receiving a telephonic notification of suspicious activity, MCD personnel shall, when appropriate, conduct immediate debriefs of arrestees, or provide the appropriate guidance to patrol officers. Upon receiving a SAR report forwarded to MCD, assigned personnel shall follow established protocols regarding the processing of such information.

E. Records Personnel—Responsibilities. Upon receipt of a SAR-related incident, crime or arrest report, records personnel shall:

- Enter the information into the CCAD system, including any appropriate CTCIB-related codes; and
- Send the original report to "CTCIB/Major Crimes Division, Stop 1012" as soon as practicable, but no later than 24 hours after the report is taken. No copies of the report shall be maintained at the Area.

F. Area Detectives Personnel—Responsibilities. Upon receipt of a SAR-related crime or arrest report Area detectives shall:

- Ensure the report has been screened by MCD personnel and referred back to the geographic Area for investigation; and
- Complete the investigation per normal policies and guidelines. Note: If the report is a SAR-related incident only, or a crime or arrest report which arrives at an Area Detective Division without having been reviewed by MCD personnel, Area detectives shall immediately forward the report to MCD (no copies shall be retained at the Area).

G. Counter-Terrorism and Criminal Intelligence Bureau—Responsibility. Counter-Terrorism and Criminal Intelligence Bureau (CTCIB) 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.

AMENDMENTS:

This Order adds Section 4/271.46 to the Department Manual.

AUDIT RESPONSIBILITY:

The Commanding Officer, Counter-Terrorism and Criminal Intelligence Bureau, shall monitor compliance with this directive in accordance with Department Manual Section 0/080.30 and shall ensure that all information is collected and maintained in strict compliance with existing federal, State and Department guidelines regarding Criminal Intelligence Systems (28 CFR Part 23 and applicable California State Guidelines).

WILLIAM J. BRATTON

Chief of Police

DISTRIBUTION "D"

Appendix C:
Sample of Los Angeles Police Department Terrorism-Related CCAD Codes

TYPE	CODE	CRIME CLASS (CC) DESCRIPTION	CCAD LONG DESCRIPTION
CC	995	Suspicious Activity Reports (SAR)	Suspicious Activity Reports
MO		**SUSPECT ACTIONS:**	
S	2100	Preoperational surveillance	Engages in suspected preoperational surveillance (uses binoculars or cameras, takes measurements, draws diagrams, etc.)
S	2101	Countersurveillance efforts	Appears to engage in countersurveillance efforts (doubles back, changes appearance, evasive driving, etc.)
S	2102	Questions about security procedures	Engages security personnel in questions focusing on sensitive subjects (security information, hours of operation, shift changes, "what do cameras film?," "do cameras record?," etc.)
S	2103	Appears to take measurements	Takes measurements (counts footsteps, measures building entrances or perimeters, distances between security locations, distances between cameras, etc.)
S	2105	Draws diagrams or takes notes	Draws diagrams or takes notes (building plans, location of security cameras or security personnel, security shift changes, notes of weak security points, etc.)
S	2106	Abandons suspicious package/item	Abandons suspicious package or item (suitcase, backpack, bag, box, package, etc.)
S	2107	Abandons vehicle in restricted area	Abandons vehicle (in a secured or restricted location, i.e., the front of a government building, airport, sports venue, etc.)
S	2108	Enters restricted area w/o authorization	Attempts to enter secured or sensitive premises or area without authorization (i.e., "official personnel," closed-off areas of airport, harbor, secured areas at significant events such as presidential speeches, inaugurations, etc.)
S	2109	Tests existing security measures	Engages in test of existing security measures (i.e., "dry run," security breach of outside fencing/security doors, etc., false alarms to observe reactions, etc.)