Institute for Homeland Security Solutions
Applied research • Focused results

Building on Clues: Methods to Help State and Local Law Enforcement Detect and Characterize Terrorist Activity

Final Report

April 2011

Authors

Kevin Strom, RTI International

John Hollywood, RAND Corporation

Mark Pope, RTI International

Garth Weintraub, RTI International

Crystal Daye, RTI International

Don Gemeinhardt, RTI International

Table of Contents

List of Figures

List of Tables

Executive Summary

For the past decade, members of the law enforcement and intelligence communities have been working to develop methods and processes to identify and thwart terrorist plots. As part of these efforts, state and local law enforcement agencies have been increasingly recognized as the “first-line preventers” of terrorism (Kelling & Bratton, 2006). The network of over 17,000 law enforcement agencies, including regional and state fusion centers, represents a resource that exponentially increases the United States’ ability to identify, report, and analyze information that is potentially terrorist-related. However, these agencies also face ongoing challenges in this counterterrorism role.

Perhaps the most pressing issue has been the lack of coordination and standardization of counterterrorism practices at the state and local levels. For example, in the absence of federal guidance, local jurisdictions have often developed different procedures for collecting and prioritizing suspicious activity reports (SARs)—reports of activities and behaviors potentially related to terrorism collected from incident reports, field interviews, 911 calls, and tips from the public. The lack of standardization has impeded the sharing and analysis of such information (Suspicious Activity Report Support and Implementation Project, 2008). Federal agencies such as the U.S. Department of Justice (DOJ), Federal Bureau of Investigation (FBI), Department of Homeland Security (DHS), and Department of Defense (DOD), among others, have made it part of their mission to standardize this process. One of the first steps was the introduction of the Nationwide SAR Initiative (NSI), which created “a unified process for reporting, tracking, and accessing of SARs” (National Strategy for Information Sharing [NSIS], 2007, p. A1-7).

This project, funded by the Institute for Homeland Security Solutions (IHSS), considered the collection and use of SARs at the state and local level. We assess how tips and clues generated from state and local sources have been used to prevent terrorist plots, assess the strengths and weaknesses of data sources from which SARs are often derived, and make recommendations for improving the collection, processing, and evaluation of tips and clues reported at the local level. The project was conducted in three phases.

Phase I included an analysis of publicly-reported terrorist plots against U.S. targets from 1999 to 2009, including both foiled and executed plots, to determine what types of suspicious behaviors and means of reporting most frequently led to (or could have led to) their discovery and ultimate prevention (Strom et al., 2010). The report published from Phase I examined open-source material on 86 foiled and executed terrorist plots against U.S. targets.

In Phase II, we conducted interviews with members of the law enforcement, fusion center, and intelligence communities to gain an improved understanding for how these agencies collect, process, and analyze SARs. In addition, we sought to gain more perspective on how these agencies could better use the information gathered and what challenges they face with respect to SARs.

Phase III of the study assessed the primary data sources for SARs, the processes used to collect and analyze SARs, and approaches used to prioritize SARs. We also developed a set of recommendations that can be used by law enforcement and fusion center personnel to improve their practices of collecting, managing and prioritizing SARs.

The work conducted across these phases resulted in a set of recommendations and conclusions, which we believe can improve the SAR process. These include the need to:

- Recognize the importance of law enforcement (including the critical role of state and local agencies) and the general public in preventing attacks, and support them through investments in education and reporting. More than 80% of foiled terrorist plots were discovered via initial clues provided from law enforcement or the general public.
- Continue to investigate Al Qaeda and Allied Movements (AQAM), but do not overlook other types of domestic terrorist groups, and pay particular attention to “lone wolves.” Less than half of U.S. terror plots examined had links to AQAM, and many non-AQAM plots, primarily those with white supremacist or anti-government/militia ties, rivaled AQAM plots in important ways. Additionally, plots by single actors (“lone wolves”) have proven particularly successful, reaching execution nearly twice as often as plots by groups.
- Ensure that effective processes and training are in place that can enable law enforcement to identify and report terrorist activity during routine criminal investigations. Nearly one in five plots were foiled when police recognized terrorist activity during investigations into seemingly ordinary crimes.
- Work to establish good relations with local communities and avoid tactics that might alienate them. About 40% of plots were thwarted as a result of tips from the public and informants. Establishing trust with persons in or near radical movements is jeopardized by tactics such as racial, ethnic, religious, or ideological profiling.
- Expand the ISE-SAR Functional Standard to include activities that were the initial clue used to discover terrorist plots such as direct tips originating from the public or an informant or clues detected during routine criminal investigations.
- Develop automated search capabilities for databases likely to contain SARs. The NSI processes depend on officers recognizing that a call record or crime report constitutes a SAR and reporting it up the appropriate channels. This may be sufficient in a vast majority of cases. However, implementing cost-effective methods for searching databases with large amounts of activity, such as in 911 call centers, may result in the identification of valid SARs that were not previously identified.
- Develop a comprehensive process which explicitly introduces scheduling of follow-up activities, checks on progress and results, and corrective actions into SAR analysis processes and information flows. Control mechanisms should include an evaluation element, a scheduling element, and a quality control element.
- Create an “instructional guide” that provides guidance to state and local agencies for evaluating SARs. We have identified general criteria for evaluating SARs, “TASCS” (Threatening, Atypical, Significant, Credible, and Specific), as well as preliminary templates for evaluating specific types of SARs based on prior cases.

1. Introduction

In recent years, it has been widely recognized that state and local law enforcement play a vital role in homeland security, including preventing terrorist attacks (Kelling & Bratton, 2006). While the need for greater inclusion of state and local law enforcement in counter-terrorism was generally accepted, there were a number of challenges to implementing this vision, including training officers on how to identify behaviors indicative of terrorism, developing mechanisms to report and share suspicious activity reports (SARs) across jurisdictions, and developing more detailed strategies for analyzing SARs.

The Nationwide SAR Initiative (NSI) was launched in part to address challenges by establishing “a unified process for reporting, tracking, and accessing of (SARs)” (National Strategy for Information Sharing [NSIS], 2007, p. A1-7). Regional and state fusion centers have also helped promote partnerships and information sharing. However, there remains a need to develop improved processes for generating useful tips and leads as well as for developing effective methods for reviewing and analyzing the large volume of information that is reported across a wide variety of local data sources.

This project, funded by the Institute for Homeland Security Solutions (IHSS), focused on the collection and use of SARs at the state and local level, including how such information has been used to prevent terrorist plots, the local sources from which SARs are often derived, and recommendations for improving the collection, processing, and evaluation of tips and clues reported at the local level. The project had three key phases, which collectively resulted in a series of findings and recommendations for policy makers and practitioners.

Phase I included an analysis of all identified terrorist plots against U.S. targets from 1999 to 2009, including both foiled and executed plots, to determine what types of suspicious behaviors and means of reporting most frequently led to (or could have led to) their discovery and prevention. This analysis sought to provide state and local law enforcement partners with an improved understanding of the types and sources of clues that should be emphasized to more effectively detect and disrupt terrorist activity before it occurs.

Phase II featured interviews with members of the law enforcement, fusion center, and intelligence communities to gain a better understanding of how these agencies collect, process, and analyze SARs. We also sought to gain a better perspective on how agencies could better use the information gathered and challenges faced with respect to SARs.

Phase III involved assessing the primary SAR data sources to better understand their strengths and limitations. We also developed a set of comprehensive recommendations that can be used by law enforcement (i.e., first-line supervisors; middle and upper management staff) and fusion center personnel to improve their practice of collecting, processing, and evaluating SARs, including adjustments to existing or proposed processes that would increase the utility of the data and the subsequent intelligence that is developed.

2. Phase I – Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999–2009

Overview

In the Phase I analysis, we examined all identified terrorist plots against U.S. targets from 1999 to 2009, including both foiled and executed plots, to determine what types of suspicious behaviors and means of reporting most frequently led to (or could have led to) their discovery and ultimate prevention. This analysis sought to (1) identify and assess the meaningful characteristics of terrorist plots; (2) characterize the initial clues of terrorist activity; (3) characterize the evidence that led to full-scale counterterrorism investigations; (4) characterize how these full-scale investigations progressed; and (5) analyze plots that ended in an attack to determine if there were clear indicators that could have been detected.

While there has been no shortage of counterterrorism research, the Phase I analysis is unique in two key respects. First, unlike small-*n* qualitative case studies, which typically suffer from an inability to generalize findings (Goldthorpe, 1997; Lieberson, 1991), or large-*n* statistical analyses that are often too general and thus not useful to investigators at a practical level (Brady & Collier, 2004; Mahoney & Rueschemeyer, 2003), this study seeks the middle ground. Specifically, the analysis uses quantitative techniques to characterize qualitative case studies of terrorism incidents in order to provide practical recommendations to law enforcement. Second, unlike most counterterrorism research, which has focused on the types of activities terrorists engage in prior to carrying out an attack (e.g., Smith, Damphousse, & Roberts, 2006; Memorial Institute for the Prevention of Terrorism, 2007), this analysis focuses on the activities of law enforcement and the public at large that have proven most effective at thwarting plots.

Methods

Defining Cases to Include

In this study, we included recent cases of U.S. terrorism satisfying the following criteria:

- *The case fits the definition of "terrorism" used to define cases in the Global Terrorism Database (GTD).* Specifically, the case reflects an "intentional act of violence or threat of violence by a non-state actor" meeting two of the three following requirements: (1) the act was aimed at attaining a political, economic, religious, or social goal; (2) the act included evidence of an intention to coerce, intimidate, or convey some other message to a larger audience (or audiences) other than the immediate victims; or (3) The action must be outside the context of legitimate warfare activities (START,2010).
- *The case can include a plot that reached execution, a plot foiled prior to reaching execution, or material support to a terrorist organization clearly in service of a future*

*plot. “Exec*uted” plots include those that were actually carried out, even if they did not result in casualties or were stopped during the moment of execution (e.g., the Christmas day bombing plot was counted as an executed plot despite the bomb failing to detonate). “Foiled” plots include only thwarted plots that were deemed as legitimate threats; hoaxes and cases in which alleged perpetrators were subsequently acquitted were excluded. Cases of “material support in service of a future plot” typically involved suspects conducting site surveillance of U.S. landmarks to assist terrorist groups in determining which landmarks to attack; cases of recruiting U.S. persons to train with or fight for the Taliban or other radical groups overseas were not included.

- *The planned or executed acts of violence in the case were intended to cause casualties or catastrophic damage to critical infrastructure.* During our initial search for incidents, we uncovered a significant number of small-scale attacks against property, almost all of which were conducted by animal rights and environmental groups (e.g., vandalism of auto dealerships, arsons of new housing developments, and destruction of lab equipment). Although the cumulative financial impact of these attacks is undoubtedly large, including them in our study posed significant challenges. First, such attacks have generally received little national coverage, and thus information about them was severely limited. Second, small-scale attacks directed only at property are typically given lower investigative priority. In fact, none of the more than 135 identified animal rights and environmental group attacks against property were foiled prior to execution. Therefore, including such cases would likely produce an imbalanced analysis. As a result, small-scale attacks intended strictly to damage property, unless the targets were deemed to be critical infrastructure (e.g., dams, power plants, bridges), were discarded.
- *The plot was directed against a U.S. target outside of a conflict zone.* This criterion includes targets within U.S. boundaries, as well as U.S. embassies, consulates, and military bases abroad. However, U.S. targets in countries with high insurgent or terrorist paramilitary activity, such as Iraq, Afghanistan, and Pakistan, were excluded.
- *The case took place between January 1, 1999, and December 31, 2009*. In selecting our study period we sought to evaluate a minimum of 10 years of data. Selecting 1999 as a start date also ensured that some of the first wave of AQAM plots (notably the Millennium Plot) as well as several major militia and Y2K plots were included.
- *The case can include plots of any ideological motivation*. While AQAM and AQAM-inspired violence has received a great deal of attention since 9/11, we examined cases across the full range of ideological motivations, including broadly leftist ideologies, animal rights causes, the environment (besides animal rights), opposition to abortion, opposition to government authority (militia groups), and white supremacist (including Neo-Nazi) beliefs. In a few cases, the exact motivations of the plotters were either unknown or not clearly ideological in nature.
- *Information about the case was publicly available*. Only cases discussed in open sources are included. Sources used include media accounts, legal records, government publications, research databases, and listings by terrorism “watchdog” groups.

We believe that the cases included in this analysis are representative of recent activity that is generally considered terrorism against U.S. targets. We recognize that restricting the cases to those publicly known is a limiting factor that may skew the specific numbers in this study (notably, plots foiled through intelligence efforts that never became public and plots that ended on their own are likely underreported). However, we believe that the general trends in our findings are valid and informative.

Identifying Cases

Cases were identified from a variety of publicly available information sources. Research databases included the GTD from 1999 to 2007, augmented with the Worldwide Incidents and Tracking System (WITS) for 2008 to 2009. Government sources included publications and reports from the FBI, DOJ, DHS, and the White House. We also reviewed media accounts and summaries, which proved particularly helpful for information regarding more recent incidents.

In addition, terrorist incidents were identified from incident summary lists maintained by several advocacy groups, including the Heritage Foundation (tracking predominantly AQAM and AQAM-inspired groups), the Southern Poverty Law Center (tracking anti-government groups and those motivated by racial, ethnic, religious, or other types of bias), and the Fur Commission (tracking environmental and animal rights groups). Although information from these advocacy groups was useful in identifying cases of interest, we drew from other sources to code the fields of interest wherever possible.

Coding Process and Analytic Methods

Identified cases were added to a customized Microsoft Access database, which served as the central repository for all information collected or extracted. All cases were reviewed independently by multiple project staff to verify that they were consistently coded and that they satisfied the inclusion criteria. Cases were coded for a number of attributes, including group ideology/motivation, group size, means of attack, nature of attack, target type, the initial clue that led to (or could have led to) the plot’s discovery, source of the initial clue, and the secondary clue that led to a full-scale investigation. These codes were developed after all cases were identified and refined to ensure they accurately characterized the types of clues and activities identified. The variables and the codes used can be found in **Appendix A**.

Using this coding scheme, we identified cases with similar attributes to establish trends and patterns within the dataset. We emphasize that given the incompleteness of the data these counts should not be confused with statistical analyses. Similarly, many of the counts are small (e.g., a plot was foiled a certain way only once or twice) and could not be used to draw meaningful statistical inferences, even if perfect data were available. Additionally, cases known only to intelligence agencies are likely underreported, as mentioned. Furthermore, it is unlikely that we found every relevant case through our searches. While these limitations should be noted, we believe that the trends and patterns in the cases are informative.

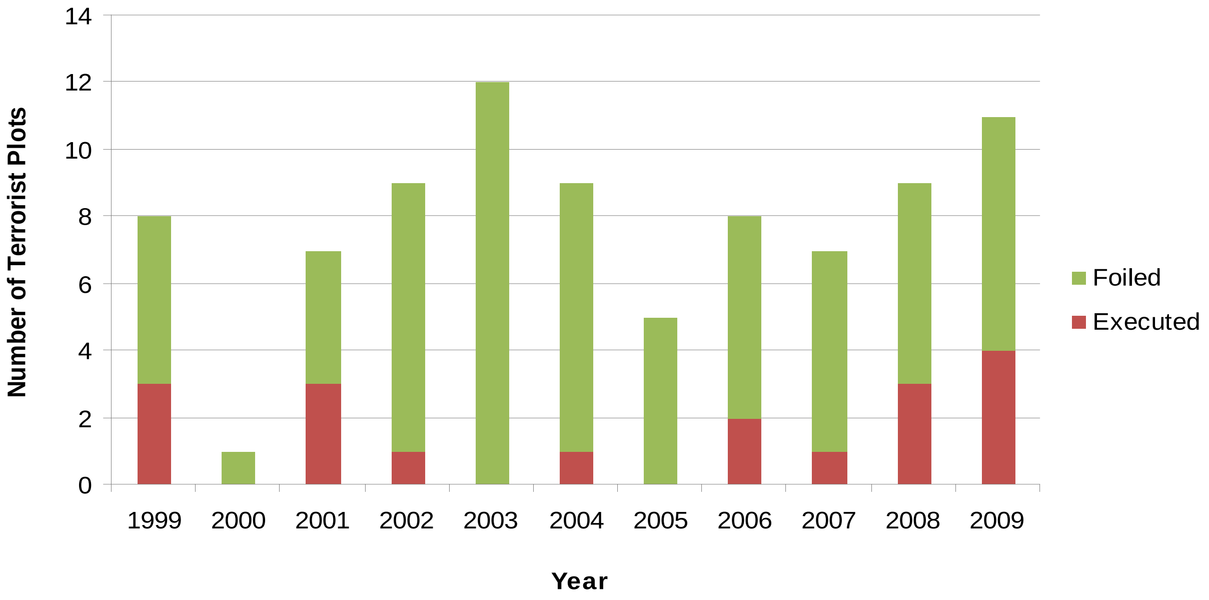
Results

Characterizing Terrorist Plots in the United States, 1999–2009

We identified 86 cases that met the specified criteria. Of these 86 cases, 18 plots reached execution and caused—or were intended to cause—casualties. The remaining 68 cases were plots that were intended to cause casualties but were thwarted prior to execution. Assuming these identified cases are generally representative, the United States is interdicting about 80% of terrorist plots intended to cause casualties or destroy critical infrastructure.

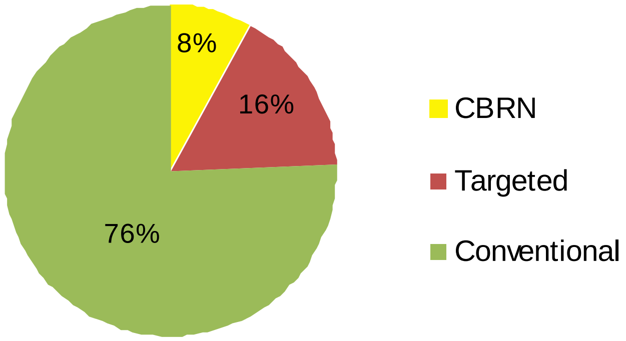
From 1999 to 2009, our data indicate an average of approximately 8 plots (1.6 executed plots and 6.2 foiled plots) per year. However, the number of plots varied significantly from year to year, ranging from a low of 1 in 2000 to a high of 12 in 2003, as illustrated in **Figure 1**.

Figure 1. Foiled and Executed Terrorist Plots by Year, 1999–2009



The nature of these plots also varied widely (see **Figure 2**). In the majority of plots (65 cases, 76%), the plan was to carry out a conventional attack, including bombings and mass shootings, to inflict casualties. By contrast, chemical, biological, radiological, or nuclear (CBRN) attacks were planned in only seven cases (8%). In 14 cases (16%), a particular person or small group was targeted (typically assassinations).

Figure 2. Nature of Terrorist Plots, 1999–2009

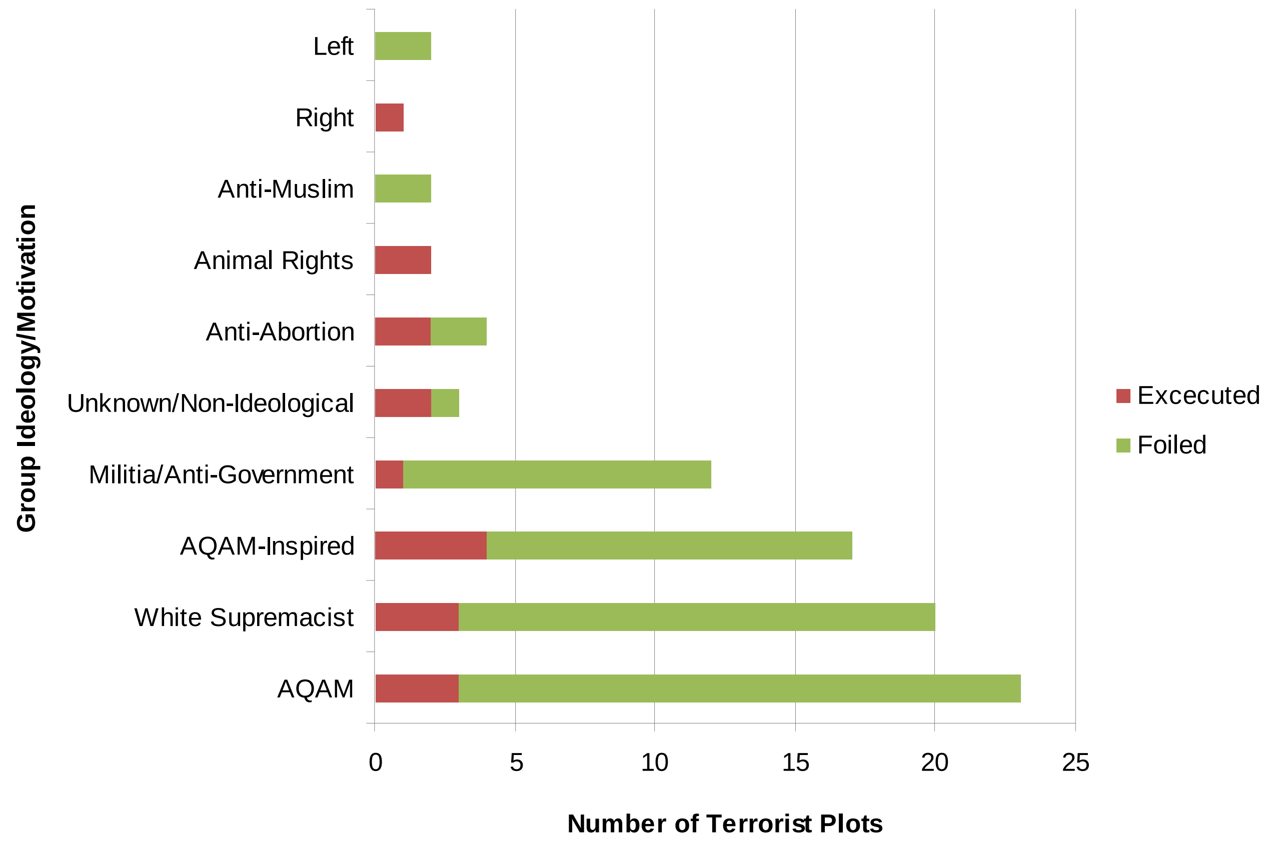


The frequency of plots also varied by group ideology/motivation. From the 86 cases examined, we were able to identify 10 distinct ideological or motivational categories. **Figure 3** provides a breakdown of these group types and the number of plots associated with them. In the figure, we distinguish between "AQAM" plots (those sponsored directly by a foreign AQAM organization) and "AQAM-Inspired" plots (those planned or carried out by individuals who did not receive direct support or training from AQAM but were nevertheless influenced by them). AQAM-inspired plots are frequently characterized by the media as "homegrown" terrorist plots, and recent research has highlighted their growing importance in the U.S. (Bergen & Hoffman, 2010).

Since 9/11, U.S. discourse on terrorism has tended to focus on AQAM and associated "Jihadists" (e.g., Sageman, 2008; Hoffman, 2003; Ackerman & Tamsett, 2009). However, our analysis indicates that non-AQAM attacks are also important. Although AQAM and AQAM-inspired plots were responsible for a plurality of attacks in our study (40 out of 86), white supremacist and militia/anti-government groups were also responsible for a significant number of attacks (20 and 12 plots, respectively).

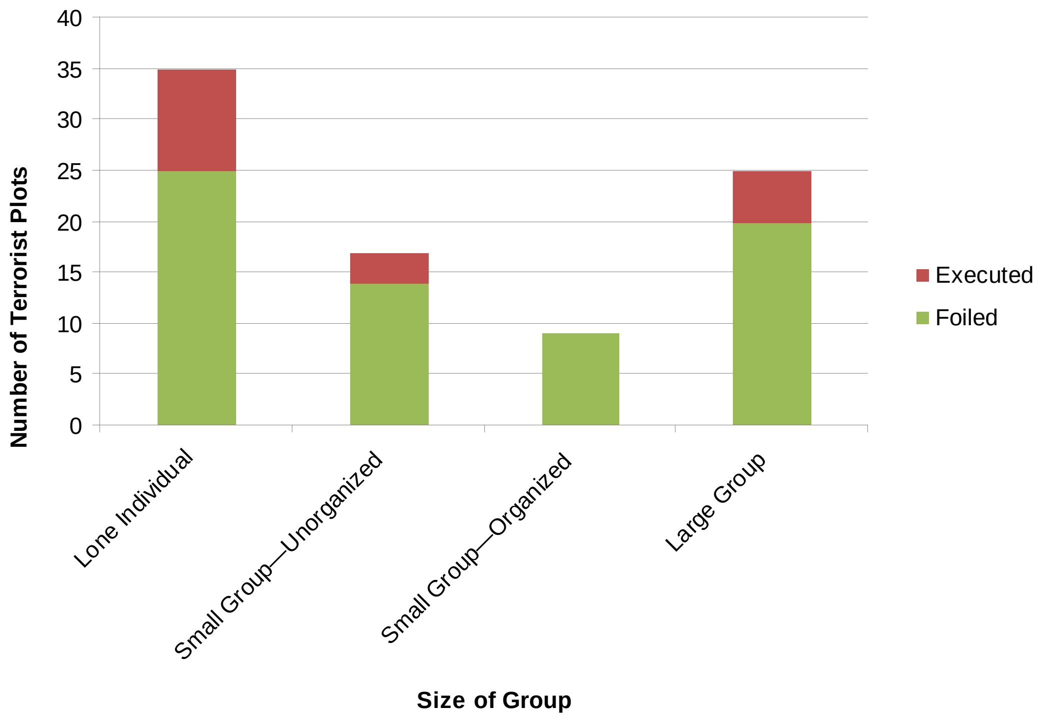
Furthermore, white supremacist and militia/anti-government plots rivaled AQAM plots in other ways. For example, the majority of CBRN plots were hatched by non-AQAM groups—three plots were by white supremacist groups, and two attacks were for unknown or non-ideological reasons (with the latter including the October 2001 anthrax attacks). Some types of non-AQAM attacks with relatively few plots are worth mentioning as well, as they were disproportionately likely to reach execution. These include plots by animal rights groups, anti-abortion activists, right wing groups, and attacks carried out for unknown or non-ideological reasons. Although the small number of such plots makes statistical inferences problematic, anecdotally, our data suggest that authorities have been less successful at thwarting these types of plots.

Figure 3. Terrorist Plots by Group Ideology/Motivation, 1999–2009



Analysis of terrorist plots by group size reveals that the vast majority of attacks were by single actors and small groups, as illustrated in **Figure 4** below.

Figure 4. Executed and Foiled Plots by Group Size, 1999–2009



More than 40% (35 cases) of terrorist plots from 1999 to 2009 were planned or carried out by single individuals, or “lone wolves” (individuals not directly under the command structure of a group or movement but who sympathize with a particular cause). “Lone wolves” have also been more successful in executing attacks; nearly 30% of plots by single actors reached execution, compared to a 16% average execution rate by small and large groups.

Plots by large groups (including 23 AQAM plots and 2 attacks by the Animal Liberation Front [ALF]) were responsible for approximately 29% of identified plots. Although large groups were less successful than lone wolves, they were more successful than small groups, executing 20% of their intended attacks. We note, however, that while we classify both AQAM and ALF as large groups, operationally, the majority of their attacks have been perpetrated by small groups of individuals, often acting with a large degree of autonomy.

Of the remaining plots, approximately 20% (17 cases) involved small, informal groups (such as the father and son duo Wade and Christopher Lay, who plotted to assassinate Texas officials involved in the 1993 Waco standoff), and 11% (9 cases) involved small organized groups (groups with names and formal organizational structures, such as the Jamiyyat Ul-Islam Is-Saheeh [JIS] group, which formed in a California prison and allegedly conspired to attack Army National Guard facilities, synagogues, and other targets throughout southern California). Overall, attacks by small groups were found to be the least successful, reaching execution in just 3 of the 28 incidents plotted (11%).

Initial Clues of Terrorist Activity

In this section, we limit our analysis to the foiled plots (68 cases) in order to understand what characteristics these plots had in common that allowed them to be thwarted. We first consider initial clues—reports that tipped off law enforcement or members of the intelligence community that there was a reasonable suspicion of future terrorist activity.

To conduct this analysis, we developed a coding scheme to categorize the clues that first brought these plots to the attention of authorities. The categories of initial clue types and examples of each are described in greater detail below in **Table 1**. In the table, we list the federal standards for categorizing suspicious activity reports potentially related to terrorism as defined in the newly created *Information Sharing Environment* (*ISE) SAR Functional Standard*, Version 1.5 (Program Manager for the Information Sharing Environment, 2009). Note that the *ISE SAR Functional Standard* focuses on suspicious activity as traditionally defined (e.g., people photographing locations that are not normally photographed). Thus, many of the initial clues identified from the plots in our dataset had no matching ISE SAR code, or a code that was only tangentially related—for example, coding a tip that a specific conspiracy was underway as "Expressed or Implied Threat." We therefore use our own coding schema in the analysis rather than the ISE SAR codes to provide a more detailed and complete list of clue types.

Table 1. Types of Initial Clues or Activities That Brought Attention to a Plot

Initial Clue	Description	ISE SAR Equivalent Code
Associations with known suspects	Authorities note meaningful associations between a known terror suspect(s) and a new suspect. (e.g., Authorities observe terrorism suspects meeting secretly with previously unknown persons.)	No equivalent
Prior terrorist activity	Authorities investigate nonviolent acts of terrorism (typically against property) and find plans and material to carry out violent attacks. (e.g., Authorities investigate suspects for nighttime arsons at churches and discover plans and material to bomb a church during services.)	Sabotage/Tampering/ Vandalism
Solicitation of an undercover agent or informant	A would-be terrorist solicits an undercover agent or informant to participate in a plot. (e.g., A member of a group asks a perceived fellow extremist to help him or her acquire explosives to blow up a government building.)	Expressed or Implied Threat; may also include Acquisition of Expertise
Online solicitation	A would-be terrorist attempts to recruit others to join a plot, or expresses interest in joining a plot, in online media (chat rooms, discussion boards, etc.). (e.g., A person asks to join an AQAM group and receive training to blow up a government building.)	Expressed or Implied Threat; may also include Acquisition of Expertise
Unsolicited public tip reporting a specific plot	A member of the general public (including associates of the perpetrator not already acting as police informants) contacts authorities to report a plot (e.g., A former member of an extremist organization learns that other members are plotting an attack and voluntarily reports this to the police.)	Expressed or Implied Threat
Direct threat from perpetrator	A would-be terrorist makes an explicit threat directly to the intended target, who then reports it to authorities. (e.g. An individual sends a letter to the IRS threatening to kill any employee who attempts to collect his/her taxes, and the threat is reported.)	Expressed or Implied Threat
"Ordinary" crime	Authorities investigate criminal activity with no known links to terrorism and discover evidence of a plot. (e.g., Authorities respond to a report of domestic violence and find attack plans at the home.)	No equivalent
Precursor crime	Authorities investigate crimes known to be associated with terrorism (e.g., counterfeiting, identity theft, robbery) and discover evidence of a plot. (e.g., Authorities arrest would-be plotters for multiple gas station robberies and during adjacent searches discover plans to carry out a terrorist attack.)	Can be Theft/Loss/ Diversion, depending on the type of crime

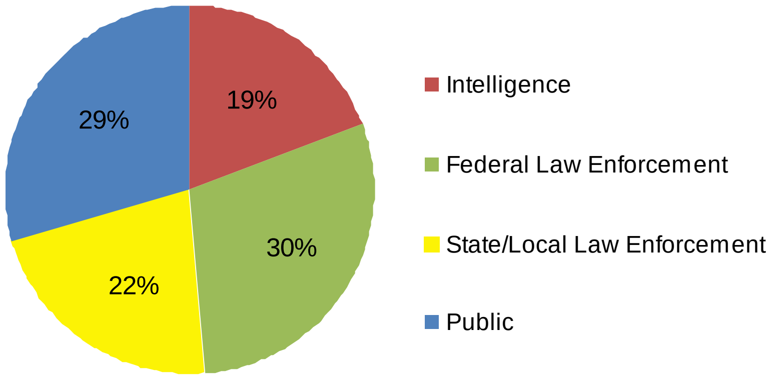
(continued on next page)

Table 1. Types of Initial Clues or Activities That Brought Attention to a Plot (continued)

Initial Clue	Description	ISE SAR Equivalent Code
Criminally suspicious activity	Authorities receive reports of criminal activity or behavior indicating the possibility of a terrorist attack. (e.g., Passersby see a man parked outside a synagogue with a rifle and call police.)	Expressed or Implied Threat
Suspicious activity—paramilitary training/travel	Authorities receive reports of individuals either setting up paramilitary training events or trying to travel overseas to receive paramilitary training. (e.g., (1) Authorities investigate reports of people regularly firing assault rifles in a mining pit. (2) A person reports that a family member is trying to book travel to receive paramilitary training in Pakistan.)	Acquisition of Expertise
Suspicious activity—potential surveillance activity	Authorities receive reports of behavior potentially related to target probing and surveillance. (e.g., Authorities detain and question people trespassing in and photographing military barracks.)	Breach/Attempted Intrusion, Eliciting Information, Testing or Probing of Security, Photography, and/or Observation/Surveillance depending on the incident
Suspicious activity—extremist rants	Authorities receive reports of an individual carrying out "violent" or "threatening" rants justifying terrorist attacks and implying the individual would like to participate. (e.g., Authorities investigate a person who routinely calls for "Jihad" against the U.S. government and who invites "trusted" individuals into secret meetings with him.)	Expressed or Implied Threat
Suspicious activity—smuggling-like behavior	Authorities investigate suspicious activity associated with smuggling contraband, typically onto an airplane or at a point of entry. (e.g., Authorities investigate a man at a border crossing who seems extremely nervous, repeatedly glances at the vehicle's trunk, and is unable to answer simple questions about his travel plans.)	Sector-Specific Incident for security checkpoints
Suspicious activity—suspicious documents found	Authorities discover documents that appear relevant to a terrorist plot. (e.g., site surveillance plans, false identification documents, or e-mail discussing a person's participation in a plot)	"Evidence" of Explicit or Implied Threats, Misrepresentation, or Observation/Surveillance depending on the content

The initial clues of the 68 thwarted plots are presented below by the source (**Figure 5**) and type (**Figure 6**) of clue. “Source” refers to the person or organization that initially observed and reported the clue—state or local law enforcement, federal law enforcement,[1] the intelligence community, or a member of the general public who voluntarily provides information to authorities (i.e., not already working as an informant). “Type” refers to the means by which the clue initially came to the attention of law enforcement, broadly categorized as investigations of crimes, reports of suspicious activity, reports of specific terrorist plots, or the discovery of associations with known or suspected terrorists.

Figure 5. Source of Initial Clues in Foiled Plots, 1999–2009



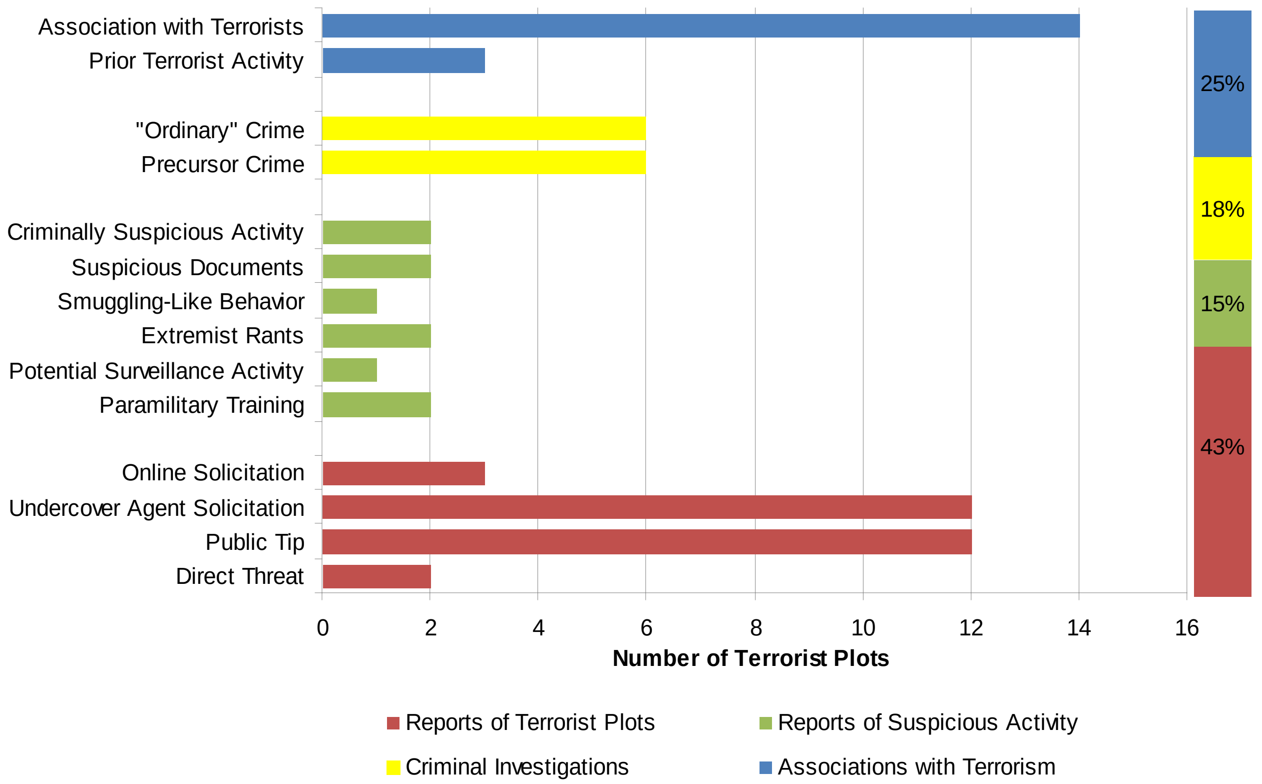
Our analysis indicates that law enforcement, assisted by the public, is generally the first line of defense in detecting terrorist plots. In over 80% of the foiled plots in our dataset, the initial clue came from law enforcement (20 federal cases and 15 state/local cases) or from public reporting (20 cases). By contrast, intelligence reporting was found to be the source of initial clues in just 13 cases (19%). As noted earlier, we acknowledge that the actual number of cases foiled by intelligence is likely higher. Nevertheless, the importance of the general public and state and local law enforcement in foiling terror plots is clear.

In **Figure 6**, we summarize the types of initial clues that ultimately foiled terrorist plots. In most cases (29 plots, 43%), the initial clue was a report of a specific plot. The vast majority of these reports (24 of 29 plots) were split between tips from the general public (12 cases) and

[1] We recognize that certain agencies (notably the FBI) perform both intelligence and law enforcement functions. Therefore, when categorizing the source of initial clues, we consider both the agency involved and the type of activities the agency was engaged in which produced the clue. For example, if the FBI discovers a plot during the course of its intelligence collection activities, such as phone or other communication intercepts authorized by the Foreign Intelligence Surveillance Act (FISA), the source is classified as “Intelligence.” Similarly, if the FBI discovers a plot during the course of a criminal investigation, the source is classified as “Federal Law Enforcement.”

would-be terrorists soliciting an undercover agent or informant (12 cases). In two cases, the plot was foiled after the perpetrator made a direct threat to their target. Only three plots were reportedly discovered through Internet monitoring activities that found suspects conspiring online to participate in terrorist activities, although we note that the open-source nature of our information may underestimate these types of activities.

Figure 6. Type of Initial Clues in Foiled Plots, 1999–2009



In 10 cases (15%), the initial clue came from a report of suspicious activity. The types of suspicious activities included criminally suspicious actions (2 cases), suspicious documents (2 cases), smuggling-like behavior (1 case), extremist rants (2 cases), and paramilitary training (2 cases). Only one case was identified in which the initial clue came from a report of possible surveillance activities, a somewhat surprising finding given the large amount of attention this type of pre-operational behavior has received.

Non-terrorism-related criminal investigations also led to a significant number of plots being foiled (12 cases, 18%). In half of these (6 cases), investigations into precursor crimes (e.g., robbery, theft, counterfeiting) revealed the larger plot, and in the other half law enforcement came upon the plots "by surprise" while investigating unrelated "ordinary" crimes (e.g., parole violations, traffic stops). The link between the investigation of criminal or "suspicious" activity and terrorism was thus significant, thwarting nearly one in three identified terrorist plots overall.

Clues Triggering Full Investigations

The second step in foiling a terrorist plot is amassing enough evidence to warrant a full-scale investigation. Often, this evidence is found as a result of authorities responding to the initial clue. Sometimes, however, the initial clue itself is sufficient to launch a full-scale investigation. In other instances, a full investigation is launched when a connection to another ongoing investigation is discovered. **Table 2** describes the types of evidence that led to full-scale investigations in the 68 foiled plots we examined and maps them to the ISE SAR code equivalents.

Table 2. Descriptions of Clues Triggering Full Investigations

"Triggering" Clue	Description	ISE SAR Code
Initial Clues Sufficient to Launch a Full Investigation		
Details of plot from intelligence	Information provided from intelligence efforts is sufficient to launch a full investigation.	No equivalent
Details of plot from public tip	Information provided in a tip about a terrorist plot is sufficient to launch a full investigation.	Expressed or Implied Threats
Details of plot from solicitation	Information provided by group members soliciting an undercover informant or agent is sufficient to launch a full investigation.	Expressed or Implied Threats
Explicit threats from suspect	Suspect made written or oral threats sufficiently concerning to launch a full investigation.	Expressed or Implied Threats
Threatening behavior by suspect	Suspect's observed behavior is sufficiently concerning to launch a full investigation.	Expressed or Implied Threats
Evidence Collected from Investigating Initial Clues Used to Launch Full Investigation		
Search following SAR that is potentially terrorism-related	Adjacent search following a report of activity potentially related to terrorism finds evidence triggering a full investigation. Evidence could include attack plans, target surveillance reports or video, weapons stockpiles, explosives material, or detonator components.	Material Acquisition and Storage or Weapons Acquisition; may be other types, depending on materiel found
Search following criminal activity	Adjacent search investigating a previous crime or criminally suspicious activity finds evidence triggering a full investigation.	Material Acquisition and Storage or Weapons Acquisition; may be other types, depending on materiel found
Surveillance following SAR that is potentially terrorism-related	Surveillance following a report of suspicious activity finds evidence triggering a full investigation. This could include documentation (video, audio) of suspects meeting with informants or undercover agents to plot an attack or seek training/materiel to carry one out.	Typically Expressed or Implied Threats

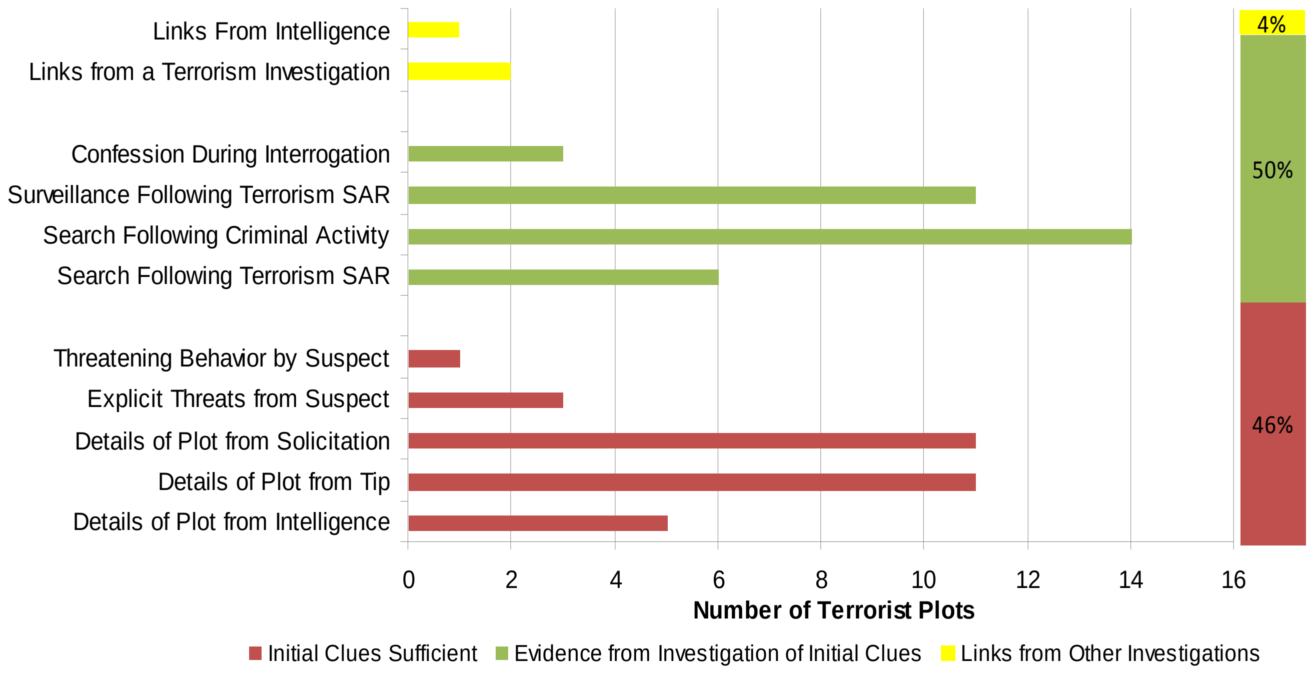
(continued on next page)

Table 2. Descriptions of Clues Triggering Full Investigations (continued)

"Triggering" Clue	Description	ISE SAR Code
Confession during interrogation for a SAR that is potentially terrorism-related	Suspect confesses to a plot while being interrogated for activity potentially related to terrorism.	No equivalent
Confession during interrogation for criminal activity	Suspect confesses to a plot while being interrogated for a crime or criminally suspicious activity.	No equivalent
Links from Other Investigations ("Connecting the Dots")		
Links from a terrorism investigation	Suspects named in an initial clue are part of another terror-related investigation.	No equivalent
Links from intelligence	Suspects named in an initial clue previously appeared in intelligence reports or databases.	No equivalent

Figure 7 below provides a breakdown of the type of evidence that triggered full-scale investigations in the 68 foiled terrorist plots we identified.

Figure 7. Evidence Triggering Full-Scale Investigations in Foiled Plots, 1999–2009



In many of the plots examined (46%, 31 cases), the initial clue alone was sufficient to launch a full investigation. However, the majority of plots (50%, 34 cases) required additional investigation or linking, demonstrating the importance of ensuring that initial clues are properly pursued after discovery.

Among the follow-up methods available to law enforcement, surveillance/undercover operations and searches following terrorism SARs proved especially fruitful. Together, these activities triggered full-scale investigations in 17 plots (25%). Equally important, however, were searches adjacent to criminal investigations (14 cases, 21%), in which the officers or agents involved thought they were investigating “ordinary” criminal activity, unaware that it was connected to terrorism. Examples of evidence discovered during these investigations include written plans to carry out an attack, surveillance reports or video, weapons stockpiles, and bomb components, such as explosives, explosive precursors, or detonators.

Although the media is filled with exhortations that U.S. intelligence and law enforcement agencies need to do a better job of “connecting the dots” (a somewhat ambiguous phrase describing the ability to find patterns or links across large databases that indicate a terrorist plot), our analysis suggests that this ability has been useful in foiling only a few terrorist plots (3 cases, 4%). Still, we recognize that the open-source nature of our data undoubtedly underestimates the importance of these technological capabilities. Our results should therefore not be interpreted as implying that investments in these programs are unwarranted. Instead, they highlight the importance of more basic processes, such as ensuring investigative leads are properly pursued, which unclassified reports suggest have foiled an order of magnitude more cases (31 cases, 46%).

With respect to the *ISE SAR Functional Standard*, although Material Acquisition and Storage and Weapons Stockpiles events never constituted an initial clue, they provided some of the most frequent secondary clues (i.e., the evidence discovered during follow-on searches). It remains an open question as to why reports of stockpiling or suspicious material have never led directly to foiling plots—even though weapons and explosive stockpiles are generally required to carry out a terrorist attack.

Missed Opportunities to Prevent Terrorist Attacks

We have found references to initial clues that could have foiled plots in 7 of the 18 executed cases. In four of these cases, it appears that the initial clues were not fully pursued—the clue either was simply disregarded or was not forwarded to appropriate agencies. The following cases are examples of these missed opportunities:

- **9/11 Attacks**: As described in *The 9/11 Report* (9/11 Commission, 2004), the Central Intelligence Agency was aware that two of the hijackers had attended a “terrorism conference” in Malaysia and had traveled to the United States. However, information about the two suspects was not shared with the FBI or the Federal Aviation Administration in a timely manner. FBI Director Robert Mueller has also publicly acknowledged other missteps that could have likely prevented the attack, including the failure to authorize the search of Mousaoui's computer in August, and the failure to follow up on requests to investigate suspicious individuals seeking flight training in Phoenix (Locy & Johnson, 2002).

- **2009 Attempted "Christmas Bombing" of Northwest Airlines Flight 253**: The attempted bomber's father reported to State Department officials concerns about his son's extremist views, recent disappearance, and possible travel to Yemen. This led to the creation of a file in the National Counterterrorism Center (NCTC) Terrorist Identities Datamart Environment (TIDE). But the record was not added to the Terrorist Screening Database (TSDB) because of a lack of specific information (DeYoung & Leahy, 2009; Lipton & Shane, 2009).
- **2009 Fort Hood Shootings**: The shooter, Army officer Major Nidal Hasan, had exchanged e-mail messages with a radical Muslim cleric and terrorism supporter (Hess & Gearan, 2009). Screening of the messages by the FBI led to the decision that the exchange was explained by a research paper Hasan was writing and they did not conduct an extensive investigation or follow-up with other relevant agencies (Cyr, 2009; US Senate Committee on Homeland Security and Governmental Affairs, 2011). This decision has been controversial, on the grounds that such extensive contacts by an Army officer with a known terrorism suspect should have been reported to the Army and given more focused attention.
- **1999 Columbine High School Shootings:**[2] In 1998, almost a full year before the attack, an affidavit for a search warrant was issued for one shooter's home, based on a complaint that the shooter was bragging online about building bombs. Police later found a small bomb matching the online description near his home. However, the lead was somehow dropped, and the search was never carried out (Toppo, 2009).

In another three cases, the attackers were already under investigation or court supervision, but still managed to execute an attack:

- **2003 Attempted "Shoe Bombing" of American Airlines Flight 63**: French officials detected suspicious behavior at the perpetrator's point of departure (Paris), as he had paid for his ticket in cash, had no checked bags, and failed to answer all of their questions. However, an extensive screening did not find the explosives in his shoes, and he was allowed to board a flight the next day. The 1-day delay probably helped prevent the explosives from detonating (Elliot, 2002).
- **1999 Shooting Spree at the North Valley Jewish Community Center in Los Angeles**: The perpetrator had a known history of violent assaults, self-injury, and, fantasizing about violent attacks; he was additionally under parole supervision at the time of the shooting (Egan, 1999).
- **2009 Shooting at the Little Rock, Arkansas, Army Recruiting Office**: The shooter was under investigation by the FBI's Joint Terrorist Task Force after being detained in

[2] Although the Columbine shootings did not have a traditional political objective, there was a clear desire to terrorize as many people as possible, including a failed attempt to blow up the school prior to the shootings. As such, the Columbine shootings were included in the GTD, and thus in our analysis.

Yemen for possessing a fake Somali passport and other counterfeit documents (Dao & Johnson, 2009; Thomas, Esposito, & Date, 2009).

While it is obviously alarming that these attacks were carried out by individuals already under supervision/investigation, it must be noted that in one case (the “shoe bombing” attempt) the investigation probably helped foil the execution, and in the other two cases (shootings), the attacks appear to have been fairly impulsive, making them extremely difficult to detect.

Conclusion

Phase I activities generated findings relevant to detecting and preventing terrorism. Results demonstrate that although the threat from AQAM groups is significant, other groups should not be ignored. In total, less than half of identified plots were sponsored or inspired by AQAM. The majority of plots outside of AQAM’s ideology have been from persons with white supremacist or antigovernment/militia ideologies. Of note, attacks from non-AQAM groups rivaled AQAM-related plots in many respects, including a greater likelihood of involving chemical or biological weapons. In addition, a large majority of plots have been conducted by single actors (“lone wolves”) and small groups. Lone wolf plots have also been the most successful, reaching execution more than twice as often as plots by groups.

A second category of findings concerns the initial clues that helped support additional investigation and dedication of law enforcement resources. Perhaps most important was the finding that over 80% of initial clues came from law enforcement (roughly split between federal and state/local) or from the general public. By contrast, intelligence reporting provided initial clues in 19% of plots, although the open-source nature of our data likely underestimates its actual importance. Analysis also revealed that in most instances, the initial clue was a report of the plot, either from a member of the public knowledgeable of the plot or from a would-be terrorist soliciting an undercover agent.

Finally, our results reiterate the importance of both fully investigating potential leads and recognizing signs of potential terrorist activity during the course of routine criminal investigations. Investigations into seemingly unrelated criminal activity, together with suspicious activity reports, led to the discovery of initial clues in nearly a third of the foiled terrorist plots identified. Furthermore, in half the foiled plots examined, law enforcement had to pursue initial clues further to establish enough evidence to launch a full-scale investigation and, in four of the 18 executed plots examined (including 9/11), clues that could have thwarted plots were not fully investigated or shared.

3. Building on Clues: Phase II – Key Stakeholder Interviews

Overview

Phase II sought to better understand how homeland security stakeholders at state and local levels collect, process, and analyze SARs. We also wanted to solicit recommendations for improving the SAR process with an understanding rooted in the needs of both state and local agencies and the context in which they operate. To better understand this perspective, we conducted semi-structured interviews with subject matter experts from the law enforcement, fusion center, and intelligence communities. The following sections describe the findings from these interviews.

Data Collection Methods

Instrument Development

A semi-structured interview guide was developed to use during the interviews. This interview guide contained broad SAR-related areas with specific follow-up questions under each area (**Appendix B** provides the full interview guide). These five areas of the interview guide generally align with the components of the NSI SAR process, including topics on

- Collection and initial reporting,
- Processing and review,
- Analysis and prioritization,
- Sharing and dissemination, and
- Follow-up and feedback.

Respondents

We sought to interview a broad range of individuals at the state and local level who were involved in collecting and processing SARs. We ultimately conducted site visits to organizations representing the following types of roles in the SAR process:

- Local police department (one agency),
- Regional fusion center (one organization),
- State fusion centers (three organizations), and
- Domestic and foreign intelligence.

A total of 20 individuals were interviewed from across these organization types. The roles of individuals that we interviewed included:

- Police officers,

- Police command staff,
- Crime analysts,
- Intelligence analysts, and
- Supervisory intelligence agents.

Site Visits

Site visits were conducted between April 2010 and November 2010. Project staff contacted potential respondent organizations to inquire about their willingness to participate. Once an organization agreed to participate, a copy of the interview guide was sent so its members could better understand the type of information we were interested in gathering while onsite. All site visits were conducted by a team of two to three project staff.

While onsite, we generally met with two to three individuals form the organization in a group interview setting. Prior to the start of the interview questions, participants were informed that their responses would be released only in aggregate form and would not be attributed to any individual.

After completing the site visit, notes were drafted that summarized the interviews. The notes were reviewed by the other members of the team to identify key themes that were consistently mentioned across organizations.

Analysis and Results

Four main themes emerged from the semi-structured interviews:

Lack of a Uniform Reporting Format for SARs

Each organization that participated in Phase II had its own form or template for reporting SARs. While there were common data elements across these forms, the reporting format used was still distinct to each jurisdiction. This variability can hinder information sharing across jurisdictions and creates a knowledge management issue when it comes to using SARs to their fullest potential. As one respondent noted, the challenge lies not in gathering more information but rather in exploiting the information that already exists. In addition, many of the variables on these SAR reporting templates are free text fields that are hard to systematically review and analyze.

Lack of a Systematic Approach for Reviewing SARs

Across organizations, the current SAR review process that respondents described is often highly subjective. In most instances, the reviewing analyst draws upon his or her past experience to assess the incoming SAR. More complex SARs can be reviewed by several staff to determine whether the SAR should be passed to other stakeholders. Individuals tended to focus their review on behaviors that are generally recognized as basic pre-operational activities that terrorists tend to engage in (e.g., materiel gathering, probing). Respondents noted that tips received by telephone are particularly difficult to assess because of their "murkiness." No organization that we met with reported regularly employing a rating scheme or assessment criteria to evaluate SARs. The vast majority of organizations we interviewed had a rotating shift of analysts staffed to review SARs, as opposed to a single dedicated person who reviewed every incoming SAR.

Tendency to Pass SARs up the Chain If There Is Any Suspicion

Organizations tend to pass SARs "up the chain" if there appears to be any chance it might have a terrorism nexus. These organizations may feel that it is the responsibility of the local JTTF or FBI to determine the SAR's ultimate disposition and nexus to terrorism. These organizations may also have received instructions from organizations higher up in the intelligence continuum that this is the proper approach to follow when SARs are received by their agency. While there are certain advantages to over reporting as opposed to underreporting this information up the proper channels, the inability to vet information at the ground level could have negative implications. For instance, one possible effect of this practice is that federal databases may be "watered down" if SARs are being forwarded that ultimately have low information value with respect to terrorism.

Frustration at Rarely Learning Outcomes

Respondents, particularly at local jurisdictions, expressed uniform frustration that they rarely learn the outcome of any information that originates from their agency that they pass up the chain. They are sometimes able to obtain informal feedback, but this feedback is not currently done in a systematic manner. This scenario has ramifications on several levels. First, without feedback, agencies will not know how to improve the SAR information they are reporting to other agencies. That is, organizations do not know if they are reporting the type of information that actually helps stop terrorism. Second, a lack of feedback will most likely lead to less vigor with respect to local level law enforcement reporting suspicious activity that could have a nexus to terrorism. Respondents acknowledged that they may not be able to learn about the specific disposition of a case due to security reasons. However general feedback on whether the submitted SAR was useful would be especially valuable.

Conclusion

In the next chapter (Phase III), we discuss these challenges in the larger context of the NSI process and how it could be strengthened. Specifically we discuss establishing formal review criteria so that SARs are systematically reviewed to determine whether a terrorism nexus might exist; our hope is that these criteria lead to a higher quality of information flowing from the local level. We also describe a feedback mechanism that will allow local law enforcement to know whether the information they have provided is beneficial.

4. Phase III – Assessment of Processes for Collecting, Processing, and Evaluating SARs

Overview

Phase III activities focused on reviewing both the data sources from which SARs originate and the Nationwide SAR Initiative (NSI) process by which SARs are managed and analyzed. The goal was to develop a set of comprehensive recommendations that could be used by law enforcement (i.e., first-line supervisors; middle and upper management staff) and fusion center personnel (i.e., intelligence analysts and supervisors) to improve their management and processing of SARs.

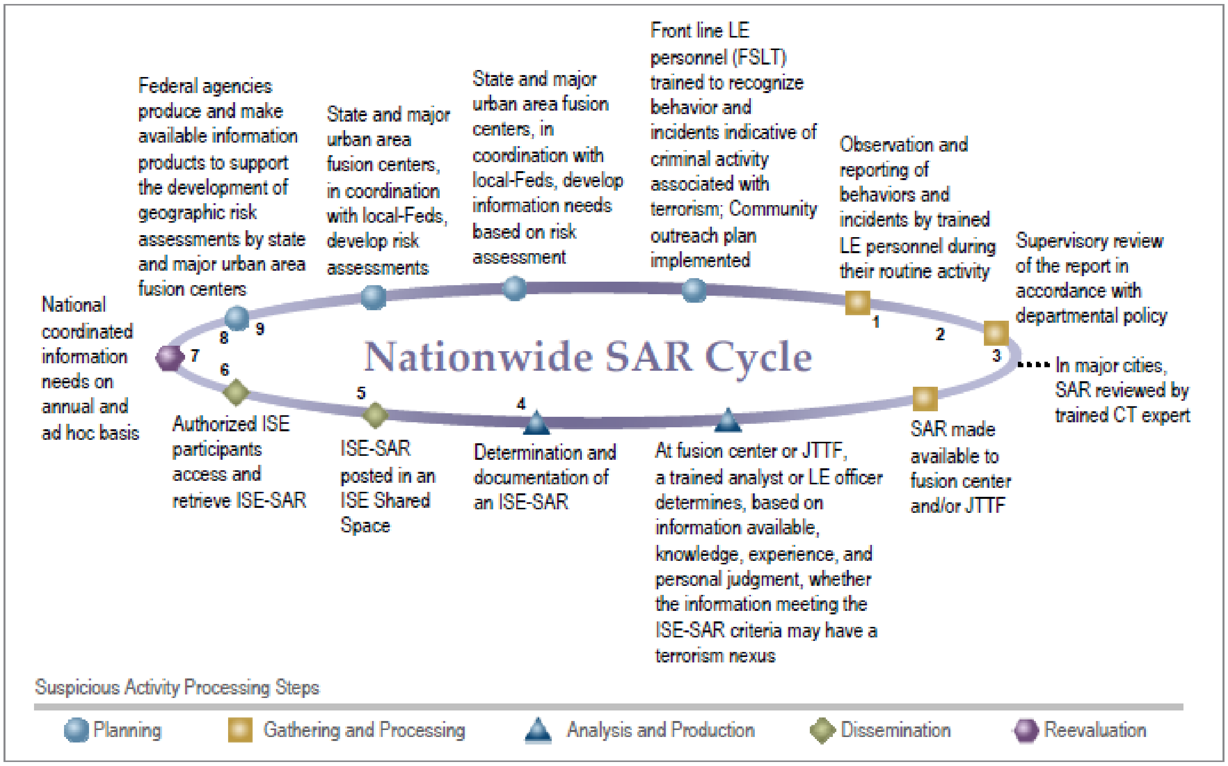
The first section describes the genesis of the SAR process created by the NSI, followed by an assessment of the primary SAR data sources, including a discussion of format, reporting method, and strengths and limitations. We also describe the common steps required for cleaning, pre-processing, and filtering these data sources. We then provide recommendations for improving the collection, processing, and evaluation of SAR data, including adjustments to existing or proposed processes that would increase the utility of the data and the subsequent intelligence that is developed.

Findings on Processes: The Nationwide SAR Initiative and the ISE-SAR Process and Architecture

The NSI sought to develop a process whereby information collected by local law enforcement could be routed to fusion centers or JTTFs and then distributed across jurisdictions in a “shared” space. The NSI began in 2007 as a way to integrate and coordinate initiatives around SARs that were ongoing so that a nationwide process could be developed. These initiatives included development of an ISE-SAR functional standard, efforts by the Los Angeles Police Department to institutionalize SAR reporting by officers, and implementation of the eGuardian system by the FBI. The NSI conducted the design work between 2007 and 2010 and has now moved to assisting agencies that adopt the NSI model.

Figure 8 depicts the NSI process for reporting suspicious activity, which starts with a frontline law enforcement officer observing and reporting behaviors that are consistent with potential terrorism indicators. As defined by the ISE-SAR Functional Standard, a suspicious activity report is “official documentation of observed behavior that may be indicative of intelligence gathering or preoperational planning related to terrorism, criminal, or other illicit intention.” The NSI notes that reports could originate from citizens or private sector personnel but, the initiative is primarily focused on law enforcement’s reporting of suspicious activity.

Figure 8. Top-Level SAR Process Flow


Nationwide SAR Cycle
Front line LE personnel (FSLT) trained to recognize behavior and incidents indicative of criminal activity associated with terrorism; Community outreach plan implemented
State and major urban area fusion centers, in coordination with local-Feds, develop information needs based on risk assessment
State and major urban area fusion centers, in coordination with local-Feds, develop risk assessments
Federal agencies produce and make available information products to support the development of geographic risk assessments by state and major urban area fusion centers
National coordinated information needs on annual and ad hoc basis
Observation and reporting of behaviors and incidents by trained LE personnel during their routine activity
Supervisory review of the report in accordance with departmental policy
In major cities, SAR reviewed by trained CT expert
SAR made available to fusion center and/or JTTF
At fusion center or JTTF, a trained analyst or LE officer determines, based on information available, knowledge, experience, and personal judgment, whether the information meeting the ISE-SAR criteria may have a terrorism nexus
Determination and documentation of an ISE-SAR
ISE-SAR posted in an ISE Shared Space
Authorized ISE participants access and retrieve ISE-SAR
1
2
3
4
5
6
7
8
9
Suspicious Activity Processing Steps
Planning
Gathering and Processing
Analysis and Production
Dissemination
Reevaluation

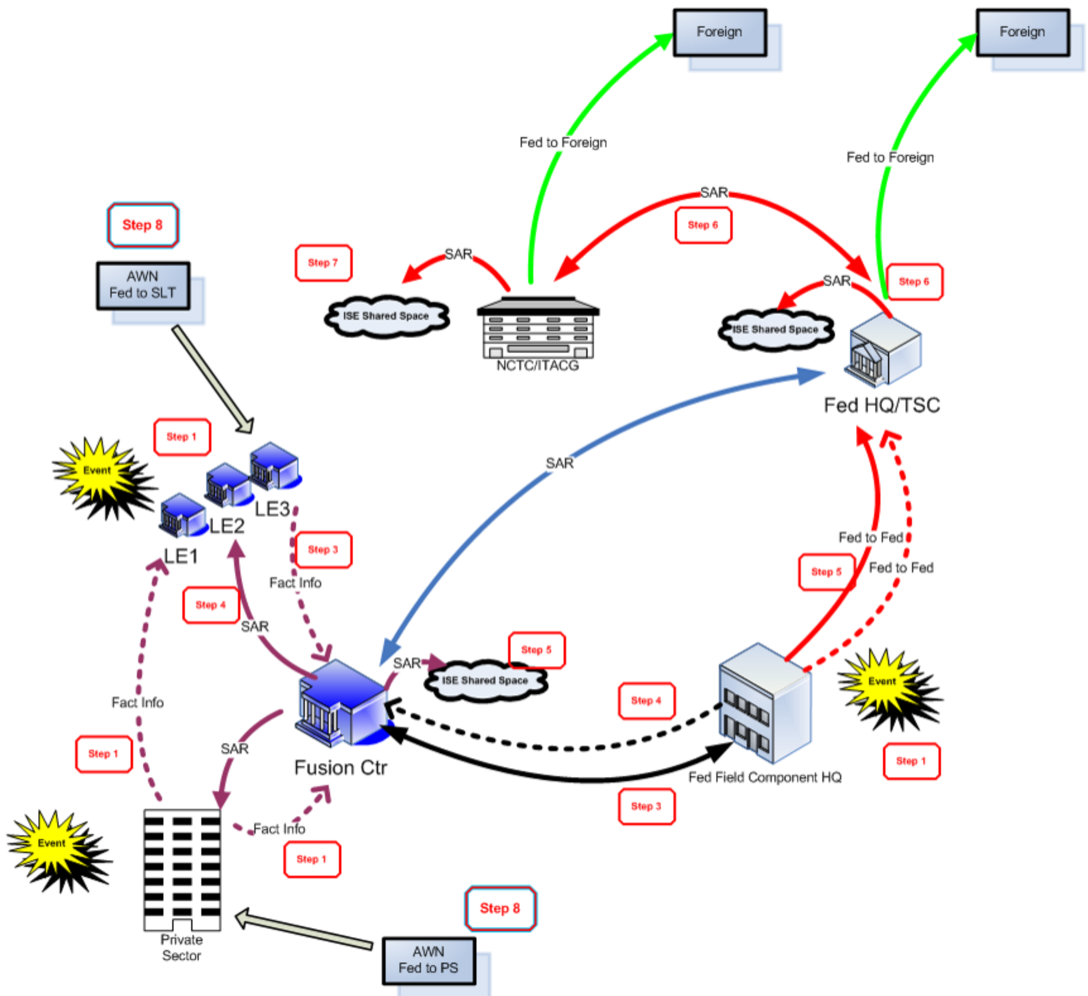
Source: Figure 1. Overview of Nationwide SAR Process, *ISE SAR Functional Standard, Version 1.5*, p. 8.

In this scenario, a SAR is documented by the officer if it meets one or more ISE-SAR criteria, which relate to criminal activity with a potential nexus to terrorism (e.g., intrusion into restricted site) or activity that could be related to terrorism but which requires additional information (e.g., probing of security measures). The report is reviewed by a first-line supervisor to ensure that it was legally obtained and has a potential nexus to terrorism. Two additional levels of review (by a counterterrorism expert and at the fusion center or JTTF) occur prior to the SAR being formatted according to the ISE-SAR Functional Standard and then sent to the ISE-SAR Shared Spaces.

Figure 9 demonstrates the intended information flow proposed by the NSI, showing the tiers of law enforcement involved, ranging from local law enforcement and private security, up through state and regional fusion centers, to federal field components, to federal headquarters functions (Terrorism Screening Center and the National Counterterrorism Center).

The bulk of the information in the system flows from the bottom up, with local agencies providing information about suspicious events and fusion centers and federal headquarters elements evaluating the resulting SARs to determine if they need to be investigated further. Feedback from the federal levels tends to be focused on providing overall information about various types of threats.

Figure 9. Information Flow Diagram for the Nationwide SAR Initiative

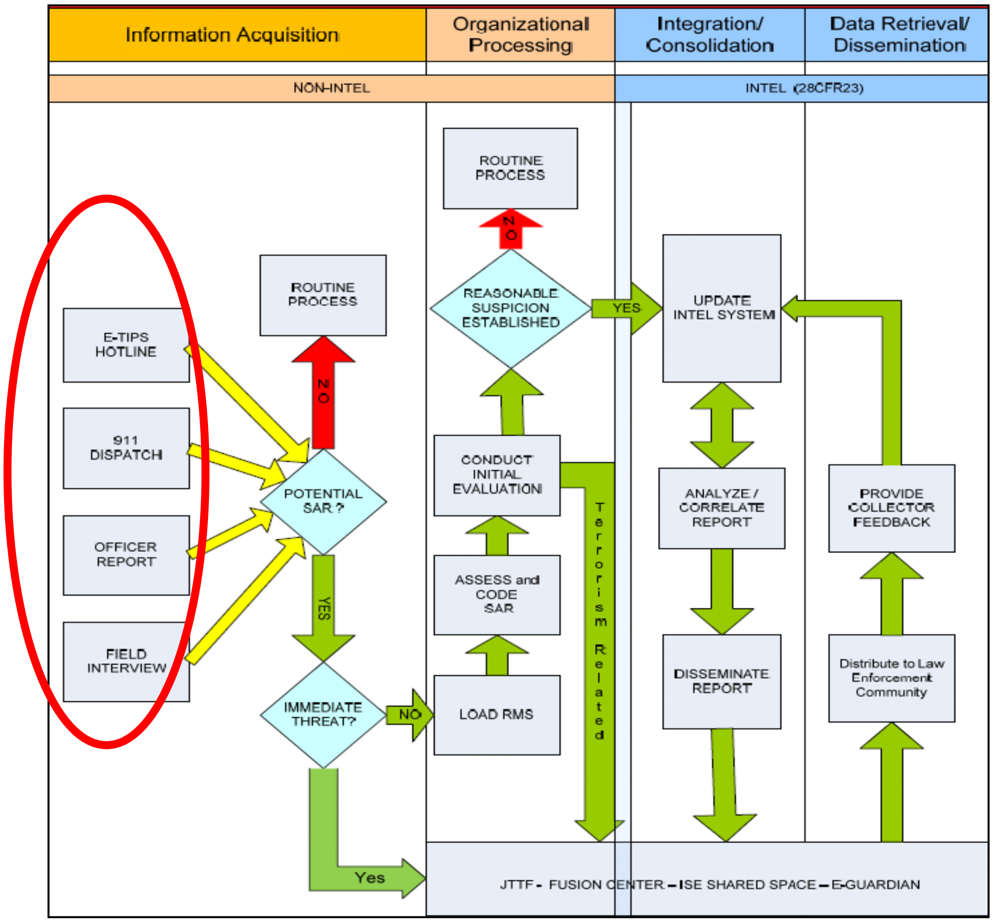


Source: Figure 3 – SAR Information Flow Diagram, *ISE SAR Functional Standard*, Version 1.5, p. 36

Findings on SAR Data: Description and Analysis of SAR Data Sources

For the nationwide SAR process to function effectively, relevant data must be initially acquired at the local level and then shared with other entities. These data will not become more detailed as they flow up, and it is vital that the data coming from the local level are as detailed and informative as possible. The SAR Notional Process (see **Figure 10**) identifies four primary sources from which SARs can be drawn from at the local level (SAR Support and Implementation Project, 2008). These sources include: (1) 911 calls for service, (2) online tips (e-tips) and separate hotlines, (3) law enforcement crime incident reports, and (4) law enforcement field interview reports. In the following sections, we discuss the analytic and reporting challenges associated with each of these data sources and how these challenges might affect the reporting of suspicious activity.

Figure 10. The Notional Suspicious Activity Report (SAR) Process

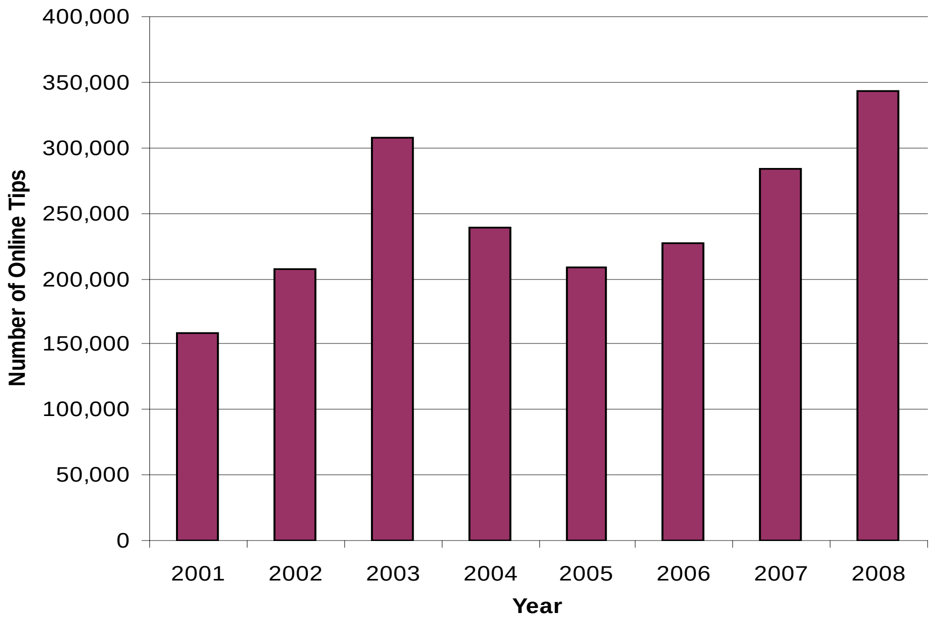

Information Acquisition
Organizational Processing
Integration/ Consolidation
Data Retrieval/ Dissemination
NON-INTEL
INTEL (28CFR23)
ROUTINE PROCESS
NO
REASONABLE SUSPICION ESTABLISHED
YES
UPDATE INTEL SYSTEM
ROUTINE PROCESS
E-TIPS HOTLINE
911 DISPATCH
OFFICER REPORT
FIELD INTERVIEW
NO
POTENTIAL SAR ?
YES
IMMEDIATE THREAT?
NO
Yes
CONDUCT INITIAL EVALUATION
ASSESS and CODE SAR
LOAD RMS
Terrorism Related
ANALYZE / CORRELATE REPORT
DISSEMINATE REPORT
PROVIDE COLLECTOR FEEDBACK
Distribute to Law Enforcement Community
JTTF - FUSION CENTER – ISE SHARED SPACE – E-GUARDIAN

Source: (SAR Support and Implementation Project, 2008)

E-Tips and Hotlines

Internet and phone tip lines have been established to provide the public with a means to report activity that may be connected to terrorism. Although some of these tip lines are designed to receive information about crime more generally, many are geared towards the reporting of potential terrorist behavior. The FBI’s internet tip line is the one of best known systems. As shown in **Figure 11**, the volume of tips was highest in 2008, the most recent year reported.

Figure 11. Volume of Online Tips Submitted to the FBI, 2001–2008



Source: Federal Bureau of Investigation (2010b).

The FBI's internet tip line is run by the Public Access Center Unit (PACU), which consists of about 25 employees. Since 2001, the PACU has received over 2.3 million online tips from around the world (FBI, 2010b). Despite the volume of tips, the FBI notes that each one is carefully evaluated by trained analysts to determine the tip's (and the tipster's) credibility. In describing the process, an FBI official reveals the methodical nature of the reviewing process:

> "At each step there's a human interface. When it goes into the Pyramid system—when it's first captured or submitted—that's automatic. But every single tip is looked at by at least two individuals who have independent quality assurance checks. And then once a tip is determined to have further investigative merit a supervisor would actually review the tip and it would be formatted into electronic communication or entered into eGuardian for further entry into the Guardian system and follow onto the Automated Case Support system." (FBI, 2010a)

The FBI's online form (located at https://tips.fbi.gov/) allows individuals to submit as much or as little information as they want. Importantly, it does not require individuals to provide identifying information, although it seems clear that the FBI has the ability to track down anonymous tipsters via their IP addresses. Text fields exist for the submitter's name, phone number, email address, street address, city, state, zip code, and a narrative with a 7,500 character limit where tipsters can enter a description of the activity or behavior they witnessed.

In addition to the FBI's tip line, many state and regional Fusion Centers provide their own online tip options to the public, and some have dedicated phone tip lines as well. Online reporting formats vary considerably from the basic (e.g., name and description of incident) to more detailed (e.g., vehicle/suspect information, ability to upload video or photographic media).

Strengths**:** Tip lines provide the public with an accessible mechanism to report suspicious activity, and the advertised anonymity likely encourages more individuals to report than might otherwise. Additionally, it provides individuals with a dedicated non-emergency resource for reporting this information instead of adding burden to 911. Thus, these reporting methods likely encourage greater reporting of suspicious activity than would otherwise occur. Furthermore, as DHS implements its “See something, Say something” campaign, more state and regional fusion centers can be expected to establish tip lines.

Limitations**:** Although tip lines help increase the volume of reports potentially related to terrorism, it is not clear that they produce higher quality reports. This speaks directly to the education aspect that must be implemented with these tip lines (e.g., DHS’s “See something, Say something” program). Too often tip lines are implemented without the public being properly educated regarding what information should be reported. Furthermore, because many tips from the public are made anonymously, it is difficult to accurately assess the credibility associated with the source.

Data Considerations**:** Online tip forms generally include variables for collecting information about the person reporting the tip (e.g., name, contact information) and a narrative description of the behavior or activity that person is reporting. They may also include suspect or vehicle information fields. The narrative description is the primary field that relates the behavior that was reported and its free text format makes it more challenging for analysis. It is not clear, however, how frequently these reporting methods are being utilized by the public or how the incoming tips are prioritized and analyzed. According to discussions with fusion center personnel, the level of vetting appears to be variable and highly dependent on the resources and personnel available.

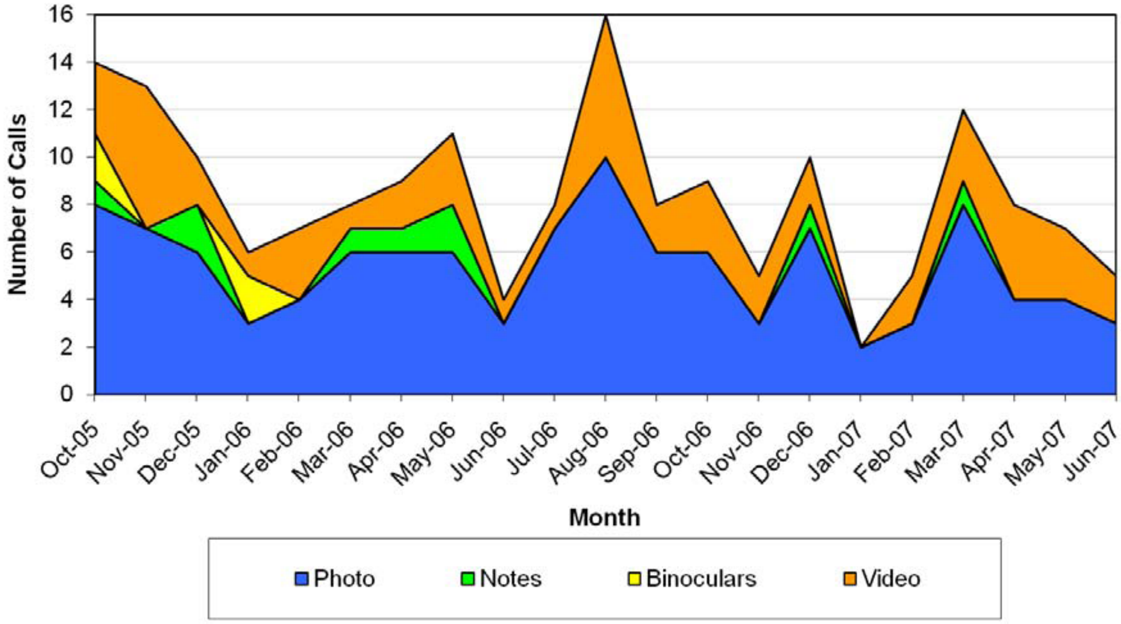
911 Calls for Service

Since the 1970s, the 911 system has enabled citizens to quickly report emergencies to first responders (e.g., police, fire, medical). 911 can also be used by members of the public to report suspicious behaviors that they deem potentially related to either criminal or terrorist activity.

In a previous project, the research team analyzed over 1.3 million 911 calls reported to the DC Metropolitan Police Department over a 20-month period to identify calls with a potential nexus to terrorism (Hollywood, Strom, & Pope, 2008). Results showed that during this time, citizens placed more than 40,000 suspicious person or vehicle calls to 911. However, following a systematic review process that used the call comments along with other information such as call type and location, less than 200 calls were classified as “potentially” related to terrorism. These calls largely represented surveillance activities such as photography and video of critical infrastructure. Although frequencies likely vary across jurisdictions as well as over time (see

Figure 12), these findings suggest that, on average, less than 0.08% of all 911 Call for Service data could be highlighted for subsequent review due to their potential nexus to terrorism. It is important to note that the primary purpose of this research was to develop a process for identifying calls that warrant review and that none of the calls identified were confirmed instances of terrorism.

Figure 12. Types of Behavior Exhibited in Calls Deemed Potentially Related to Terrorism



Source: Hollywood, Strom, and Pope (2008).

Strengths**:** One of the strengths of using 911 to report suspicious activity is the general public's access to and familiarity with the number. Unlike separate tip lines or e-tips, 911 is the primary means for the public to contact the police and comes with an expectation that immediate action will be taken in response to a call (even if the result is simply the forwarding of the call to the appropriate agency). 911 also provides authorities with some limited ability to verify the caller's identify and location, which can potentially be used to request follow up information and to help determine the caller's credibility.

Limitations**:** Most 911 systems are not set up to "flag" incoming tips as potentially terrorism-related. Furthermore, calls potentially related to terrorism will most likely be categorized as "suspicious activity" or "suspicious person," which are considered low priority calls in most police departments. In the Hollywood, Strom, and Pope (2008) study, none of the calls identified as potentially related to terrorism had an associated police incident report and, in most cases, the officer noted in the call comments that no one could be found when they responded to the scene; as a result, the 911 data are effectively lost soon after the report is made.

An alternative to automatic sorting mechanisms of Computer Aided Dispatch data is for the 911 operator to manually screen and flag calls of interest (which is the recommendation of NSI). While this may seem a straightforward and simple task, those familiar with handling tips from the public indicate that in reality the task is far more complex and requires a level of training and expertise far beyond what 911 operators currently receive (based on Phase II interviews).

Data Considerations**:** The main analytical challenges in using 911 data are tied to the volume and quality of the data. 911 data often include variables for call date and time, location (either geo-coded or address), call type, call priority, and police beat (along with a unique case ID). The call comments are not typically included with 911 datasets, but in some departments these data can be retrieved and analyzed. However, when analyzing 911 data to determine if the call contains characteristics indicative of terrorist activity, the call comments must be used. Analyzing the call comments requires some form of text analysis, which could include straightforward approaches such as flagging records with certain keywords. With this approach, considerations such as misspellings and jurisdiction-specific words must also be taken into account.

Similar to tip lines, 911 calls are not cataloged in such a way as to make them available for detailed analysis. Steiner (2010), for example, makes the case that more SARs are necessary to perform truly meaningful trend analyses, viewing each SAR as itself a meaningful data point (e.g., if there are normally one to two reports per month of surveillance of a particular nuclear power facility, a sudden spike to four or five could indicate a potential plot in the works). Currently, however, the most pressing analytic goal seems to be to determine the value of individual SARs, investigating those deemed to be credible, and eliminating those that are not.

Crime Incident Reports

Since 1929, the United States has relied on the Uniform Crime Reporting (UCR) program to capture national crime statistics. Today, crime incidents may be reported via the traditional Summary Reporting System and the National Incident-Based Reporting System (NIBRS). The volume of crime incident reports makes this a promising reporting mechanism for identifying incidents potentially related to terrorism. In 2009, for example, a total of 10.6 million crimes were reported in the United States, including 1.3 million violent crimes and 9.3 million property crimes. However, to date no codes within the UCR are specific to terrorism. The FBI is also implementing the Law Enforcement National Data Exchange System (N-Dex) system, which brings together data—including incident and case reports, booking and incarceration, and parole/probation—from across the United States to better search, link, share, and analyze criminal justice data.

Some agencies have developed their own methods for identifying and categorizing crime incident reports of interest. For example, the Los Angeles Police Department (LAPD) has developed a system by which crime incident reports can be flagged as potentially related to terrorism with the use of a simple check box that was added to the form (Inforwars, 2008). Between March 2008 and March 2009, approximately 1,374 crime incident reports were flagged in this manner, representing approximately 1.2% of the 116,050 total crime incidents reported in the UCR by the LAPD in 2009 (SAR Support and Implementation Project, 2008). The LAPD has reported that the new system led to four terrorism-related arrests and 51 reports being forwarded to the Los Angeles JTTF. The LAPD has also called for the addition of terrorism-specific crime ("MO") codes, including (1) attempts to smuggle contraband through access control points, (2) attempts to acquire illegal explosives, and (3) possession of a biological agent for illegal purposes.

***Strengths*:** A strength of crime reports in relation to SARs is the familiarity and widespread use of the system among law enforcement. The uniformity in how information is reported also allows for potentially more straightforward analysis. Furthermore, the information contained within crime incident reports has presumably been vetted by multiple layers within the law enforcement community, thus increasing its reliability and accuracy for analysis.

***Limitations*:** Because the national UCR program does not include codes specific to terrorism or the ability to identify certain incidents as potentially terrorism-related, the sheer volume of incident reports makes it a difficult source for intelligence analysts to utilize without specific names or identifying information. Additionally, even if analysis were limited to crime incidents known to be commonly associated with terrorism (e.g., money laundering, fraud, identity theft), the distinguishing characteristics that indicate a potential connection to terrorism would likely be contained in the narrative summarizing the investigative findings. Furthermore, while NIBRS may hold the promise for assessing incidents related to terrorism, this would require the addition of new codes specific to terrorism. In addition, as of 2008, only about 25% of the United States was covered by NIBRS data.

Field Interview Reports

Another means by which suspicious activity may be reported at the local level is through law enforcement field interview reports. Although policies regarding field interviews vary from department to department, circumstances that constitute reasonable suspicion may include an individual who matches the physical description of a suspect, commits a minor infraction in the presence of an officer, seems out of place for a particular time or place, is believed to have a weapon or poses a threat, or is acting in a manner that appears otherwise suspicious to the officer (West Palm Beach Police Department, 2005; Truro Police Department, 2000). Activity and behavior potentially related to terrorism may also constitute grounds for a field interview.

The frequency of field interviews also varies across jurisdictions as do the processes by which these data are recorded, saved, and shared. Formats for field interviews also vary but generally include fields to capture basic information about the individual being interviewed (e.g., name, address, phone number, physical description), the circumstances of the interview, and a narrative field to capture the results of the interview. Policies for how long information from field interviews are ultimately archived and shared can vary widely across different law enforcement agencies

It is unknown how many field interviews capture activity with a terrorism nexus. According to the LAPD, field interviews have been used to identify suspects of interest. See for example the "Success Story: LAPD Motor Officer" in which an LAPD officer noticed unusual behavior by a driver and an expired international license during a traffic stop. This resulted in a field interview report, which led to a SAR being submitted and the discovery that the vehicle was connected to a known terrorism suspect (McNamara, 2009).

***Strengths*:** As Phase I of the project demonstrated, the initial clues to a number of terrorist plots have been discovered via observations by law enforcement officers during either routine traffic stops or other routine encounters with the public. Thus, the ability to accurately capture and share data from these encounters will almost certainly provide intelligence analysts with information that has at least partially been vetted by individuals with some training in how to recognize behavior that is out of the ordinary and potentially of interest. Additionally, the mechanism for reporting field interviews already exists and is familiar to law enforcement.

***Limitations*:** Information captured in field interview reports is similar to other sources discussed in that they contain a large amount of unstructured narrative fields. In addition, the volume of reports and lack of a standardized format make searches challenging. Field interviews have also recently come under scrutiny for a perceived infringement on privacy. For example, the New York Police Department (NYPD) was forced to remove the individual names from its "stop and frisk" database (which contained over 2.5 million records going back to 2004) because many of the records did not meet a minimum threshold for inclusion (e.g., probable cause or criminal intent) (Parascandola, 2010).

Assessment and Recommendations for Improving the Collection, Processing, and Evaluation of SARs

The following section presents an assessment of the SAR processes and data sources described above followed by a set of recommendations that could be used by law enforcement agencies and fusion centers to assist in their collection, processing, and evaluation of SARs. These recommendations are divided into three subsections: 1) the collection of SARs; 2) the processing of SARs; and 3) the evaluation of SARs.

The Collection of SARs

Recommendation 1: Expand the ISE SAR Functional Standards to include reports beyond traditional SARs. In a majority of the foiled plots examined, the initial clue came from a public/informant tip or a discovery during what was initially considered a “routine” criminal investigation. These types of clues are at most indirectly referenced in the ISE SAR Functional Standard. Adding them would permit the ISE SAR Functional Standard (and Nationwide SAR Initiative) to be used for all major types of reports associated with state and local law enforcement discovering terrorist activity, significantly expediting information sharing and subsequent investigations.

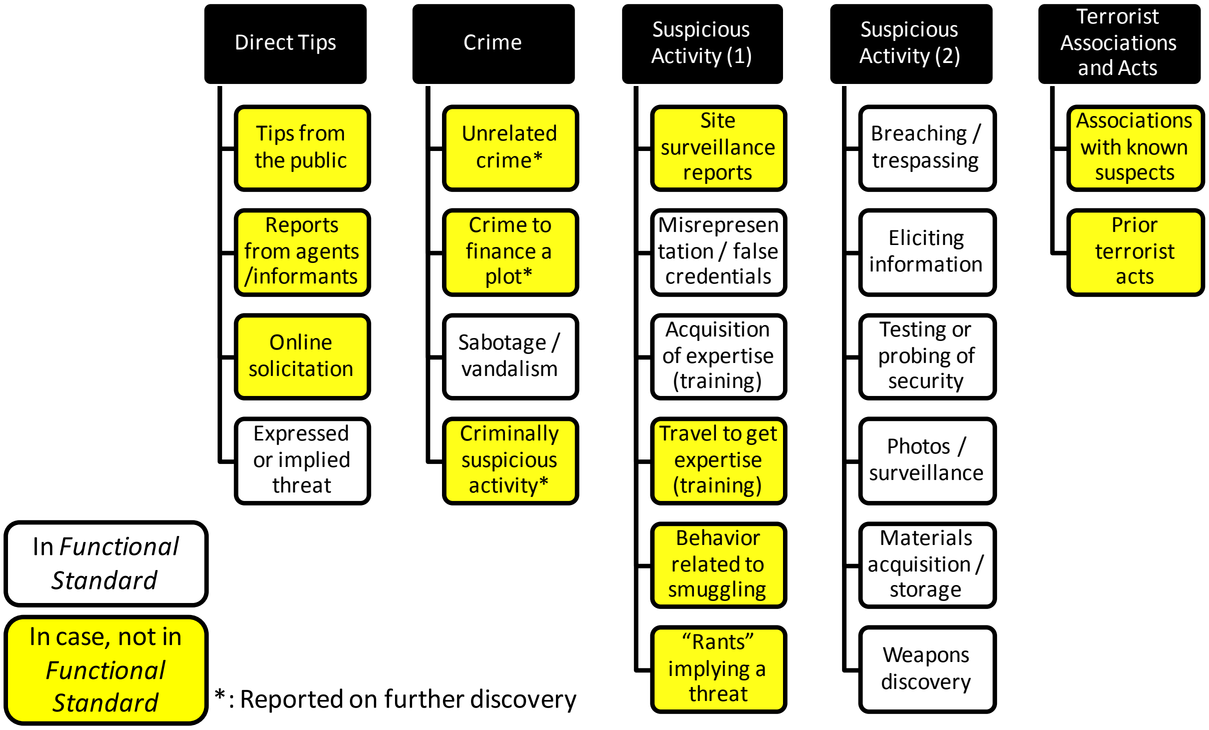
Federal, state, and local law enforcement agencies receive and process a large number of SARs. Nonetheless, we believe there are several reasons why some valid SARs captured in data collected by law enforcement go unrecognized.

First, based on the Phase I findings there were four broad types of SARs that have served as the initial clues leading to foiling terror plots. These were

- Direct tips on terrorist activity in progress, including both tips from the public and tips from agents or informants;
- Findings from criminal investigations, including investigations of both prior crimes and criminally suspicious activity;
- Findings from terrorism investigations, including both new associations of terror suspects and investigations of prior acts of terrorism; and
- Traditional SARs, which constitute what are typically thought of as reports of suspicious activity with a “terrorism nexus.”

Only the latter type is typically thought of as a SAR. While the other types are at least partially reflected in the ISE-SAR Functional Standard, it is not clear how widely they are being recognized as “SARs” and having NSI processes and architecture applied to them. **Figure 13** compares the types of SARs identified as leading to thwarting U.S. plots in at least one case to those types defined in the ISE-SAR Functional Standard. Types shown in yellow led to foiling at least one plot, but are not recognized in the ISE Functional Standard.

Figure 13. Comparing Types of SARs Leading to Foiled Plots With Types of SARs recognized in the *Functional Standard*


Direct Tips
Tips from the public
Reports from agents /informants
Online solicitation
Expressed or implied threat
Crime
Unrelated crime*
Crime to finance a plot*
Sabotage / vandalism
Criminally suspicious activity*
Suspicious Activity (1)
Site surveillance reports
Misrepresentation / false credentials
Acquisition of expertise (training)
Travel to get expertise (training)
Behavior related to smuggling
"Rants" implying a threat
Suspicious Activity (2)
Breaching / trespassing
Eliciting information
Testing or probing of security
Photos / surveillance
Materials acquisition / storage
Weapons discovery
Terrorist Associations and Acts
Associations with known suspects
Prior terrorist acts
In *Functional Standard*
In case, not in *Functional Standard*

*: Reported on further discovery

We recommend that the types shown in yellow be added to the ISE Functional Standard. We recognize that some of these types—notably reports from undercover agents/informants and reports on associations from intelligence work—may not be able to be included in the primary NSI SAR architecture due to the need to keep them secret. However, we believe it is important that these SAR types be recognized as such and that processes similar to that proposed for the main SAR architecture be used to evaluate these SARs and direct follow-up actions. (In many cases, the initial tips required additional vetting; they did not immediately rise to the level of triggering a full investigation, and thus should be considered a type of SAR.) We also believe it would be useful to apply the Functional Standard data format to these closely held types of SARs, to expedite data capture, processing, and need-to-know sharing.

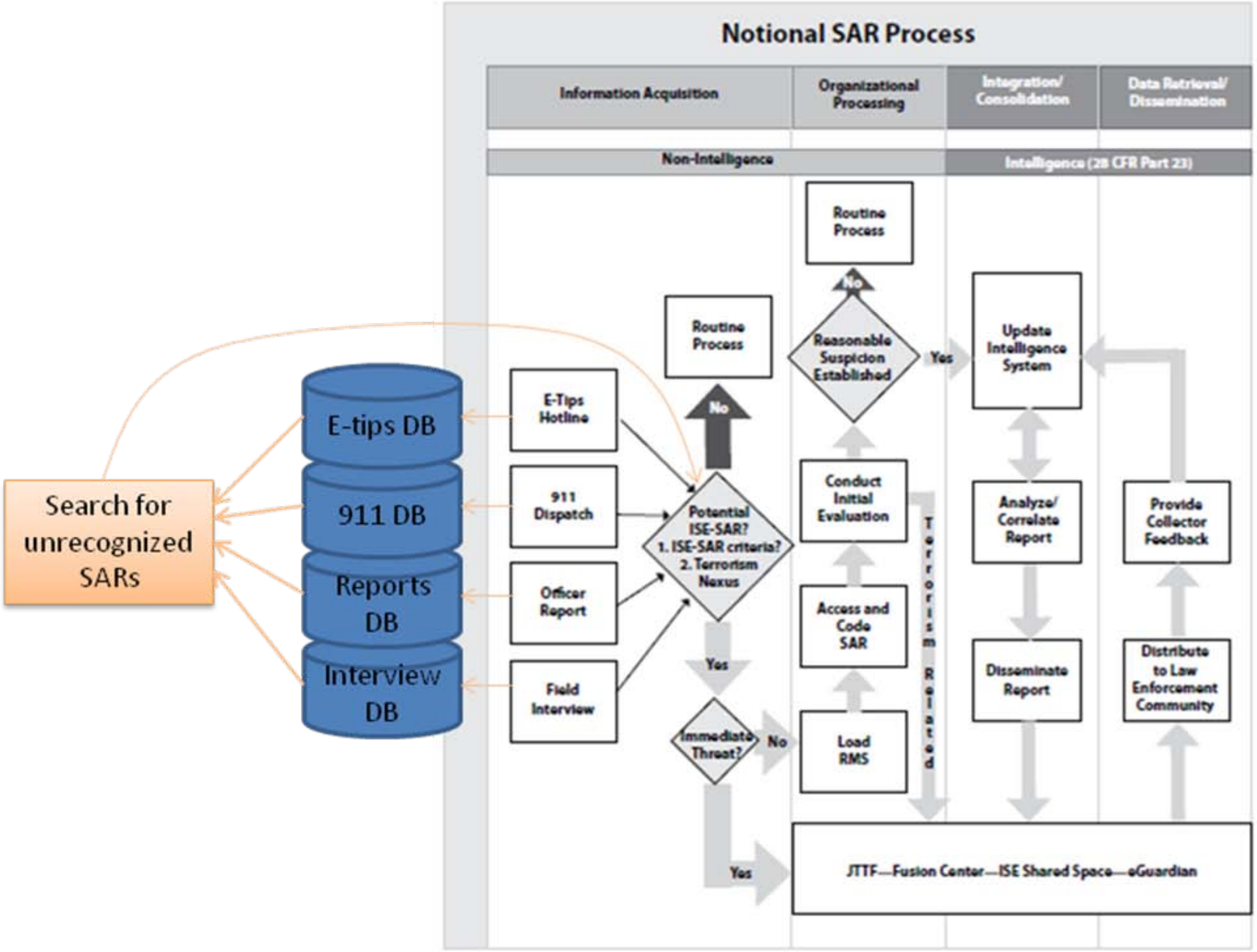
Recommendation 2: Incorporate Automated Search Capability on Databases Likely to Contain SARs

The NSI processes depend on a law enforcement agent recognizing that a call record or report constitutes a SAR and reporting it into the appropriate channel. Relying on manual discoveries—especially in databases seeing huge amounts of activity, such as in 911 call centers—will result in valid SARs going unrecognized. In our earlier study of Washington, DC's

911 call data, for instance, the calls for potential site surveillance or probing were typically coded as “suspicious person” or “suspicious vehicle,” and had not been acted upon since the initial call and response.

We recommend creating an automated trawler capable of searching through databases containing likely valid SARs, such as 911 and 311 call databases, databases of online and call-in tip reports, crime and other officer reports, and field interview reports. In light of the privacy issues associated with this recommendation, the automated trawler should be used only to identify potential cases on interest and would still require law enforcement personnel to review the case and determine if it met the ISE-SAR criteria. **Figure 14** shows what such a capability might look like when applied to the Notional SAR Reporting Process.

Figure 14. Adding an Automated SAR Detection Capability to the Notional SAR Process


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

While the process in **Figure 14** still includes manual identification and referral of incoming data, the process now has automated filtering components as well. In particular, incoming calls and reports are copied to mirror databases and searched for reports that might be valid SARs. An analyst would review flagged reports and forward those that are potential SARs for review.

Recommendation 3: Expand NSI Architecture to Detail Mechanisms for Private Sector Reporting

Third, we recognize that private security groups are logging their own SARs at sites they protect (for companies or non-profit organizations, for example). While the Functional Standard information flow diagram allows for SAR reporting from private organizations, it is not clear how established such reporting relationships are. We recommend further development of reporting mechanisms from private organizations in the NSI architecture.

The Processing of SARs

Recommendation 4: Develop Comprehensive Process Model to Ensure Incoming Tips and Clues are Properly Pursued and Shared

The most important improvements needed for SAR processes relate to following up on incoming tips and reports (“initial clues”). Improvements are needed to ensure that initial clues are analyzed, acted upon, and shared to the extent appropriate.

Broadly speaking, follow-up activities include finding links, direct action, and information sharing.

Finding links involves searching for activity potentially related to the SAR. Examples include reports of the same types of suspicious activity, same people, organizations, vehicles, bank accounts, and so on. Finding associations between persons named in a SAR and known terrorist persons or activity is especially useful. Some links will be found through database searches; others will be found through informal, person-to-person information sharing.

Direct activity involves tasking resources to follow up on the SAR. Examples of direct actions include conducting field interviews concerning the SAR, as well as conducting searches and surveillance if a probable cause threshold for some criminal activity is met.

Information sharing involves sharing information about the SAR with relevant agencies. Inbound sharing involves asking for information on links between the SAR and other persons, assets, and events of interest. Outbound sharing involves posting the SAR to the NSI (and other relevant systems), allowing other agencies to see the SAR in response to queries, and sending the SAR to other organizations that might have an interest.

Managing follow-up activities for SARs creates a requirement to add a control mechanism to SAR processes. The control mechanism needs to contain three elements:

The ***evaluation element*** assesses the SAR (and additional information resulting from follow-up activities when it arrives) and determines what follow-up actions should be taken.

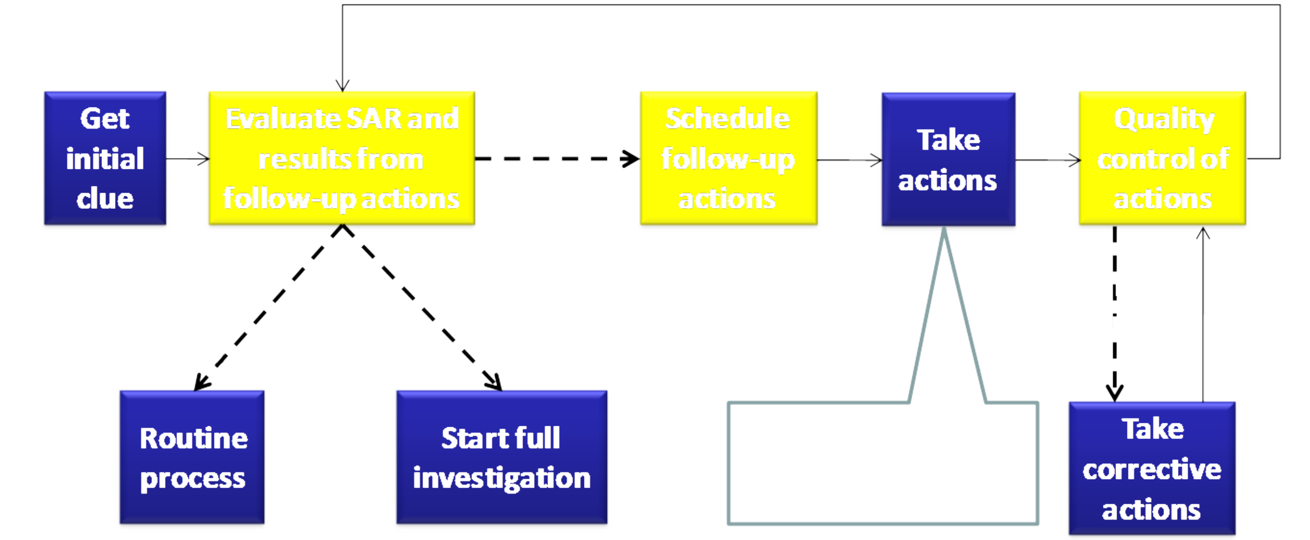
The ***scheduling element*** tasks follow-up activities to be completed by specific persons (and resources) by specified times. The scheduling element also specifies how the activity should be performed and what results are expected (typically, standard templates define desired activity performance).

The ***quality control element*** ensures that the follow-up activities occurred and that activity performance met expectations. Should problems be discovered, this element then determines and schedules corrective activities.

Control elements are partially addressed in the ISE-SAR Functional Standard and related policy. Notably, evaluation elements are present, but coverage of follow-up scheduling and quality control elements is at most implicit. We recommend that all three elements of control be discussed explicitly in federal guidelines for handling SARs.

Figure 15 shows a notional process for analyzing SARs, adding follow-up actions and control elements to the SAR processes described above. Control elements are highlighted in yellow. The process is iterative and dependent on feedback. When a SAR comes in, it is evaluated to determine what further actions are appropriate. If the SAR is considered to be of likely low risk, the "routine process" is applied, which means that the SAR is filed for reference in the appropriate databases, but no further action is taken. If the SAR is considered to be high risk (e.g., the SAR is threatening and detailed enough to predicate an investigation), a formal investigation is launched.

Figure 15. Notional Process for Analyzing SARs


Get initial clue
Evaluate SAR and results from follow-up actions
Schedule follow-up actions
Take actions
Quality control of actions
Routine process
Start full investigation
Take corrective actions

However, for SARs that are threatening but not yet reaching the level of probable cause for a specific plot, follow-up actions are also warranted. Thus, the next step of the process is to schedule appropriate follow-up activities, followed by taking actions that broadly fall in the categories of finding links, taking direct investigative actions, and sharing information. As scheduled task deadlines are reached, the next step is to perform quality control on the actions and their results. If problems are found, corrective actions are scheduled and taken (and are themselves then subject to quality control). If not, the results are forwarded back to the evaluation element to assess the SAR, in light of any new information that has been discovered, and determine appropriate next steps.

The above process can be supported by using XML data standards to track both the content and the status of each SAR. This means having the data format capturing each SAR, including fields related to follow-up activities and results, with subfields for who will do the follow-up activities and by what date/time they are due. (There should also be a field reflecting a positive decision that the SAR is now considered low-risk and that further follow-up activities will not be conducted.) There should also be XML fields to track the results of the actions as well as any problems that arose along with corrective actions. Detecting at least some types of timeliness problems could be automated, by having the tracking system call an alert if a field for an activity result is not updated by the activity's deadline. The ISE SAR Functional Standard provides for some of the needed fields already; it provides "follow-up activity" fields that include start date/time, assigned by, assigned to, activity status, and activity disposition fields.

The Evaluation of SARs

Recommendation 5: Develop a Standardized Instructional Guide to Assist Analysts and Supervisors in Evaluating and Prioritizing Incoming Tips and Clues

State and local analysts we interviewed commonly expressed a desire for a standard guide that would assist them when assessing whether a SAR is genuinely a report of potential terrorist activity and warrants additional review and action; right now, there is no such guide. Further, analysts also expressed a desire to obtain feedback on SARs reported to federal agencies on whether the SARs did, in fact, constitute genuine threats; such feedback reportedly occurs rarely, if ever. As a result, analysts expressed concern that the tendency is to pass along SARs that are remotely terrorism-related to federal authorities, which may lead to overloading databases with largely useless reports and wasting law enforcement resources.

We believe that a "one-size-fits-all" evaluation guide for SARs is probably not realistic. The Phase I results showed wide variation in the initial clues that led to foiled plots, with multiple types of initial clues appearing only once or twice. Expert judgment will almost certainly be required in evaluating SARs.

However, we believe that we can develop an instructional guide that relies heavily on prior cases and subject matter expertise. This guide does include some initial evaluation templates based on a combination of Phase I results (and related analysis of clues leading to foiling material support to terrorism cases) and subject matter expertise. We emphasize that the subsequent templates are based on a handful of exemplars plus judgment and they should be seen as strictly preliminary. Nonetheless, we believe they will provide analysts with some useful insights when analyzing SARs.

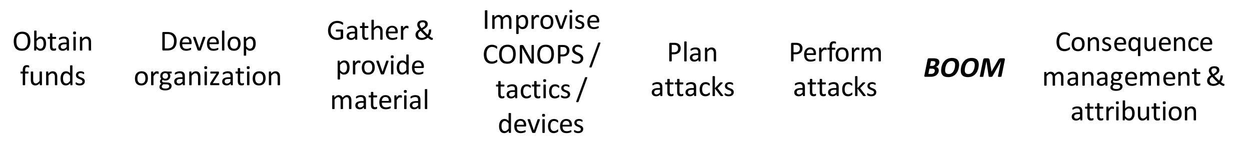
We also recommend that federal authorities routinely provide local and state agencies with feedback on SARs—if not for every SAR, then at least on a representative sample. This feedback does not need to provide the outcome of an investigation; the feedback can be limited to whether SARs like the one provided were useful, and why.

General Evaluation Factors

To create the common templates, we first identified themes that regularly appeared in the SARs leading to thwarting plots. These themes can be summarized as *TASCS—Threatening, Atypical, Significant, Credible, and Specific.*

Threatening. The activity described has a clear relationship (“nexus”) to a terrorism-related activity. More precisely, this means the SAR can reflect activity anywhere in the “terrorism attack chain, including early planning and training stages before the conspirators have settled on a specific target and mode of attack.” By “attack chain,” we mean that terrorist plots broadly follow a common sequence of steps, similar to DHS’s “IED Attack Chain” (shown in **Figure 16**).

Figure 16. A Terrorism Attack Chain (Adapted from DHS’s “IED Attack Chain”)


Obtain funds
Develop organization
Gather & provide material
Improvise CONOPS / tactics / devices
Plan attacks
Perform attacks
BOOM
Consequence management & attribution

Experts we talked to noted interdicting would-be terrorists in early activities is highly desirable, as it allows for the greatest margin of safety to the public and the greatest opportunities to collect intelligence. Consequently, credible reports pertaining to initial-stage terrorist activity should be ranked as highly as late-stage reports, even if specific plots details such as target and means of attack are absent. A report of persons traveling overseas to receive paramilitary training, for example, should receive high priority.

As noted in Phase I, a large proportion of plots were foiled as a result of investigating seemingly “ordinary” crimes or suspected criminal activity. While crime-related reports are indeed threatening, they are typically not directly associated with terrorism. Instead, it is discoveries from adjacent searches during criminal investigations that produce evidence with a terrorism nexus. These special types of SARs are discussed below.

Atypical. Common, benign explanations for the reported behavior are highly unlikely. For example, photographing a landmark like thousands of other tourists is likely not terrorism. Trespassing in secure areas without a reasonable explanation (including burglary, an “ordinary crime”), conversely, is highly atypical.

For direct tips of terrorist plots, “Atypical” tends to be satisfied by definition. However, it still provides a useful check to ensure that the tip is reporting genuinely terrorist activity.

Significant. The SAR describes behavior reflecting genuine personal commitment on the part of the suspect. Thus, simply sending inflammatory e-mail or posts (including most crude death threats) does not count; there needs to be an emphasis on SARs that report “doing” rather than “saying.” Similarly, simply being part of a specific racial/ethnic/ideological group does not constitute a threat; associations with suspected terrorists need to be more substantial than just casual personal or business contacts.

Credible. There is reason to believe the person making the report was reliable, such as a report from a law enforcement officer or security personnel trained in counterterrorism or from someone who has a specific relationship with the person they are reporting on.

Specific. The report is at least somewhat precise and detailed, providing enough information to permit a true evaluation.

Table 3 presents a sample of how these criteria would be applied to four cases included in the Phase I analysis. Following Table 3 is a description of each plot along with the rationale for why the TASC elements did or did not apply to the initial clue for the plot. After this overview using these 3 cases we describe how the TASCS criteria relate to the different types of SARs identified during Phase I.

Table 3. Terrorist Plots and the TASCS Criteria

Terrorist Plot	Threatening	Atypical	Significant	Credible	Specific
NW Flight 253/Christmas Bombing	X	X	X	X	X
David Guy McKay and Bradley Neil Crowder	X	X	X	X	X
Stephen John Jordi	X			X	X
William Krar	X	X	X		

<u>NW Flight 253/Christmas Bombing</u>: On December 25, 2009, a passenger on Northwest Airlines Flight 523 from Amsterdam to Detroit, Umar Farouk Abdulmutallab, attempted to detonate plastic explosive powder hidden in his underwear. Prior to the attempted attack, Abdulmutallab’s father warned authorities about his son’s extremist views and his belief that his son was in Yemen with al Qaeda operatives and other radical Muslims planning an attack on the United States.

This direct tip meets the criteria of threatening, atypical, significant, credible, and specific. The codings of "threatening" and "specific" are worth special mention. The father did not provide any information that his son was involved with a specific terror plot. However, he did provide specific information about his son being involved with terror-related activities, in this case traveling to Yemen to join in Al Qaeda operations there.

In addition, this direct tip is coded as "atypical" largely by default, as the behavior being reported is joining an Al-Qaeda related group. It is considered credible also by default, since the person making the tip was a close relative. Finally, it is considered significant because Abdulmutallab's father reported a significant commitment on his son's part – travel to Yemen to meet with al Qaeda members and potentially engage in terrorist activity.

David Guy McKay and Bradley Neil Crowder: Bradley Crowder, espoused leader of a radical left-wing group called the "Austin Affinity Group," and David McKay, a reported group member, were arrested for allegedly plotting to attack the 2008 Republican National Convention in St. Paul, MN. An FBI Informant infiltrated the group six months prior to the convention, recorded conversations, and travelled with them to the convention from Austin, TX. As a result, the FBI was able to track the group's activities. McKay and Crowder were eventually arrested in St. Paul after purchasing supplies at a local Wal-Mart to make Molotov cocktails. Following a search of an apartment the men were using, police found 8 Molotov cocktails, gas masks, slingshots, helmets, knee pads and containers of a gasoline and oil mixture. Police also discovered a rental trailer containing 35 homemade shields with protruding screw heads, which officials allege the men planned to use against police.

This initial clue fits all of the TASCS criteria. It is threatening and atypical, as the informant both heard direct details of the plot and witnesses the plotters purchase supplies for Molotov cocktails. The informer's status with the FBI provides credibility, and detailed reporting provided specifics. Finally, the purchasing of the materials represents significant action towards carrying out the plot; this was no longer just discussion of taking violent action against the Republication National Convention.

Stephen John Jordi: In 2003, Stephen Jordi, a fundamentalist Christian, was arrested for an alleged plot to bomb abortion clinics in South Florida. It is reported that Jordi's brother alerted authorities of the potential attack, which triggered the FBI to conduct surveillance and use an informant. Over the course of the next several months, the informant kept tabs on Jordi as he surveilled potential targets and acquired supplies. He was finally arrested after being lured by the informant to a boat where bought a .45 caliber pistol and silencer.

The initial clue, the brother's report, is coded as threatening, credible, and specific as the tip came from a relative who provided information about a specific target being attacked. The clue was not coded as atypical since there may have been some prior explanations based only on the brother's initial report. Furthermore, the clue was not coded as significant since, based only on the brother's initial report, it was not clear that the Jordi has exhibited a genuine personal commitment via specific activities. This level of commitment was established following the information provided by the police informant.

William Krar: In 2003, FBI agents arrested white supremacist and anarchist William Krar, along with his wife and a member of the New Jersey Militia, for their roles in an alleged CBRN plot involving 2 lbs of sodium cyanide he had in his possession. Authorities were alerted to the plot when Krar mistakenly mailed a package of fake documents, including forged birth certificates, United Nations and Defense Department identification cards, to an individual he thought was a member of the New Jersey Militia. The recipient of the package called the police who then notified the FBI.

The initial clue, the mistakenly mailed package of fake documents, is coded as threatening, atypical, and significant as the types of documents in the package, fake documents that could potentially allow access to sensitive facilities, indicate that there was mal intention, it is not typically something that would be sent via mail, and is significant because of the sensitive nature of the materials. The clue was not coded as credible since the individual receiving the package could not verify who sent it or what their status was. Furthermore, the clue was not coded as specific since the package of fake documents did not contain any details on specific plans for the materials. The credibility and specificity was established following surveillance conducted by the FBI in response to learning of the fake documents.

Evaluating Direct Reports of Terrorist Activity

Direct reports of terrorist activity constituted the primary source of initial clues that led to thwarted plots. However, this category also had one of the largest executed-plot rates—there were shortfalls with tip evaluations and follow-up activities, as discussed previously.

In addition, undercover agent or informant solicitation was a major source of foiling plots, with the same number of plots foiled by undercover solicitation as direct tips.

Detecting online solicitation also proved useful; three cases were foiled in this manner. Note that multiple follow-up communications were needed to identify those who were truly serious. Threats made by plotters led to foiling two plots. Importantly, the threats were not simply standard prank bomb threats; they were atypical, specific, and threatening. Table C-1 (in **Appendix C**) provides an initial evaluation template for direct reports of terrorist activity.

Evaluating SARs Derived From Criminal Investigations

Criminal investigations proved to be responsible for clues leading to foiling 12 plots. This explains why we have emphasized processes to report terrorism-related discoveries during criminal investigations. The cases were split between precursor crimes directly related to furthering a plot and "ordinary crimes" unrelated to the plot. Effectively, investigating crime provides a two-for-one bonus—most often, the result is solving crimes, but in very rare cases the result was foiling a terrorist plot.

We emphasize that crime (and criminally suspicious activity) constitute special types of initial clues. For the most part, the crimes being investigated were not initially associated with terrorism (i.e., the "Threatening" criteria did not initially apply). Instead, what identified the plot were discoveries during searches adjacent to criminal investigations. Table C-2 (in **Appendix C**) provides an evaluation template for evidence found during these searches.

Evaluating Potential Associations to Terrorist Suspects and Acts

Identifying associations with known terrorists is most commonly associated with intelligence efforts; it was also tied for the number one source of initial clues. However, evaluating which associations were meaningful was an issue. From reports of the cases, the associations were significantly stronger than simple acquaintance or business associations. Examples include suspicious communications, being roommates, participating in suspicious meetings, and so on.

In three cases, investigating prior terrorist activity also helped prevent future attacks. The cases included both prior terrorist attacks (typically, low-level attacks such as vandalism or arson) and material support to terrorism. Table C-3 (in **Appendix C**) provides an initial template for evaluating potential associations.

Evaluating Traditional Reports of Suspicious Activity

Here, "traditional" SARs refer to what is typically thought of as a SAR—a report of suspicious activity that is consistent with terrorist or criminal activity, but typically does not constitute illegal activity. The *ISE SAR Functional Standard* heavily represents these types of SARs. Traditional SARs collectively were responsible for a significant portion of initial clues. Six types of traditional SARs were represented as initial clues with no one type appearing more than three times. The common factor was that aggravating circumstances were present.

Reports of paramilitary training, or traveling to seek paramilitary training, were an initial clue for two foiled terrorist plots, as well as multiple cases of perpetrators attempting to provide material support to terrorist organizations overseas. A direct tip referencing paramilitary training also came into play in the 2009 "Christmas Bomber" case, in which the perpetrator's father reported his son had traveled to Yemen to seek paramilitary training.

Potential surveillance activity, including reports of suspicious photography, videography, and other surveillance and probing activity of sensitive areas, is one of the most frequently referenced and reported SARs. However, a direct observation of such activity led to foiling only a single plot. Conversely, surveillance reports appeared as part of "suspicious document" finds and triggered investigations during secondary searches in several cases. It is not clear whether PSA reports are an underperforming area or are just hard to detect in practice.

The one common factor across the traditional SARs was that aggravating circumstances making the reports genuinely atypical and threatening were present. The one PSA SAR included trespassing into military barracks "to see how U.S. soldiers spent New Year's." "Extremist rants" went beyond heated political opinions to include, in one case, a threat against a government building. Suspicious document SARs included a mis-shipped box of counterfeit security badges, detailed surveillance reports, and a false passport in a conflict area.

As with criminal investigations, SARs for criminally suspicious behavior are not associated with terrorist activity until discoveries are made as a result of investigating the behavior. Thus, the template for evaluating discoveries during routine investigations (Table C-2 in ***Appendix C***) applies. SARs for one type of criminally suspicious behavior, smuggling-like behavior, are worth noting. In two cases, terrorists attempting to smuggle explosives through a checkpoint were flagged for matching drug courier profiles.

Tables C-4 through C-8 (in ***Appendix C***) provide sample templates for evaluating various types of traditional SARs. All should be considered preliminary, as they are each based on a small number of cases. Table C-4 presents a sample template for evaluating PSA SARs. Table C-5 presents a template for evaluating SARs related to paramilitary training and travel to seek paramilitary training. Table C-6 presents a template for SARs related to the discovery of false documents and other forms of misrepresentation. Table C-7 presents a template for SARs related to extremist rants. Finally, Table C-8 presents a template for SARs related to smuggling-like behavior observed at security checkpoints.

5. Conclusion: Key Recommendations and Directions for Future Research

Significant progress has been made in establishing SAR processes, developing a common data format, and providing training to recognize and report SARs. At the federal level, the most notable among these efforts include the Nationwide SAR Initiative and the *ISE SAR Functional Standard* (now Version 1.5). The following identifies some critical results developed from this study, as well as corresponding recommendations for law enforcement, homeland security officials, and policy makers.

Recognize the importance of law enforcement, including state and local agencies, and the public in preventing attacks and support them through investments in education and reporting capacity. More than four in five foiled terrorist plots were discovered via initial clues from law enforcement or the general public. Nearly a quarter of foiled plots were prevented due to clues discovered by state or local law enforcement.

Continue to investigate AQAM, but do not overlook other types of terrorist groups, and pay particular attention to "lone wolves." Most U.S. terrorist plots have not originated with AQAM. Although a large proportion of would-be terrorists have been inspired by AQAM, white supremacist and anti-government/militia ideologies have motivated a large proportion of terrorist plots. There was also a strong trend that most attacks were committed by single actors ("lone wolves") or small groups of people. This trend is particularly noteworthy as lone wolves were found to be almost twice as likely as groups to successfully execute attacks.

Ensure processes and training are in place that enable law enforcement personnel to identify terrorist activity during routine criminal investigations. Nearly one in five thwarted plots were foiled as a result of investigations into seemingly unrelated crimes. Law enforcement personnel need proper training and the necessary checks and balances within their agencies to ensure that they identify and follow up on situations where an investigation of an ordinary crime may lead to potentially terrorism-related activity.

Work to establish positive relationships with local communities and avoid tactics that might alienate them. Of the 68 foiled plots examined, approximately 40% were thwarted as a result of tips from the public or reports by informants. Acquiring information from these sources depends on the ability to establish good relationships between law enforcement and communities with persons in or near radical movements, an ability that is jeopardized by indiscriminately targeting individuals and groups due to their race, ethnicity, religion or ideology.

Expand the ISE SAR Functional Standards to include reports beyond traditional SARs. In a majority of the foiled plots examined, the initial clue came from a public/informant tip or a discovery during what was initially considered a "routine" criminal investigation. These types of clues are at most indirectly referenced in the ISE SAR Functional Standard. Adding them would permit the ISE SAR Functional Standard (and Nationwide SAR Initiative) to be used for all major types of reports associated with state and local law enforcement discovering terrorist activity, significantly expediting information sharing and subsequent investigations. Direct tips of terrorist activity and findings during routine criminal investigations are not explicitly part of the types of SARs recognized by the ISE SAR Functional Standard. Some other types of relevant activity are only indirect matches; an example would be that the closest match for overseas travel for paramilitary training is "acquisition of expertise.

Develop secondary processes for finding SARs in existing data stores. A subset of SARs likely remain undetected in data stores around the country, such as in 911 phone calls and crime incident reports. Past research has shown that for 911 data in particular there are very few systematic processes in place for identifying potential instances of site surveillance or other forms of suspicious behavior related to terrorism. We believe there would be value in developing a routine process for automatically flagging potential 911 calls, crime incidents and other relevant events on a routine basis so that they can be reviewed in more detail by human analysts.

Explicitly introduce scheduling of follow-up activities, checks on progress and results, and corrective actions, into SAR analysis processes to ensure that initial clues are properly pursued and findings shared. For cases in which initial clues did not immediately trigger a full investigation, doing the basics of investigating leads and sharing information across agencies led to foiling the vast majority of plots. Proper training, information technology, and oversight are needed to support the coordination and "quality assurance" of pursuing leads and sharing of findings. Failures to fully follow up on SARs have led to major plots being executed. Specifically, law enforcement must ensure (1) leads are investigated, whether through interviews, contact with informants or agents, or searches, as appropriate; (2) relevant information is shared with other agencies responsible for the investigation of terrorism suspects and those responsible for safeguarding access to U.S. points of entry and aircraft; and (3) investigations are escalated when sufficient evidence has been found.

Create an "instructional guide" that provides overall guidance to look for reports that are Threatening, Atypical, Significant, Credible, and Specific (TASCS) combined with preliminary evaluation templates for specific types of SARs based on prior cases. Fusion center personnel reported a need for a standard evaluation guide for SARs. However, wide variation in what has led to foiling terror plots means that a single guide is not feasible. An instructional guide for evaluating tips and clues, largely based on prior cases of terrorism, can assist law enforcement officers, intelligence analysts, and first-line supervisors in developing a more rigorous process for prioritizing incoming tips and clues from a variety of sources. However, further testing, evaluation, and refinement of the instructional guide is required to ensure that it is both useful for an operational environment.

Possible Directions for Future Research

This study has presented findings and recommendations relevant to law enforcement, homeland security officials, and policy makers. However, there are a number of ways in which this research could be furthered including:

Expanding the scope of the cases studied. The case study analysis presented in this report is limited to known U.S. cases occurring from 1999 to 2009. Additional research might expand the cases studied in several ways. A baseline project would be to continue tracking cases in the United States past 2009. An alternative would be to examine cases prior to 1999; while dated, earlier time periods would include major terrorism cases such as the Oklahoma City bombing and the Atlanta Olympics bombing. A third alternative would be to examine cases in other Organisation for Economic Co-operation and Development (OECD) countries.

Working with fusion centers to examine actual SARs in more detail. In this project, we examined only open media articles about cases. It would be useful to partner with fusion centers to examine samples of SARs that led to foiled plots, as well as SARs that were found to be false positives. We can envision a combination of content analysis and quantitative analysis (text-mining) to attempt flagging differences between the true-positive and false-positive SARs, which might lead to refined SAR evaluation guide. At a minimum, we would be able to compare the numbers of true positive and false positive SARs to derive estimates of the conditional probabilities of various types of SARs being true positives.

Examining targeting preferences in past terrorist attacks. This case study analysis focused on how cases of terrorism have been prevented. However, this analysis could be extended using the same data to study targeting preferences for terrorists over the same time period, using both qualitative and quantitative analysis.

Improving risk assessment models. Immediately after the 9/11 attacks, there was a great deal of demand for models to assess the risks of various types of terror attacks. These models were necessarily driven largely by subject matter expert opinion. However, it should be possible to include what will soon be an entire decade's worth of post-9/11 data of actual and foiled plots in these models, using, for example, various Bayesian approaches.

References

9/11 Commission (2004). *Final report of the national commission on terrorist attacks upon the United States.* Washington, DC: National Commission on Terrorist Attacks

Ackerman, G., & Tamsett, J. (2009). *Jihadists and weapons of mass destruction*. Boca Raton, FL: CRC Press.

Bergen, P., & Hoffman, H. (2010) *Assessing the terrorist threat: A report of the Bipartisan Policy Center's National Security Preparedness Group*. Bipartisan Policy Center. Retrieved September 10, 2010 from http://www.bipartisanpolicy.org/sites/default/files/NSPG%20Final%20Threat%20Assessment.pdf.

Brady, H. E., & Collier, D. (Eds.) (2004). *Rethinking social inquiry: Diverse tools, shared standards*. Lanham, MD: Rowman and Littlefield.

Carafano, J. (2009, December 28). *Re-learning the lessons from the thwarted Detroit airline bombing*. Heritage Foundation web blog. Retrieved April 7, 2010, from http://www.heritage.org/Research/Reports/2009/12/Re-Learning-the-Lessons-from-the-Thwarted-Detroit-Airline-Bombing

Cyr, E. (2009, November). *FBI reassessing past look at Fort Hood suspect*. Associated Press. Retrieved February 10, 2010 from http://www.wusa9.com/news/Fort_Hood/story.aspx?storyid=93462&catid=282

Dao, J., & Johnson, D. (2009, June 3). Suspect in soldier attack was once detained in Yemen. *New York Times*. Retrieved February 9, 2010 from http://www.nytimes.com/2009/06/04/us/04recruit.html?_r=1&ref=us

DeYoung, K., & Leahy, M. (2009, December 28). Uninvestigated terrorism warning about Detroit suspect called not unusual. *Washington Post*. Retrieved February 9, 2010 from http://www.washingtonpost.com/wp-dyn/content/article/2009/12/27/AR2009122700279.html

Egan, T. (1999, August 14). Racist shootings test limits of health system, and laws. *New York Times*. Retrieved February 8, 2010 from http://www.nytimes.com/1999/08/14/us/racist-shootings-test-limits-of-health-system-and-laws.html?sec=&spon=&pagewanted=all

Elliot, M. (2002, February 16). The shoe bomber's world. *Time*. Retrieved February 9, 2010 from http://www.time.com/time/world/article/0,8599,203478-1,00.html

Goldthorpe, J. H. (1997). Current issues in comparative macrosociology: A debate on methodological issues. *Comparative Social Research, 16*, 1–26.

Hess, P., & Gearan, A. (2009, November 21). Levin: More e-mails from Ft. Hood suspect possible. *Associated Press*. Retrieved February 9, 2010 from http://www.newyorkdailytimes.com/news/story/y/48847_levin-more-emails-from-ft-hood-suspect-possible.htm

Hoffman, B. (2003). Al Qaeda, trends in terrorism, and future potentialities: An assessment. *Studies in Conflict & Terrorism*, *26*(6), 429–442.

Inforwars. (2008). LAPD's Anti-terrorism method may become U.S. model. Retrieved 28 February, 2011 from http://www.infowars.com/lapds-anti-terrorism-method-may-become-us-model/

Kelling, G. L., & Bratton, W. J. (2006). *Policing terrorism*. New York: Manhattan Institute.

US Senate Committee on Homeland Security and Governmental Affairs. (2011). A ticking time bomb: counterterrorism lessons from the U.S. government's failure to prevent the fort hood attack. Retrieved May 1, 2011 from http://hsgac.senate.gov/public/_files/Fort_Hood/FortHoodReport.pdf.

Lieberson, S. (1991). Small N's and big conclusions: An examination of the reasoning in comparative studies based on small number of cases, *Social Forces*, *70*(2), 307–20.

Lipton, E., & Shane, S. (2009, December 27). Questions on why suspect wasn't stopped. *Washington Post*. Retrieved February 9, 2010 from http://www.nytimes.com/2009/12/28/us/28terror.html

Locy, T. & Johnson, K. (2002, May 29). FBI missed 9/11 clues, director says. *USA Today*. Retrieved September 17, 2010 from http://www.usatoday.com/news/washington/2002/05/30/fbi-missed-clues-usat.htm

Mahoney, J., & Rueschemeyer, D. (Eds.) (2003). *Comparative historical analysis in the social sciences*. New York: Cambridge University Press.

McNamara, J. (2009). Suspicious activity reporting. Retrieved February 25, 2011 from http://it.ojp.gov/docdownloader.aspx?ddid=1062

Memorial Institute for the Prevention of Terrorism. (2007). *Terrorism warnings* (poster). Retrieved July 1, 2010, from http://www.mipt.org/Websites/mipt/Images/media/Terrorism%20Warnings%20Push%20Card%20-%20New.pdf

National Strategy for Information Sharing (NSIS). (2007, October). *Information sharing: Success and challenges in improving terrorism-related information sharing*. Retrieved April 5, 2010, from http://nsi.ncirc.gov/documents/National_Strategy_for_Information_Sharing.pdf

Parascandola, R. (2010). Gov. paterson signs law forcing nypd to delete stop and frisk database. Retrieved February 21, 2011 from http://www.nydailynews.com/news/ny_crime/2010/07/16/2010-07-16_gov_paterson_signs_law_forcing_nypd_to_delete_stop_and_frisk_database.html

Program Manager for the Information Sharing Environment. (2009, May 21). *Information sharing environment functional standard for suspicious activity reporting, Version 1.5*, ISE-FS-200. Retrieved June 24, 2010, from http://www.niem.gov/pdf/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf

Sageman, M. (2008). *Leaderless Jihad: Terror networks in the twenty-first century*. Philadelphia, PA: University of Pennsylvania Press.

Smith, B. L., Damphousse, K. R., & Roberts, P. (2006). *Pre-incident indicators of terrorist incidents: The identification of behavioral, geographic, and temporal patterns of preparatory conduct*. Washington, DC: National Institute of Justice. NIJ Grant 2003-DT-CX-0003. Retrieved July 1, 2010, from http://www.ncjrs.gov/pdffiles1/nij/grants/214217.pdf

Strom, K.J., Hollywood, J. S., Pope, M. W., Weintraub, G., Daye, C., & Gemeinhardt, D. (2010). Building on Clues: Examining Successes and Failures in Detecting U.S. Terrorist Plots, 1999-2009. Institute for Homeland Security Solutions

Study of Terrorism and Responses to Terrorism (START). (2010, May). *Global Terrorism Database: GTD variables and inclusion criteria*. Retrieved July 9, 2010, from http://www.start.umd.edu/gtd/downloads/Codebook.pdf

Suspicious Activity Report (SAR) Support and Implementation Project. (2008). Findings and recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project. Retrieved April 5, 2010, from http://iwitnessvideo.info/files/mccarecommendation-06132008.pdf

Thomas, P., Esposito, R., & Date, J. (2009, June 3). Recruiter shooting suspect had ties to extremist locations: Investigators probing attack to determine whether shooting suspect acted alone. *ABC News*. Retrieved February 9, 2010 from http://abcnews.go.com/Politics/story?id=7732467&page=1

Toppo, G. (2009, April 14). 10 years later, the real story behind Columbine. *USA Today*. Retrieved February 8, 2010, from http://www.usatoday.com/news/nation/2009-04-13-columbine-myths_N.htm

Federal Bureau of Investigation. (2010a). Inside the Internet Tip Line: Special Agent Eric Reese, watch commander of the Public Access Center Unit, describes what happens when crime tips are submitted on the FBI website. Retrieved October 22, 2010 from http://www.fbi.gov/news/videos/mp4/tips062909.mp4%20%20%20/view

Federal Bureau of Investigation. (2010b, June 26). To track a threat: Inside our internet tip line. Retrieved October 22, 2010 from http://www.fbi.gov/news/stories/2009/june/tips_062609/

Steiner, J. (2010). More is better: The analytic case for a robust suspicious activity reports program. *Homeland Security Affairs, 6*(3).

Truro Police Department (June 1, 2000). Field Interview and interrogations (OPS-6.08). Retrieved November 10, 2010 from http://www.truropolice.org/On%20Line%20Manuals/Field%20Interview%20and%20Interrogation.pdf

West Palm Beach Police Department (2005). Field interview – SOP III-11. Retrieved November 10, 2010 from http://www.wpbpolice.org/policies/downloads/-III-11FIELDINTERVIEW.pdf

Hollywood, J. S., Strom, K. J., & Pope, M. W. (2008). *Developing and testing a method for using 911 calls for identifying potential pre-planning terrorist surveillance activities*. Prepared for the National Institute of Justice.

Appendix A. Description of Variables and Coding Scheme

The full dataset is available upon request.

Variable	Description
Identifying information	• Unique ID • Short name for the plot • Date plot was executed or thwarted with an arrest • Location of plot/intended target • Whether the plot reached execution
Plot description	Text field describing names, dates, places, and a brief summary of the allegations/convictions
Group ideology/motivation	Structured field describing the group's ideology: • Left (broadly "Leftist" ideologies besides those related to environmental or animal rights causes) • Right (anti-liberal beliefs distinct from militia/anti-government and white supremacist ideologies) • Anti-Muslim • Animal rights • Anti-abortion • Militia/anti-government (groups rejecting federal governmental authority) • Al Qaeda and Allied Movements (AQAM) • AQAM-inspired (persons who are motivated by AQAM but have no direct connections with an AQAM group; commonly categorized as "homegrown terrorists") • White supremacist (includes both traditional white supremacist and neo-Nazi groups) • Unknown/non-ideological (persons motivated by unknown ideological reasons or for reasons not clearly ideological but still intended to terrorize a particular community, e.g., the attacks at Columbine)
Group size	Structured field indicating the composition of the plotter(s): • Single Individual ("lone wolf") • A small unorganized group (a collective effort with no formal structure) • A small organized group (a collective effort that has a name and a formal structure) • A large group

Variable	Description
Type of target	Structured field describing the type of target: • Abortion (clinic or doctor) • Aircraft (always a commercial jet liner) • Airport • Bank • Bridge • Bus • Community center • Convention (such as the Republican National Convention) • Gas station • Gas storage tanks (natural gas storage tanks) • Government executive (targeted for assassination) • Government building • Home/House • Judicial personnel (judges or law enforcement officials targeted for assassination) • Military base • Power grid (can be power plants or transmission lines) • Religious building (examples have included churches and mosques) • School • Scientist (targeted for assassination) • Shopping mall • Skyscraper • Street (refers to an attempt to shoot or bomb a crowd of people on a street) • Train • Unknown
Nature of attack	Structured field labeling the plot as one of the following: • Chemical, biological, radiological, or nuclear (CBRN)—plots to use weapons of mass destruction in some form • Conventional—plots to use conventional means of attack, such as bombings or shootings to kill people indiscriminately • Targeted—plots to assassinate or injure specific individuals
Type of initial clue	Structured field for the type of the initial clue that tipped off law enforcement (see **Table 1** for a full list of the variables used)
Source of initial clue	Structured field for where the clue came from: • Intelligence efforts • Federal law enforcement • State/local law enforcement • Tips from the general public (unsolicited)

Variable	Description
Investigation progression	Text field describing how investigators found sufficient evidence to launch a full investigation
“Triggering” clue	Structured field for the type of evidence that led to a full investigation (see **Table 2** for a full list of the variables used)
End result	Text field describing the final outcome of the plot and actions taken against plotters/attackers
Sources	Text field listing the references used in the case

Appendix B. Phase II Interview Guide

Suspicous Activity Report Project - Phase II

Law Enforcement Interview Guide
(Estimated Interview Duration: 60 minutes)

A. STUDY BACKGROUND

While much has been done in recent years to improve the collection and sharing of law enforcement information, to date there remains limited progress in the development of methods to better analyze and share information from Suspicious Activity Reports (SARs). SAR data, which comes from a variety of sources—including 911 calls for service, police field interview reports, crime incident reports, tip lines, and classified informants/undercover agents—provide investigators with information that may prove critical to thwarting developing terrorist plots. However, several problems in the SAR process persist, including the lack of standardized formats and practices across jurisdictions and the inability to link suspicious incidents across disparate data sources. These issues pose unique challenges for analysts and investigators.

This study aims to gain a better understanding of the SAR process in order to develop more effective methods for detecting and analyzing information that may be associated with terrorist activity. Specifically, this project seeks to improve the collection, processing, filtering, linking, and prioritizing of SAR information to enable law enforcement to more effectively thwart terrorist attacks before they occur.

The goal of the project is not to criticize or draw attention to the problems of any specific department or agency. The names of the individuals and agencies involved in this study will not appear in any published reports, and your participation in this project is completely voluntary.

B. INTERVIEWEE BACKGROUND

1. **Tell us about your position and the types of duties you perform.**

   Probes:

   a. Number of years with agency?
   b. Number of years in present position?

2. **Describe your individual role in the SAR process.**

   Probes:

   a. Day-to-day frequency of SAR handling?
   b. Overall experience level with SARs?
   c. What are some of the specific functions you regularly perform with regard to SARs? Can you provide some examples?
   d. What types of training have you received to perform these duties?

3. **Describe your department/agency's role in the SAR process.**

   Probes:

   a. How does your department/agency fit into the overall SAR process?
   b. What specific tasks is your department/agency responsible for?
   c. What do you perceive are your department/agency's biggest strengths? Weaknesses?

C. COLLECTION AND INITIAL REPORTING

1. **How is suspicious activity reported by civilians to your agency?**

   Probes:

   a. In what format are these data received? Stored?
   b. How do civilians most commonly report suspicious behavior?
   c. Can you give some examples of the types of things civilians typically report?

2. **How is suspicious activity reported by police?**

   Probes:

   a. In what format are these data received? Stored?
   b. How do police most commonly report suspicious behavior?
   c. Are there ways to "flag" ordinary incident reports? If so, who does this?
   d. What type of training is given to officers on how to recognize activity of interest?

3. **Which type of reporting (police vs. civilian) is more frequent?**

4. **Where is this information stored? How long is it kept?**

5. **Who has access to this information?**

   Probes:

   a. Within your agency?
   b. External to your agency?

6. **In the last 5 years, have there been any significant changes to these reporting methods/formats?**

   Probes:

   a. What in your opinion prompted these changes?
   b. How have these changes impacted the SAR process?

D. PROCESSING AND REVIEW

1. **Who within your agency initially processes these reports?**

   Probes:

   a. What types of systems do they use for processing?
   b. What level of training or qualifications are required?

2. **Who is responsible for reviewing these reports?**

3. **Describe the basic process of how these reports are processed and reviewed.**

   Probes:

   a. How many people are involved?
   b. How much of the process (if any) is automated?
   c. Are the processes different for different types of reports?
   d. What in your opinion works well in the process?
   e. What could be improved?

4. **What happens when there is information missing from these reports?**

   Probes:

   a. What type(s) of information is most frequently missing?
   b. Are there ways to reduce the amount of missing information?
   c. Are reports ever "cleaned"? If so, how often?

E. ANALYSIS AND PRIORITIZATION

1. **How do you determine which reports are meaningful (i.e., potentially related to terrorism)?**

   Probes:

   a. What type of training have you received in this area?
   b. How much of the process is subjective and how much is rule-based?
   c. Can you provide some examples of reports you thought were particularly meaningful?

2. **What type(s) of information is generally the most important in making these determinations?**

3. **Are particular types of reports given greater weight than others? Which ones?**

4. **How are incidents connected across different databases and reports?**
   Probes:

   a. Are any of these mechanisms automated?
   b. What do you see as the biggest challenges to connecting incidents?
   c. Are there certain databases/reports that are harder to connect than others?
   d. Is your agency able to connect your data with data from other agencies/jurisdictions?

5. **How are potential threats sorted and prioritized?**
   Probes:

   a. Who's responsible for this sorting and prioritization?
   b. Are there particular levels of threat assigned?
   c. Are there guidelines/SOPs to help assign threat levels?
   d. How much of a threat assessment is based on the investigator's suspicions/experience?

6. **Has your agency studied trends in these reports to determine how the process can be improved?**

7. **How do you think the sorting and prioritization process could be improved?**

8. **Have you come across practices (either within or outside your agency) that you think are particularly effective?**

9. **Do you think that information from SARs is useful in uncovering potential acts of terrorism?**
   Probes:

   a. What percentage of the time?

F. SHARING AND DISSEMINATION

1. **How is information disseminated outside your agency?**

   Probes:

   a. What systems or procedures are in place to facilitate the sharing of SAR information?
   b. What type of format is used to share information?
   c. Are some types of information shared more effectively than others? Which ones?
   d. How much of the sharing is a result of "pushing" and how much a result of "pulling"?
   e. How much of the sharing process is automated?

2. **What do you think could be done to improve communication between different agencies and jurisdictions?**

   Probes:

   a. What do you think works best about the current system of information sharing?
   b. What do you see as the biggest weaknesses?
   c. Have you encountered specific instances where better sharing of information could have helped identify terrorist activity earlier?
   d. What types of changes to information sharing have been made over the last 5 years?
   e. Have you noticed any improvements as a result of these changes?
   f. What do you see as the biggest remaining challenges?

F. FOLLOWUP AND FEEDBACK

1. **What happens to SARs after they have been disseminated to other agencies?**

   Probes:

   a. Do you hear back from the recipient agencies?
   b. Are there mechanisms in place to ensure that the appropriate agencies actually received the information?
   c. What do you when other agencies send you information?

2. **Is it helpful to have feedback on reports that you submit?**

3. **How do you think the feedback process could be improved?**

Appendix C. Sample Templates for Evaluating Different Types of SARs Using the TASCS Criteria

Table C-1. Sample Template for SARs Related to Direct Tips of Terrorist Activity

Includes: tips from the public; reports from agents and informants; online solicitation from someone wanting to engage in a terror attack; direct threat of an attack
Threatening: report of a suspect engaging in terrorist-related activity anywhere along the event chain, including initial planning and/or solicitation
Atypical: no benign explanations for the reported behavior are apparent, such as lawful protest activities
Significant: behavior reported shows a significant commitment (time, resources) to carrying out an attack (or providing material support to terror attacks, such as travel for site surveillance); for online solicitation and direct threats, subsequent communication confirms the perpetrator is willing to make substantial commitments to carrying out an attack
Credible: witness able to explain how and why he or she learned of the terror-related activity; for online solicitation and direct threats, subsequent communication confirms the perpetrator is serious about carrying out an attack
Specific: witness able to describe the terror-related activity in detail; for online solicitation and direct threats, subsequent communication confirms the perpetrator is serious about carrying out a specific attack, as opposed to general material support

Table C-2. Sample Template for Materials Found During Searches Adjacent to Criminal Investigations

Includes: discovery of materiel with terrorism implications, such as weapons, explosives, electronics components, and suspicious documents
Threatening: (1) large caches of weapons, any CBRNE materiel other than standard household / industrial products; (2) caches of electronics components (timers, etc.) without cause; (3) documents describing plans to carry out an attack; detailed site surveillance reports
Atypical: no benign or “ordinary crime” explanations for the materiel. Ex: (1) Weapons numbers or types atypical for the area; any CBRNE materiel without justification. (2) Large quantities of components not normally collected without justification (e.g., person runs a repair business) (3) Documents either contain express threats or describe features of sites in far more detail than tourism, without business justifications
Significant: size and/or scope of materiel shows significant commitment (time and resources) by suspect
Credible: officer/agent able to explain the circumstances of the search
Specific: officer/agent able to describe the materiel in detail (or provide the materiel)

Table C-3. Sample Template for SARs Related to Suspicious Associations and Communications

Includes: discovery of associations/communications with known terrorists and terror suspects
Threatening: (1) Relationship involves meetings or communications that are associated with terrorist activity; (2) relationship is close and continuing such that the associate would be likely to know what was going on (roommates, close relative, etc.)
Atypical: not a casual association, such as a routine business relationship (e.g., pizza delivery), casual acquaintance, or infrequently contacted relative
Significant: (1) participation in meetings and communications are not casual (involve travel or active participation); (2) ongoing close and continuing relationship
Credible: observer able to explain how and why they learned of the suspicious associations
Specific: observer able to report significance and/or content of associations in detail

Table C-4. Sample Template for SARs Related to Site Surveillance

Includes: discovery of site surveillance reports; use of false credentials/misrepresentation on site; breaching/trespassing; elicitation; security probing; photography/observations
Threatening: witness/reviewer can identify how behavior might contribute to a downstream terrorist attack; behavior is a criminal violation in its own right (e.g., trespassing, misrepresentation)
Atypical: not behavior typical of tourists and work crews (including nosy/lost tourists); reasons given for behavior not credible
Significant: intrusions appear intentional; site surveillance sessions are unusually lengthy or detailed
Credible: witness able to explain why he or she was there and why he or she could see behavior; witness had some knowledge of what constitutes specific activity
Specific: witness able to report behavior in detail

Table C-5. Sample Template for SARs Related to Paramilitary Training and Travel

Includes: paramilitary training (e.g., acquisition of weapons/explosives/other military expertise); suspicious travel to seek such training
Threatening: (1) training: training in skills key to carrying out a terrorist attack, such as weapons, explosives, HAZMAT, infantry tactics; (2) travel: traveling to a paramilitary camp or area known for such training camps
Atypical: (1) training: no professional or recreational justification; (2) travel: no professional, recreational (tourism), or personal (visiting friends and family) justification; (3) both: reasons given not credible
Significant: training or travel: substantial commitment in terms of time and resources devoted
Credible: observer able to explain how he or she was able to learn or about or observe person's training, training plans, or travel plans
Specific: observer able to describe key details of suspect's training or travel activities

Table C-6. Sample Template for SARs Related to Discoveries of Suspicious Credentials/Misrepresentation

Includes: misrepresentation/false (suspicious) credentials
Threatening: facility/infrastructure that is the site of the attempted breach is of high relevance for terrorism (airports, mass transit, critical infrastructure sites, sensitive military sites, etc.); surrounding communications or evidence implies credentials are for terrorism-related purpose
Atypical: upon investigation, no "ordinary" reason (prank, ordinary crime) identifiable
Significant: Same as atypical
Credible: observer able to explain how and why he or she learned of the misrepresentation/false credentials
Specific: observer able to describe key details of suspect's misrepresentation and/or how the observer discovered the false credentials and why they are false

Table C-7. Sample Template for SARs Related to Extremist Rants

Includes: extremist rants
Threatening: key factor: rants must imply action—either solicitation for a plot or a credible threat of violence
Atypical: not routine expressions of extremist views, including sympathies for violent acts
Significant: repeated and/or lengthy discussions clearly implying solicitation or a threat of violence—not offhand remarks or expressions of emotion
Credible: witness able to explain how and why he or she was involved in the discussions and why he or she believes the suspect should be investigated
Specific: witness able to describe content of discussions in detail

Table C-8. Sample Template for SARs Related to Smuggling-Related Behavior on Transportation Systems

Includes: smuggling-related behavior at transportation checkpoints (TSA checkpoints, border crossings, ferries, etc.)
Threatening: person matches profiles for carrying contraband, as commonly taught by U.S. government agencies
Atypical: on investigation, either no materiel discovered, or “ordinary crime” material discovered (drugs, food); if weapons discovered, person does not have a credible justification (including routine “criminal” justifications)
Significant: materiel discovered has significant utility in carrying out a terrorist attack
Credible: witness able to explain how and why he or she identified the person as a suspect (typically security personnel)
Specific: witness able to describe person’s behavior and discovered materiel in detail