Document Title:	Developing and Testing a Method for Using 911 Calls for Identifying Potential Pre-Planning Terrorist Surveillance Activities
Author:	John Hollywood ; Kevin Strom ; Mark Pope
Document No.:	222911
Date Received:	May 2008
Award Number:	2006-IJ-CX-0024

Opinions or points of view expressed are those of the author(s) and do not necessarily reflect the official position or policies of the U.S. Department of Justice.

May 2008

Developing and Testing a Method for Using 911 Calls for Identifying Potential Pre-Planning Terrorist Surveillance Activities

Final Report

Prepared for

National Institute of Justice
810 Seventh Street, NW
Washington DC, 20531

Prepared by

John Hollywood
Kevin Strom
Mark Pope
RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI Project Number 0210385.001

RTI Project Number
0210385.001

Developing and Testing a Method for Using 911 Calls for Identifying Potential Pre-Planning Terrorist Surveillance Activities

Final Report

May 2008

Prepared for

National Institute of Justice
810 Seventh Street, NW
Washington, DC 20531

Prepared by

John Hollywood
Kevin J. Strom
Mark Pope
RTI International
3040 Cornwallis Road
Research Triangle Park, NC 27709

RTI International is a trade name of Research Triangle Institute.

Table of Contents

Chapter **Page**

Appendix

List of Figures

List of Tables

Number **Page**

Executive Summary

ES.1 Background

Terrorist attacks are sudden and purposively designed to shock the general public. Yet, terrorist attacks also require significant planning. Selecting targets, observing and testing security measures, and asking probing questions represent critical activities in the terrorist attack cycle. These specific activities, referred to as “hostile surveillance,” offer the best opportunity to prevent and deter terrorist attacks before they occur, because these activities require terrorists to expose themselves, making it easier to detect their true intentions. Historically, hostile surveillance that has culminated in a terrorist attack has been identified post-attack, after a larger pattern of ongoing suspicious behavior was identified, compiled, and characterized, and after the true nature of the activity was revealed.

Law enforcement agencies face several challenges to collecting data on and analyzing reports of suspicious activity, including instances of potential terrorism planning behavior. One of these challenges is a lack of available data sources on suspicious activity, especially sources that are fairly comprehensive in terms of their coverage across jurisdictions. A second challenge is the lack of methods and tools for analyzing available data sources—such as 911 call for service (CFS) data— including approaches for processing, analyzing, and prioritizing large volumes of data. A third challenge that is specific to suspicious activity behavior is differentiating between potential cases of terrorism and innocuous behavior that was misinterpreted by citizens, officers, or security personnel.

ES.2 Study Objectives

This project developed and tested an analytic method for extracting useful information from suspicious behavior reports that were voluntarily given by concerned citizens using 911. To accomplish the study objectives, RTI International created a methodology for analyzing incidents of suspicious behavior—called Trinity Sight™—which was applied to CFS data from the Washington, D.C., Metropolitan Police Department (MPD).

The specific study objectives were as follows:

1. Apply data mining approaches to a commonly available data source in order to produce operationally relevant findings. Specifically, we sought to determine whether CFS data collected from a large metropolitan area with multiple potential terrorist targets could be explored and modeled in a manner that is applicable to counterterrorism activities.

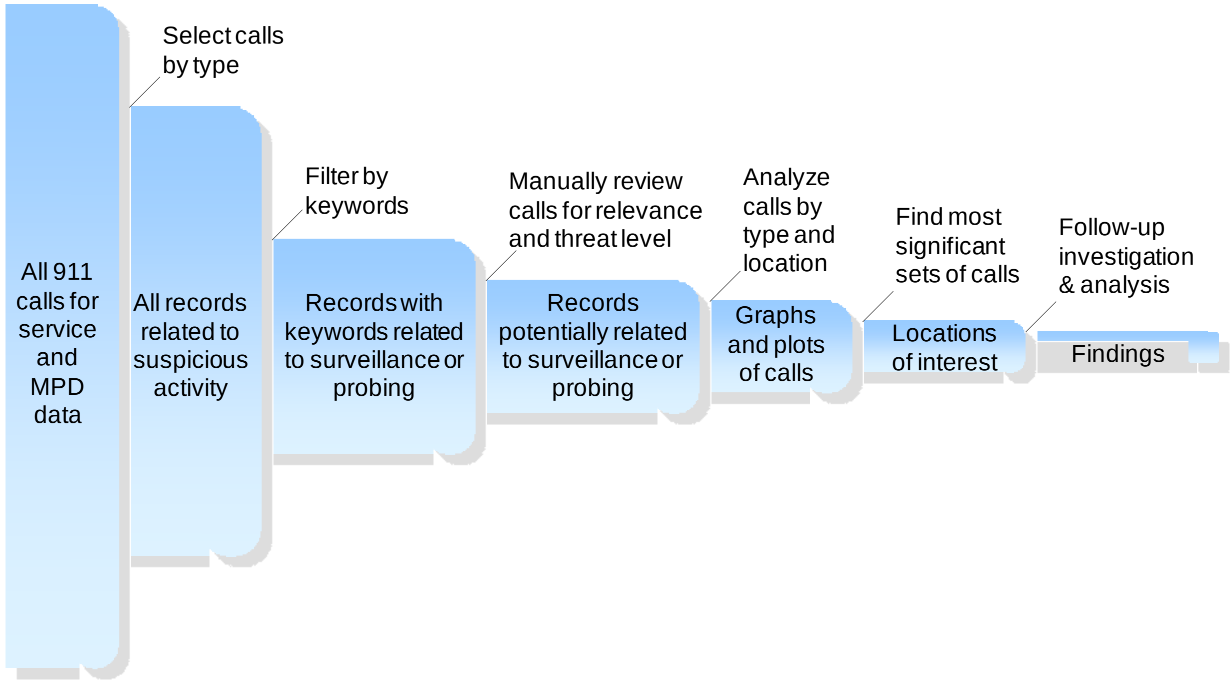
2. Develop and document an analytic process that identifies, analyzes, prioritizes, and visualizes suspicious activity data that law enforcement agencies or fusion centers can incorporate into their standard operating procedures. As a part of this analytic process, a threat classification system was developed that prioritizes specific cases based on time, location, and nature of the activity.

3. Identify successful processes that allow state and local agencies to integrate and analyze multiple data sources related to potential terrorist threats. Ultimately, the goal is to highlight the value of CFS data for homeland security purposes, including how to collect and analyze the information and how to visualize and disseminate relevant output.

ES.3 Methods

To accomplish these objectives, we analyzed more than 1.3 million 911 CFS records using data mining approaches and a threat classification system that identified and prioritized suspicious activity incidents that were potentially related to pre-attack activities. Figure ES-1 summarizes the complete process, beginning with all 911 calls received by the MPD from October 2005 through June 2007.

Figure ES-1. Process for Analyzing 911 CFS Records


All 911 calls for service and MPD data
Select calls by type
All records related to suspicious activity
Filter by keywords
Records with keywords related to surveillance or probing
Manually review calls for relevance and threat level
Records potentially related to surveillance or probing
Analyze calls by type and location
Graphs and plots of calls
Find most significant sets of calls
Locations of interest
Follow-up investigation & analysis
Findings

EOD = explosive ordnance demolition; MPD = Metropolitan Police Department.

We first extracted records based on classified call types that were most likely to contain incidents relevant to hostile surveillance, resulting in a population of about 100,000 records. These call types included suspicious person, suspicious vehicle, suspicious package (listed under multiple types), bomb threat, “investigate the trouble,” and “other” records.

We then examined a sample of these 100,000 records to look for keywords that might indicate an incident was potentially relevant to preoperational activities. Keywords related to conducting surveillance—video, photography, taking notes, and using binoculars—were closely associated with suspicious person and vehicle reports. For suspicious packages, keywords were related to cases in which an explosive ordnance demolition (EOD) team was called out or the police were called to close traffic in support of a response from a federal agency (e.g., Federal Bureau of Investigation [FBI], U.S. Secret

Service, Capitol Police). The keyword filters were applied to the 100,000 records, resulting in the selection of about 1,200 records for further review.

These 1,200 records were manually reviewed to remove duplicates and assess each record's relevance to hostile surveillance or probing. On manual review, about 350 records were duplicates, related to "ordinary" work, crime or tourism, or had comments declaring them to be "good intent" (such as a person returning to pick up forgotten luggage). About 850 potentially relevant records remained. These records included about 200 suspicious person and vehicle reports that were potentially related to pre-attack surveillance. The records also included about 350 suspicious package reports potentially related to conducting attack rehearsals or probing emergency response (i.e., generate an EOD team response or supported the FBI or Secret Service in closing off roads), about 75 markedly suspicious package reports that had genuinely suspicious attributes (e.g., white powder, odd or threatening messages), and about 200 bomb threats potentially related to providing a warning or probing emergency response.

We then evaluated the times, locations, and potential links between incidents to identify incident clusters warranting additional analysis. We used a combination of bar charts, trend charts, and geospatial plots to identify incident clusters. We also assessed the risk level of the incidents and clusters. Table ES-1 shows the framework used to rate the risk of potential surveillance calls, which assigns points along multiple dimensions: 0 to 3 points is considered low risk, 4 to 6 points is moderate risk, and 7 to 10 points is high risk. (We found no high-risk potential surveillance calls.) The framework was based initially on our experience with prior counterterrorism research and was modified after consultation with other RTI and MPD subject matter experts.

We similarly divided suspicious package calls into ordinary and "markedly suspicious" package calls based on call comments implying that they may have been left deliberately, contained odd or threatening messages, or looked like a bomb (note that we did not characterize bomb threat calls). We then searched the 911 records again for incidents possibly related to those in the identified clusters. Finally, we identified locations of interest and provided evidence for and against the proposition that those locations were probable terrorist targets.

ES.4 Results

The number of cases identified as potentially related to preoperational terrorist activities represented only a small proportion of all suspicious calls (less than 1,000 calls out of approximately 1.3 million). Notably, the approximate 200 potential surveillance calls differed from other suspicious person and vehicle calls by time of day and call location. We also identified multiple clusters around the city and were able to evaluate the risk level of these clusters.

ES.4.1 Characterization of Potential Surveillance Calls, by Time

These findings give the results of characterizing the potential surveillance calls by time, comparing the time block (e.g., 8 am to 12 pm) and day of the week between the 177 potentially hostile surveillance calls and all 14,000 suspicious person and vehicle calls. Calls that were potentially terrorist related were reported most frequently between 12 pm and 4 pm from a downtown location, while all suspicious person and vehicle calls were concentrated at night.

Table ES-1. Risk Rating Framework for Potential Surveillance Events

Dimension	Score	Description
1. Atypicality of reported activities	Unusual:1 point	Could be explained by ordinary work, tourism, or criminal behavior. Examples include photographing office buildings, lesser-known landmarks, and airplanes.
	Highly atypical: 2 points	Not readily explainable, especially if behavior is risky. Examples include photographing highways, railroads, and other public infrastructure.
	Threatening: 4 points	Matches known pre-attack signatures. Examples include using large numbers of cell phones (or discarding them), attempted trespassing, and asking probing questions.
2. Attractiveness of target	Attractive: 1 point	Well-known landmark (and hence well monitored) or opportunity for significant casualties. Examples include high-density office and residential buildings, well-known Washington, D.C., landmarks and Metrobus.
	Highly attractive and atypical: 2 points	Not normally photographed and could result in massive casualties or disruption to Washington, D.C. Examples include highway bridges and overpasses, chemical facilities, and Metrorail
3. Membership in a cluster	Moderate confidence: 1 point	Moderate confidence that the calls could be due to the same group of individuals because they are reasonably close in space, time, and descriptions.
	High confidence and atypicality: 2 points	Atypicality score of at least 2, and high confidence that the calls are due to the same individuals because they are very close in space, time, and description.
4. Presence of police report	Police report: 2 points	Call record includes a police report number.
Total	10 points maximum	

Figure ES-2 breaks down the calls by type of surveillance employed: photography, videography, taking notes, or using binoculars. If the call comment was unclear about whether photos or video were being taken, we assumed photography. The figure shows no significant changes between the types of surveillance employed.

ES.4.2 Characterization of Potential Surveillance Calls, by Location

Potential surveillance calls were concentrated in downtown areas, while suspicious person/vehicle calls were distributed throughout the city. We also characterized potential surveillance calls by the hybrid location listing, combining named locations, major types of locations, and geographic areas. As shown in Figure ES-3, a large proportion of calls concerned highways. Military locations were also named regularly, while other named locations included a power plant, a section of railroad, and hospitals.

Figure ES-2. Potential Surveillance Calls, by Month and Type of Surveillance

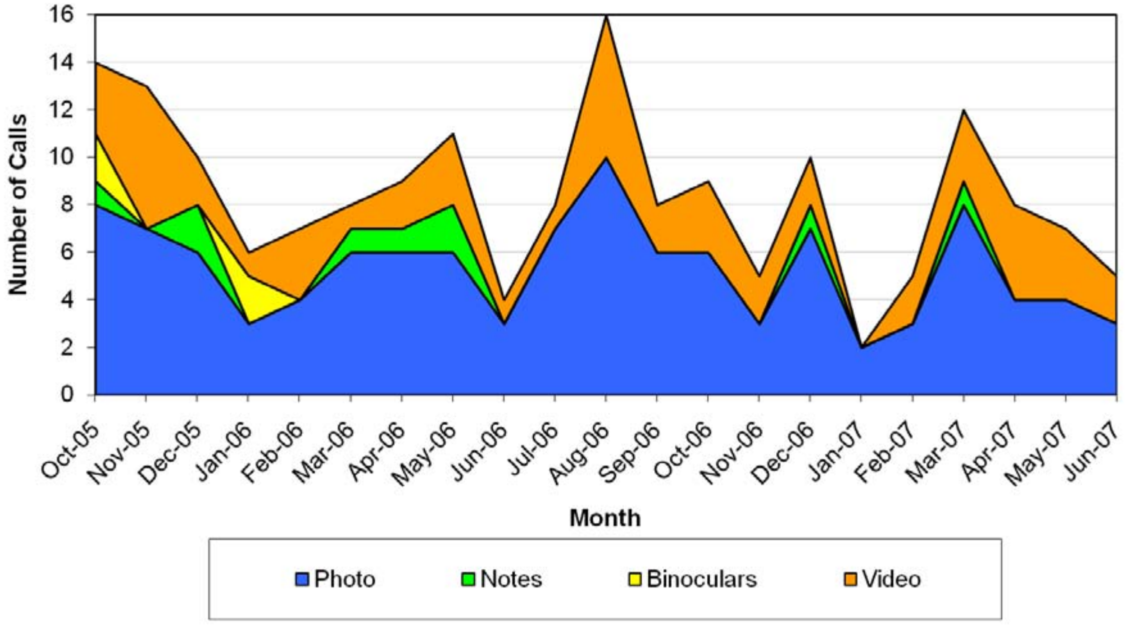
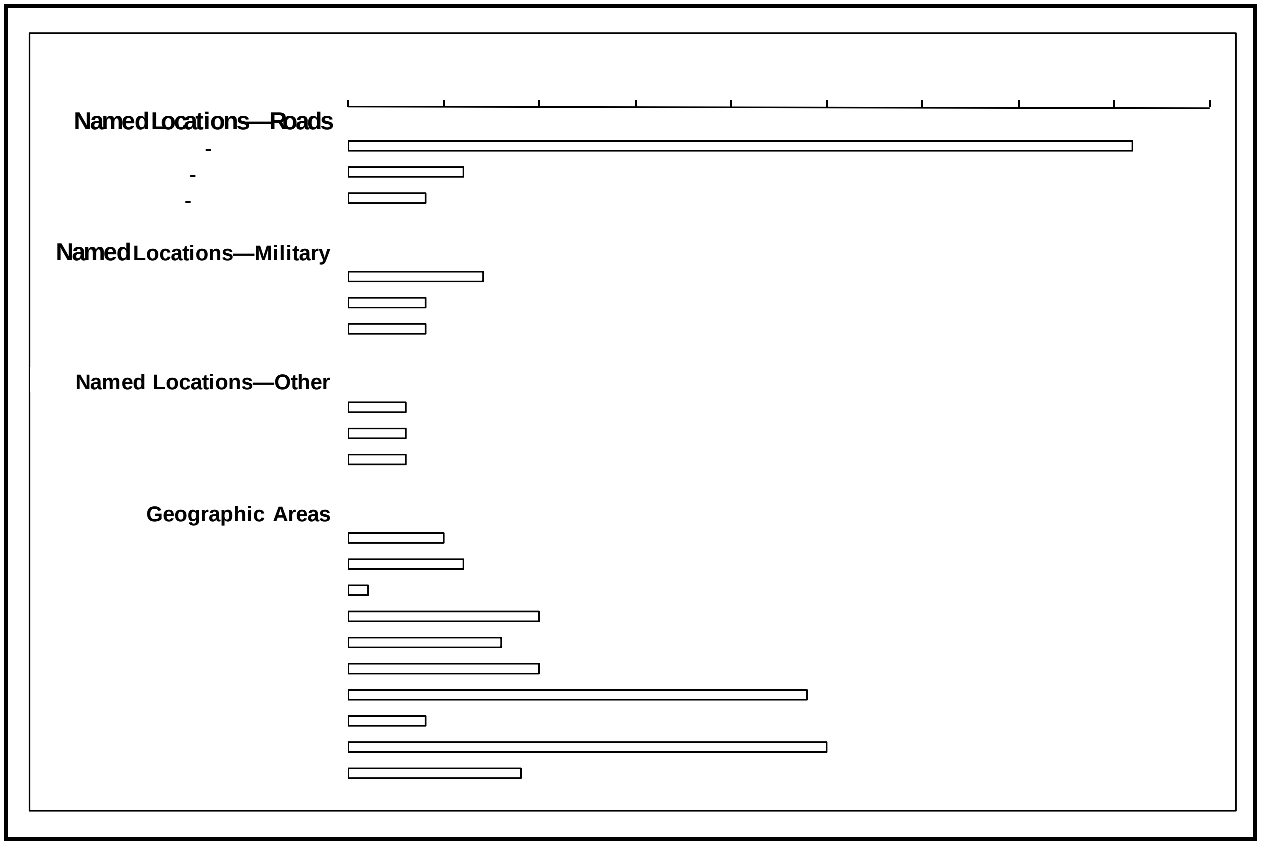


Figure ES-3. Potential Surveillance Calls, by Location



ES.4.3 Characterization of Potential Surveillance Calls, by Nature of Activity

Figure ES-4 shows the distribution of potential surveillance calls by risk assessment using the risk classification scale developed for the project. We found the following results:

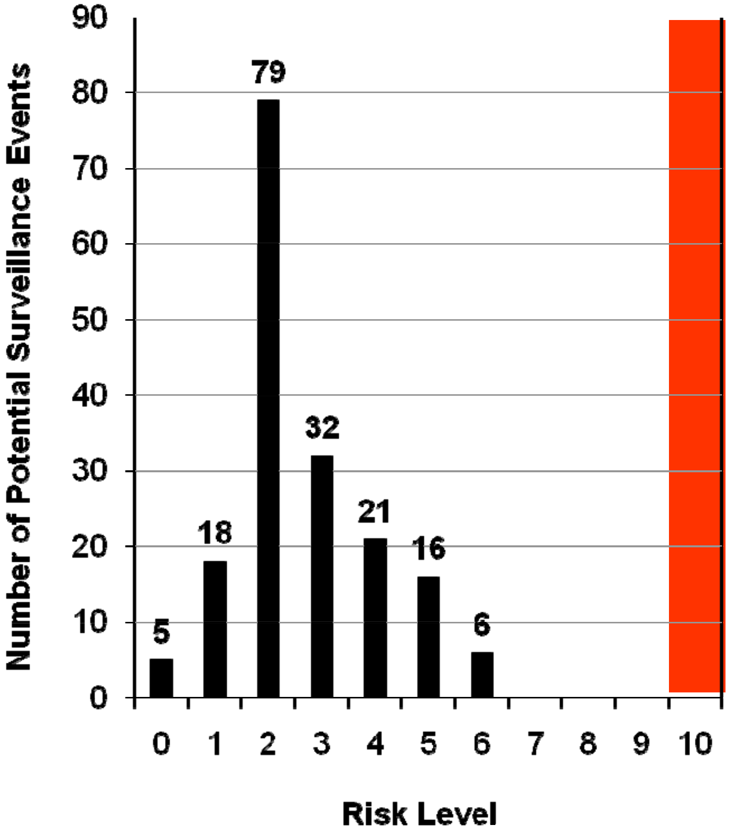
1. Six events scored 6. These calls were inconsistent with ordinary behavior, were for a highly attractive target, and were part of a high-likelihood cluster (i.e., strong possibility that all reports were of the same people) of similarly atypical observations.

2. Sixteen events scored 5. These calls had similar risk characteristics as those scoring a 6, but were part of a medium-likelihood cluster (i.e., much lower probability that the same people were responsible for all observations) or the target was not as attractive.

3. Twenty-one events scored 4. These calls were similar to those scoring a 5, but were not part of a cluster or the target was not highly attractive.

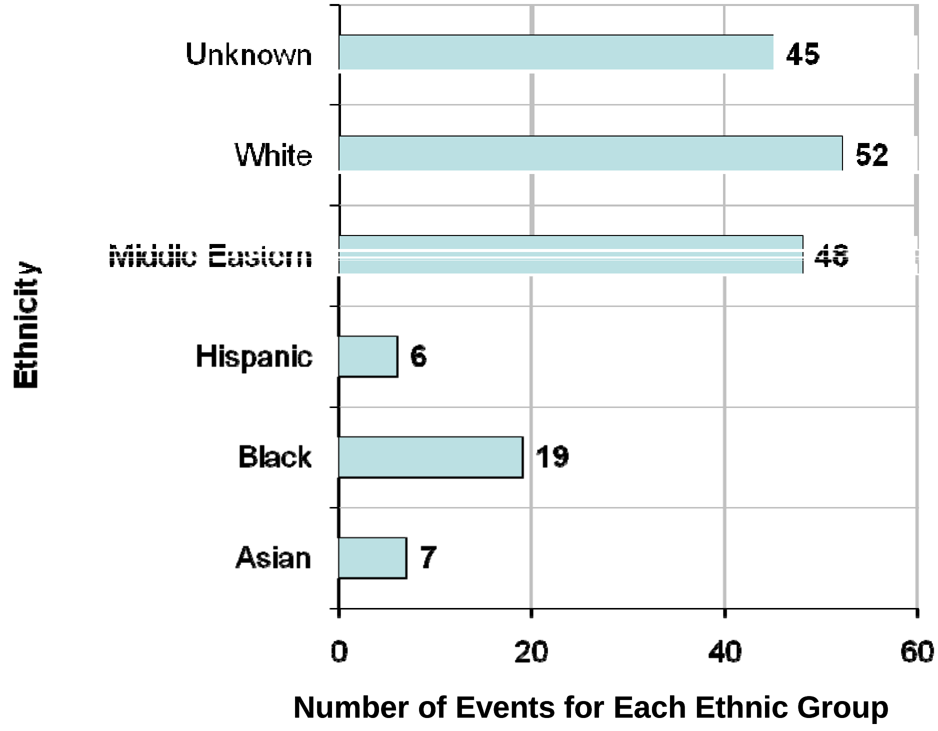
4. Finally, the remaining calls were rated as 3 or less. These are comparatively unlikely to represent actual preoperational surveillance.

Figure ES-4. Potential Surveillance Calls, by Risk



We also considered the reported ethnicities of the suspects, if available, to ensure that our analysis was not simply detecting large numbers of persons described as “Middle Eastern” engaged in what would otherwise be normal behavior, such as photographing landmarks. As shown in Figure ES-5, while the number of “Middle Eastern” persons was overrepresented, white persons were reported most frequently. We suspect that there is some over reporting of “Middle Eastern” persons because of callers’ biased suspicions.

Figure ES-5. Ethnicities of Persons Reported in Potential Surveillance Calls



ES.5 Locations of Interest

Based on the incident patterns, we identified 11 locations of interest. Four of these qualify as focus areas of most concern, as shown in Table ES-2. Within the table, the locations are listed in reverse order based on the number of incidents. The table provides arguments for and against the proposition that the locations are actually being targeted. The remaining seven locations of interest, which have fewer incidents and lower risk scores, are shown in Table ES-3.

Table ES-2. Locations of Greatest Concern

Location	Arguments For	Arguments Against
1. I-395: 14th Street Bridge and Maine Ave Overpass	• 32 incidents in all, 22 on bridge itself, 10 for Maine Street overpass area • 16 potential surveillance calls for taking pictures and filming in six clusters; some personal risk involved • Maine Street area has 6 potential surveillance calls that sweep area from multiple perspectives; not near landmarks or airplanes • Other notable calls: — Persons wearing black clothes and black skull caps in a bridge tower — People "working" on the bridge from rowboats; neither DC or Arlington knew of them — "Shackles" with a line hanging from underside of the bridge — Disruption to this area would have major consequences	• Stopped cars and people more likely to be noticed • Many calls could be tourism of airplanes and D.C. landmarks, especially on 14th Street Bridge
2. Union Station	• 26 incidents, 9 in 2007; mix of activity • Increased activity in recent months • Only instance of linked suspicious packages (2x Union Station, 1x Fairchild Building, 12/8/2006)	• Over half are for suspicious packages - natural location to leave luggage • Some bomb threats appear to be crank calls
3. Washington Hospital Center	• 6 total; includes markedly suspicious package addressed to "Department of Justice" (Apr 07), followed by bomb threat (Jun 07) • Seen increased activity for hospitals	• Not clear if incidents have pre-operational value
4. Mayflower Hotel	• 4 incidents, including a markedly suspicious package and a person taping the hotel (including the loading dock) in May • Seen increased activity for hospitals	• Incidents do not appear directly related

Table ES-3. Other Locations of Interest

Location	Arguments For	Arguments Against
5: I-395 northern exits	• 29 calls for northern tunnels and related on-ramps–16 potential surveillance, 13 suspicious package • 5 seemingly related calls of a man taking pictures of traffic at various exits, one potentially related call of a man with bags "messing with something" in the 3rd Street Tunnel	• Stopped cars and people more likely to be noticed • Many packages could be trash or fallen luggage • Incidentals from cluster are old – last was March 2006
6: Bolling AFB/Naval Station	• 14 potential surveillance calls in this area, most from people on I-295 taking pictures towards the military facilities	• Stopped cars and people more likely to be noticed on highways • Uncertainty in what was actually being surveyed
7. Venable LLP	• 7 bomb threat calls	• Bomb threats have limited pre-operational value
8. DC Public Safety Service Center	• 4 bomb threat calls	• Bomb threats have limited pre-operational value
9. Sibley Memorial Hospital	• 3 potential surveillance calls: 2 in one cluster involving chemical plant	• Surveillance activity not repeated recently
10. AT Afribank	• 2 markedly suspicious packages, one involving white powder, one leaking oil	• Incidents do not appear directly related
11. DC Public Health Commission	• 2 markedly suspicious packages, one involving brown powder, one a pipe with wires wrapped around it	• Incidents do not appear directly related
12. Iraq Chancery	• Molotov cocktail–only weapon found • Natural target due to war	• Only one incident

ES.6 Conclusions

This project developed and tested an analytic process for utilizing CFS data to identify potential terrorist threats. CFS data are comprehensive in terms of their inclusion of both minor and major forms of behavior and are commonly available, which means that jurisdictions do not have to spend scarce resources on "new" systems to track suspicious behavior. Furthermore, the techniques used to analyze the 911 call data were straightforward, and complex analyses and software tools were not needed to develop standards for collecting and analyzing information on suspicious activity reports.

Based on this study, there are several recommendations that law enforcement agencies can adopt to improve their capacity for collecting and analyzing suspicious activity data:

1. Law enforcement agencies should ensure that all necessary information related to all suspicious activity is collected electronically at the local level. Of particular interest is the final call disposition; that is, whether a call did or did not end up being suspicious and why. This information can assist in better classifying future incidents because it can help differentiate between incidents.

2. Key data elements need to be present to extract and process call data (e.g., date and time of call, location of incident, nature of incident). The second set of data elements includes whether the record is (1) new, (2) previously in the main database but not previously extracted, (3) previously reviewed but discarded, or (4) reviewed and found to be relevant for

counterterrorism purposes. This field supports comparing previously analyzed records with new call records.

3. While comprehensive automation of the CFS analysis process is a subject for future research, there are some comparatively simple tasks that could be automated using Visual Basic programming in Microsoft Access and Excel, including providing analysts with simple window inputs for filtering, querying and sorting, reviewing, and analyzing data.

This project has demonstrated that CFS data can be a useful source for counterterrorism planning. The techniques used for “filtering out the noise” of the 911 CFS data were straightforward and did not require complex analyses or software tools. Ultimately, these processes will allow local law enforcement agencies to (1) integrate previously underutilized data into existing analytic practices, (2) identify potential signs of terrorist pre-planning activity in specific jurisdictions, and (3) identify operationally relevant information to support follow-up investigations. Appendix C presents a guide for jurisdictions interested in implementing the architecture in the short term; more broadly, Appendix D presents a summary of how the process developed in this project might fit into a larger data fusion architecture.

Analyzing these data can produce results that were previously unknown, or they can reinforce and illuminate existing counterterrorism activities. For instances where the information was not known previously, the data can serve as a trigger to collect more detailed data to verify whether actual terrorist activity was taking place. For situations where the results confirm or negate existing beliefs about assets most threatened by a potential terrorist attack, adjustments can be made to counterterrorism strategies. Findings can also be used to establish a baseline level of suspicious activity in jurisdictions. Future research should test the methods used in this study in other jurisdictions to continue to refine and improve the developed process. Such research should include jurisdictions with different characteristics and vulnerabilities than Washington, D.C.

1

Introduction

1.1 Overview

Case reviews of the Africa Embassy bombings, the September 11 attacks, and the London and Madrid transportation bombings have revealed that terrorist groups engage in extensive, long-term target surveillance (The 9/11 Commission Report, 2004). For example, the suspects in the London 2005 bombings carried out a “dry run” on the subway system several weeks before the attacks. Terrorist preoperational surveillance was also reported among key financial institutions in New York City, New Jersey, and Washington, D.C., which prompted the Department of Homeland Security (DHS) to raise the terrorist threat level (CNN, 2004). In 2007, authorities thwarted a terrorist plot in Germany, when individuals were caught conducting surveillance of U.S. military facilities near Hanau (Eddy, 2007).

Local law enforcement agencies are well equipped to detect and report suspicious activity related to terrorism pre-planning, such as the systematic observation of potential terrorist targets. Municipal and county police officers, in addition to outnumbering their federal and state counterparts, have an intimate knowledge of what constitutes “normal” behavior in their communities. However, despite recommendations that local law enforcement officers shift from “first responders” to “first preventers,” these agencies have been given limited guidance on what their role should be in detecting and preventing potential terrorist attacks (Kelling & Bratton, 2006).

Analyzing and characterizing suspicious activity data may give law enforcement and security professionals the ability to anticipate, prevent, deter, and respond in a more effective manner to terrorist and other criminal threats. Analyzing suspicious behavior reports can also identify specific areas within jurisdictions that are at risk because of elevated preoperational planning and can also highlight previously undetected vulnerabilities in either the physical or operational security of a particular location. The improved collection and analysis of suspicious activity data can be used to establish baselines of hostile surveillance in a given jurisdiction and to prioritize incidents worthy of closer inspection and follow-up. Unfortunately, it has historically only been after an incident occurs that a larger pattern of hostile surveillance has been identified and characterized.

There are several key challenges that affect the reporting and analysis of suspicious activity data. One, suspicious actions suggestive of preoperational planning are infrequent and are intended to appear innocuous to uninformed observers. Trying to identify suspicious behavior indicative of something far more sinister often resembles looking for the proverbial needle in the haystack. Two, behaviors can be misinterpreted by citizens, officers, or security personnel reporting the behavior, resulting in an unknown number of false-positive reports. Three, there has been little guidance on how to collect, analyze, and disseminate operationally relevant information from existing data sources.

One promising information source on terrorist pre-planning activity is suspicious behaviors reported by citizens using 911 calls for service (CFS). CFS data files typically contain large volumes of data and have limited information on the incident and any follow-up by officers on the scene. These calls can reflect a wide range of behaviors, including activities related to illegal drug activity; criminal casings of people, places, or things; and loitering. Yet, data mining has been used successfully in the public safety and security arena to support the development of effective prevention and response strategies. Data mining tools have been used successfully on a smaller scale in characterizing and modeling suspicious activity reported in relation to a single facility in Richmond, Virginia, known to be of interest to terrorists (McCue, 2005).

For the current National Institute of Justice (NIJ)-funded project, RTI partnered with the Washington, D.C., Metropolitan Police Department (MPD) to examine the feasibility of using a new analytic process involving 911 CFS data to generate useful information on suspicious activity. The MPD receives approximately half a million CFS annually, which include an estimated 40,000 reports of unusual or suspicious behavior—reports that are not currently analyzed in a complete or systematic fashion. This study sought to determine whether a complex set of suspicious activity reports could be explored and modeled to make recommendations for terrorism prevention and deterrence efforts. The project is intended to create a proof of concept, so the methodology developed will need to be validated and tested in other localities in future projects. The ability to scale this work to include a larger number of observations and greater automation offers the promise of using 911 CFS records as an additional data source for identifying potential risks associated with the terrorist attack pre-planning process. The failure to integrate 911 CFS data into a larger, more strategic approach to information-led policing could result in missed information and lost opportunities for intervention and prevention. This is especially true for those 911 calls that do not result in a formal police incident report.

1.2 Project Objectives

This study analyzed CFS data from a 2-year period in Washington, D.C., to determine the usefulness of these data in identifying potential patterns in terrorist hostile surveillance, including the processes that terrorists engage in during pre-planning attack phases. As part of the project, we developed and tested a process for identifying, extracting, and analyzing incidents that we defined as potentially indicative of hostile surveillance activity. In particular, the study sought to determine whether an analytic process used to analyze behaviors around a single financial entity in Virginia could be applied successfully to suspicious activity across an entire metropolitan area.

The specific objectives of this study were as follows:

1. Apply basic data mining approaches to a commonly available data source in order to produce operationally relevant findings. Specifically, we sought to determine whether CFS data collected from a large metropolitan area with multiple potential terrorist targets could feasibly be explored and modeled in a manner that would generate findings directly applicable to terrorism detection and prevention activities.

2. Develop and document an analytic process for identifying, analyzing, prioritizing, and visualizing suspicious activity data that can be incorporated into standard operating

procedures within law enforcement agencies or fusion centers, including creating a threat classification system that allows selected cases to be prioritized depending on location, time, and nature of the activity.

3. Identify successful processes and activities that state and local agencies can use to integrate and analyze data sources on potential terrorist threats. Ultimately, the goal is to highlight the value of CFS data for homeland security purposes, including how the information should be collected and analyzed and how relevant output should be visualized and disseminated.

1.3 Organization of the Report

This report is divided into seven major sections. Section 1 includes a brief literature review of issues related to hostile terrorist surveillance and the data sources commonly used to describe suspicious activity. Section 2 provides an overview of Trinity Sight™, the law enforcement–specific analytic process used to process and analyze public safety data. Section 2 provides an overview of Trinity Sight™, the law enforcement–specific analytic process used to process and analyze public safety data. Section 3 describes our analysis of 911 CFS data to identify incidents potentially related to preoperational surveillance, such as taking photos or video of target locations. Section 4 expands our analysis to identify multiple types of incidents potentially related to preoperational surveillance and probing, including leaving suspicious packages and making bomb threats to see when and how authorities respond. Section 5 identifies locations of interest that have seen clusters of suspicious incidents, and assesses the risk to these locations. Finally, Section 6 discusses the study’s implications, limitations, and potential applications for future research and policy.

Appendix A presents the complete set of 911 variables used in the analysis. Appendix B presents a description of additional analyses outside the main methodology, which combined 911 CFS data with additional 2007 incident data on suspicious packages. Appendix C provides an implementation guide for jurisdictions interested in using the methodology in the short term. Finally, Appendix D presents a data fusion architecture for homeland security and discusses how the methodology in this paper fits into the architecture.

1.4 Literature Review

1.4.1 Terrorist Attack Planning Cycle and Opportunities for Detection

In order to effectively plan for an attack, terrorists must conduct target selection and operational planning activities on multiple occasions. These activities are designed to blend in with normal, everyday activities and are often difficult to spot. However, the more often the terrorists conduct their malevolent activities, the greater the chance they will reveal their true intentions and be detected by authorities. By exploiting this vulnerability in the first two phases of the attack planning cycle, it is therefore possible to identify attacks before they reach fruition.

While terrorist attacks seem to occur without warning, significant pre-planning often precedes these incidents, and this pre-planning is a critical phase in the terrorist attack planning cycle. This cycle has been identified as having six distinct phases, including target selection, planning, deployment, attack, escape, and exploitation. Of these six phases, the target selection and planning phases represent the best opportunities for law enforcement and homeland security officials to conduct counter surveillance and stop an attack before it is carried out. The target selection and planning phases are the best opportunities for prevention because, in these two phases, terrorists engage in activities and behaviors that place them at the greatest risk for detection (STRATFOR, 2005b).

The target selection and planning phases together are commonly referred to as preoperational surveillance. In addition to these phases presenting the best opportunity for detection by law enforcement and counterterrorism officials, they are also the most important phases, from the terrorist's perspective, for achieving a successful attack. This hypothesis is borne out by training materials recovered from al-Qaeda operatives that underscore the importance the terrorist organization places on these preoperational activities. These training manuals emphasize gathering intelligence—using both open and covert measures—regarding a target's physical characteristics, general surroundings, security procedures, and important persons (DHS/Federal Bureau of Investigation [FBI] bulletin, 2005).

The difficulty in detecting actual terrorist preoperational surveillance lies in the fact that there are numerous behaviors that could be terrorist related, but in reality are not. For example, in addition to terrorists, perpetrators of traditional crime also conduct preoperational surveillance. Added in with these two groups are average citizens, whose behaviors (e.g., a tourist filming a landmark) may appear to be hostile. This results in a lot of "noise" associated with potential incidents of preoperational surveillance, thereby making it difficult to identify specific cases involving possible terrorist attacks.

During the target selection phase, several potential targets may be under surveillance by terrorists while they attempt to identify the one target that best fits the planned attack. Variables of interest that are monitored during this phase can include security procedures and access requirements, as well as the potential value of the target to the overall goals or objectives of the terrorist organization. For example, al-Qaeda has traditionally chosen targets that are either symbolic in nature (e.g., the Pentagon) or that will cause death and injury on a large scale (e.g., the Madrid train bombing) (STRATFOR, 2005a). Surveillance activities during this phase will be predominantly static, meaning that the terrorists will not likely initiate contact with the intended target; these static activities can include videotaping a facility or taking notes regarding behavior patterns of security personnel.

Terrorists use a variety of information sources when selecting a target. One source that is emphasized in terrorist training materials is open source information (OSI), particularly information available on the Internet. Information gleaned from this resource can include names and photographs of important persons (e.g., government officials, security leaders), the target's present and future capabilities, and crisis management plans. The value of OSI should not be underestimated, as terrorists themselves estimate that as much as 80% of the information needed regarding a target can be obtained from publicly available sources (al-Qaeda, n.d.).

After a target has been selected, operational planning begins in earnest, although the amount of time devoted to this phase prior to the actual attack varies greatly depending on the size of the attack and the vigilance of the terrorist operatives. During the operational planning phase, the terrorist continues to survey the potential target in order to develop the tactics and strategy for the planned attack; eventually, these activities will move from static to active. Terrorists may use a range of surveillance activities, including static photography; video; and active physical probing of the perimeter, security features, and security personnel. This operational planning phase may also include a dry run of the attack. For example, in reviewing earlier surveillance footage, authorities found that the London transportation bombers had made a practice run less than 2 weeks before the attack was carried out.

Since September 11, there have been numerous incidents of preoperational surveillance, some of which are more characteristic of true attack planning than others. One specific example involved the ferry system in Washington State. FBI officials examined 157 suspicious incident reports that occurred near or on ferries and concluded that 19 of the incidents were likely terrorist preoperational surveillance. Included in these 19 incidents were cases in which individuals asked probing questions about ferry operations or took pictures and videos of the ferry stairwells, car decks, and ferry workers. One of the individuals involved was a known subject of an ongoing FBI investigation (Carter, 2004).

1.4.2 Terrorist Incidents in the United States

Activity by potential terrorists known as "hostile surveillance" includes a systematic review of a potential target or targets and can support target selection, as well as the development of specific tactics and strategy during the attack-planning process. Hostile surveillance generally is intended to be covert or to appear relatively innocuous to uninformed observers. Unfortunately, it has historically only been after an incident occurs that a larger pattern of ongoing suspicious behavior or presumptive hostile surveillance activity can be identified, compiled, and characterized, so that the true nature of the activity is revealed.

Review of the Africa Embassy bombings, the September 11 attacks (The 9/11 Commission Report, 2004), and the London and Madrid transportation bombings revealed extensive, long-term surveillance of the targets, including a "dry run" in London several weeks before the attacks. Prior to the attack on the school in Belsan, the terrorists had collected information on this and related facilities in support of target selection, as well as preparation of the operational plan, tactics, and strategy—information gathering that included preoperational surveillance of the school (The 9/11 Commission Report, 2004). Hostile surveillance in support of target selection and attack planning is not confined to Muslim extremists or international terrorists. The Animal Liberation Front (ALF), and the Earth Liberation Front (ELF), so-called "special interest" domestic terrorist groups, also rely on hostile surveillance in support of intelligence gathering and operational planning (Testimony of James F. Jarboe, 2002), as do other predatory criminals. The recovery of detailed, operationally relevant reports on financial institutions within the United States suggests ongoing, hostile surveillance of our critical infrastructure (Joint DHS and FBI Advisory, 2004).

In the U.S., there have been a limited number of studies on terrorist incidents, including the preparation and planning cycles associated with both successful and unsuccessful terrorist attacks, such as the American Terrorism Study (Smith & Damphousse, 1999; Smith, Damphousse, & Roberts, 2006). These studies have relied on federal court records and OSI to construct statistical databases from which inferences are then drawn. In these studies, terrorist groups are generally broken up into four categories: left-wing, right-wing, international, and single issue. Findings from these studies have shown a general trend toward smaller groups, more individual indictments, and a smaller number of large conspiracy cases, which points to a model of terrorism that has been called "uncoordinated violence" (Barkun, 1997).

These studies also found that terrorists engage in much more preparatory activities, including crime, prior to a terrorist attack (Smith & Damphousse, 1999).

Smith, Damphousse, and Roberts (2006) investigated pre-incident indicators of terrorist incidents by selecting a mix of right-wing, left-wing, international, and single issue cases from the American Terrorism Study database, and geospatial information was coded on terrorists' residences, planning locations and activities, and target locations. Findings showed that the planning cycle began about 2 to 3 months prior to committing an attack, with a pause in planning activities 3 to 4 weeks before the attack. The analysis also showed that terrorists generally live and conduct planning activities very close to their selected target, with about half residing within 30 miles of the target. This tendency to "act locally" indicates that law enforcement can be proactive by monitoring high-risk areas. The study also found that terrorists conducted crimes as a part of the planning process, including creating false identities and stealing (either to obtain money or explosive materials and weapons). These particular crimes could be taken into account when trying to isolate potential terrorist activity from all other behavior (Smith, Damphousse, & Roberts, 2006).

1.4.3 Applying Intelligence Models to Counterterrorism

Taking raw data and refining it into intelligence that can be used by policy makers follows a standard process. Both the Central Intelligence Agency (CIA) and FBI intelligence models have five basic steps: (1) planning/requirements, (2) collection, (3) processing and exploitation, (4) analysis and production, and (5) dissemination. The planning/requirements phase begins the cycle as intelligence needs are laid out by policy makers (e.g., president, director of national intelligence) and information sources related to these needs are identified. Various methods of gathering data are used during the collection phase, including HUMINT (human intelligence), SIGINT (signals intelligence), and OSINT (open source intelligence). This collection process yields a vast amount of data that must be transformed and reduced to be useful to analysts, and this transformation and reduction is completed during the processing and exploitation phase; analysts using 911 CFS data face a similar challenge. Intelligence is actually created during the analysis and production phase. During this phase, the available information is evaluated for its reliability, validity, and relevance. The final stage, dissemination, returns the intelligence to the policy makers who requested it in a standard reporting format (e.g., daily threat assessments).

However, intelligence failures with regard to September 11 and Iraq weapons of mass destruction (WMD) claims have led to criticism from both within and outside the intelligence community. One of these criticisms is that the model described above is outdated for the current threats facing the United States. The intelligence community has been criticized as a top-down institution that does not fit well in the current information age, where businesses are networked and flattened to handle rapidly changing environments (Russell, 2004; Bureau of Justice Assistance [BJA], 2005). Medina (2002) argues that the current intelligence model is based on an information scarcity approach that was appropriate for the 1960s and 1970s, when obtaining information on world events was much more difficult given the larger number of closed societies. This paradigm made it necessary for intelligence agencies to provide information to policy makers that they could otherwise not obtain. By default, this model is reactive and requires new developments to occur for the intelligence process to begin. In today's information-abundant society, with its ever-expanding communication technology, policy makers are often aware of these events before the intelligence community provides the information to them. This new paradigm means that the intelligence community must begin to focus on providing ideas, and not just intelligence, to policy makers.

1.4.4 Applying Intelligence-Led Policing to Counterterrorism

Intelligence-led policing (also called "information-led policing") is a "…collaborative enterprise based on improved intelligence operations and community-oriented policing and problem-solving" (BJA, 2005). Information-led policing focuses on identifying, analyzing, and managing persistent and emerging problems by better using intelligence and information sharing to develop effective solutions (Maguire, 2000). Information-led policing gained notoriety during the mid-90s with the creation of CompStat by the New York Police Department (Walsh, 2001).

Information-led policing approaches can be used for both tactical and strategic purposes. Tactically, information-led policing supports investigations and crime prevention on a day-to-day basis. Strategically, information-led strategies can help develop long-term solutions to problems being addressed on a tactical level (Peterson, 1997). For example, information-led strategies could tactically be used to investigate an open-air drug market and then strategically be used to develop a plan for systematically disrupting the market.

Following the September 11 attacks, law enforcement agencies were given new responsibility with respect to preventing and responding to terrorism. While some have argued that this additional responsibility hampers law enforcement's ability to combat traditional policing problems, others have noted that the intelligence-led policing model is well suited to terrorism prevention. Particularly, local law enforcement is in the best position to notice activity within its patrol area that is not normal. Combining their knowledge with other strategies, such as public-private partnerships and cooperation with community members, puts law enforcement in a good position to identify and investigate potential terrorist activity.

To leverage the knowledge of both local jurisdictions and federal agencies, the federal government has emphasized the establishment of a network of fusion centers to collect, analyze, disseminate, and use homeland security–related information. DHS created a specific framework for local governments to request fusion center funding in fiscal year 2007 (DHS, 2007). The Congressional Research Service's 2007 report on state, local, and regional information fusion centers noted that over 40 had been established since the September 11 terrorist attacks. However, the same report also noted that,

> while many of the centers have attacks as a high priority, little "true fusion," or analysis of disparate data sources, identification of intelligence gaps, and pro-active collection of intelligence against those gaps which could contribute to prevention is occurring. (Masse, O'Neil, & Rollins, 2007)

Little detail has been written about how to conduct fusion, including in official guidelines. The Department of Justice (DOJ) and DHS Fusion Center Guidelines says little beyond defining data fusion as "turning information and intelligence into actionable knowledge" and that data fusion refers to "the overarching process of managing the flow of information and intelligence across levels and sectors of government" (DOJ & DHS, 2005). Similarly, DOJ has recently released a document ("Analyst's

Toolbox") listing software tools and databases deemed useful in a survey of law enforcement analysts (DOJ, 2006); however, the document does not describe specific methodologies for using the tools.

1.4.5 Citizen Reporting of Suspicious Events: Exploiting Call for Service Data

Humans seem uniquely suited to notice unusual actions, incidents, and behavior. It is not unusual to interview a witness after a major event and have the person recount unreported suspicious behavior that indicated something bad was about to happen. In fact, De Becker (1997) recounted cases of workplace violence where the event was so anticipated that as soon as the shooting started people made comments that correctly identified the suspect before the actual nature of the event was even known. Citizens are frequently in a good position to observe and report the suspicious or unusual behavior that may be associated with hostile surveillance because they have the best sense of what is "normal" in their community. The value of this so-called "natural surveillance" has not been lost on many law enforcement and security organizations that encourage citizens to report unusual or suspicious behavior (De Becker, 1997).

For example, in 2006, London's Metropolitan Police Department initiated public hearings to engage community support for terrorism prevention, noting that public ownership and solutions to the problem of terrorism will enable better community intelligence and trust and, in turn, reduce the chance of terrorist attacks. Similarly, in 2005, the Boston Police Department announced that it was restarting a neighborhood watch and community-policing program, which trains individuals in the community on the type of suspicious behavior indicative of terrorism. Boston Police Commissioner Kathleen O'Toole noted that "…it won't be an intelligence czar in Washington who notices something peculiar happening in Boston." The important takeaway from this program is that it increases the number of trained observers, as opposed to simply creating more observers, thereby increasing the likelihood that law enforcement will receive good intelligence.

In the rush to establish specific systems for collecting and disseminating information on terrorism, it has often been overlooked that every community in the United States has an existing mechanism, CFS systems, that can be used to report suspicious behavior. Ultimately, CFS data are useful in addressing a variety of crime problems; unfortunately, these data are often underutilized and not analyzed in such a way as to inform police tactics and operations. Existing CFS systems provide a unique opportunity to harness existing infrastructure in the cause of identifying and preventing terrorism. These systems provide a pulse for a community's criminal activity, which includes citizens' reports of activity that they perceive to be outside of what they consider "normal." Undoubtedly, some of these reports could be related to terrorist activity and may provide insight that would inform counterterrorism operations. Furthermore, because the data are citizen generated rather than department driven, they could be used as independent assessment measures of other terrorism indicators that local law enforcement may use (e.g., specific operations, informants).

Police departments have analyzed their CFS data to improve operational efficiency by identifying frequent types of calls (e.g., 911 hang-ups, alarm calls) and calls that used a disproportionate amount of resources (e.g., traffic accidents).CFS data have also been used by law enforcement and researchers in "hot spot" determination and social disorder measurement. All of these examples use data-driven approaches to address crime problems without having to expend additional resources to gather data. For example, Warner and Pierce (1993) used CFS data related to 60 Boston neighborhoods to determine what social factors contributed to high rates of assault, robbery, and burglary. Sherman and Weisburd (1995) used CFS data to determine the effect increased patrol presence has on crime “hot spots.” More recently, the Akron, Ohio, Police Department analyzed its CFS data to improve operational efficiency by identifying frequent types of calls (e.g., convenience store robberies where no charges would be pressed) and calls that used a disproportionate amount of resources (e.g., traffic accidents).

While advanced data analysis using CFS data is limited due to legacy systems (Pendleton, 2006), recent advances in information technology have created new potential for these systems. For example, the city of Chicago records both the original call and the audio communication between dispatch and officers in the field, which is then indexed for searching. The recorded audio is often used to support legal cases such as domestic violence calls, where the abuse in question may be captured on the audio (Goldfayn, 2007). In Baltimore, a program called Operation Care identified 91 people who were responsible for more than 2,000 911 calls in 2007, largely for ongoing health problems (Kohn, 2008). To limit the burden on emergency services, the program will attempt to get these individuals health insurance and connect them with other services that officials hope can improve their long-term health.

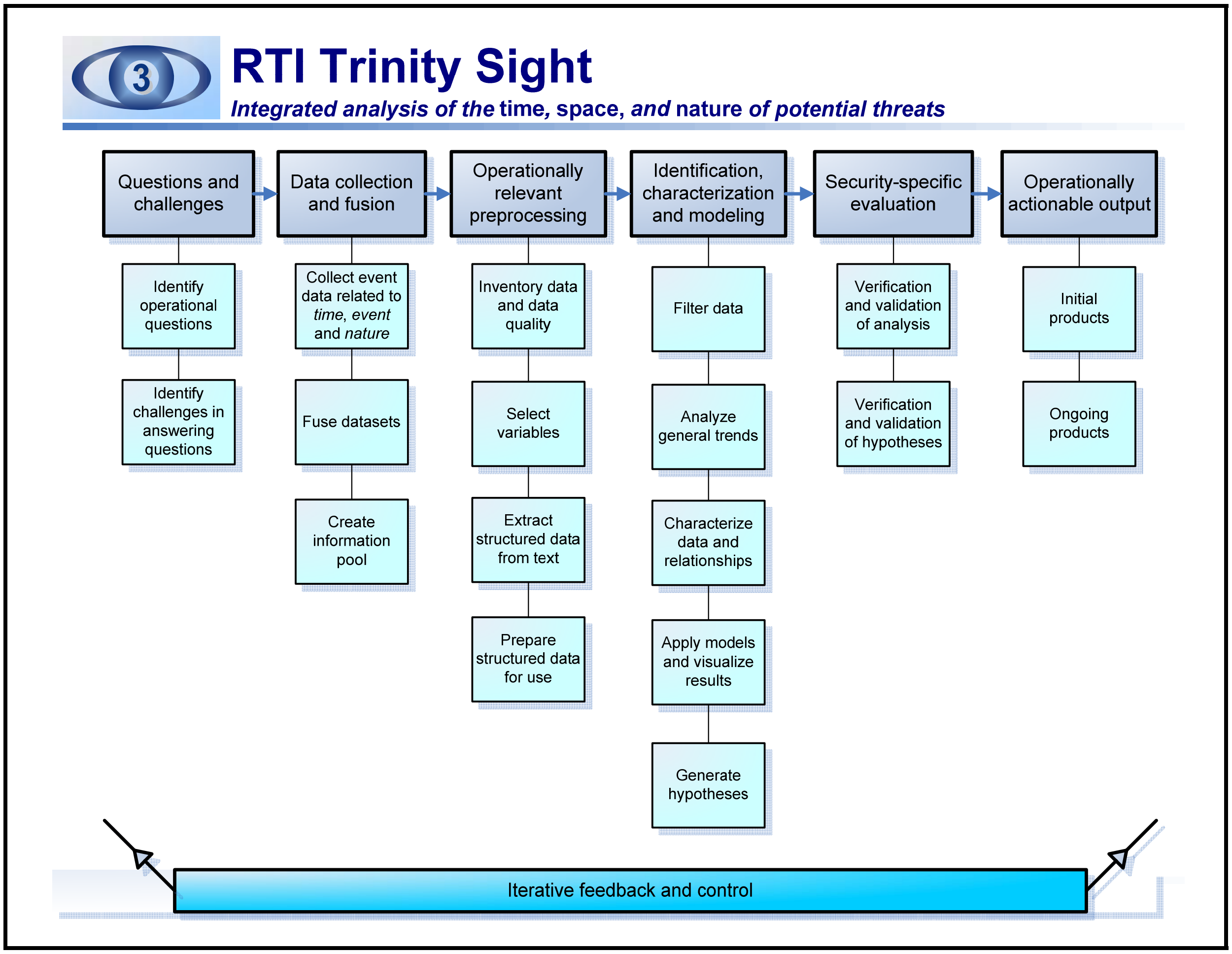
In this project, we partnered with MPD to develop and test an analytic method for extracting useful information from 911 calls, focusing specifically on suspicious behavior reports reported by citizens. As a part of this process, a threat classification system was developed that prioritizes specific cases based on time, location, and nature of the activity. Ultimately, the objective of this project is to develop an analytic process by which law enforcement agencies or fusion centers can routinely identify, analyze, and prioritize suspicious activity reports using 911 data. The following sections detail the development and use of this methodology.

2

The RTI Trinity Sight™ Analysis Methodology

RTI has developed a methodology, RTI Trinity Sight™, to analyze events for counterterrorism and crime prevention purposes. In this project, we applied Trinity Sight™ to analyze 911 CFS data. The focus of Trinity Sight™ is characterizing the time, space, and nature of suspicious incidents and using the results to identify clusters of incidents worth further investigation. Figure 2-1 diagrams the major elements of the Trinity Sight™ process, which is divided into phases and subsidiary tasks. For the sake of simplicity, the process is shown in a linear fashion; in practice, there are potential feedback loops between most tasks. For example, for this project, discussion of analysis results led to additional research questions and processing of additional data sets. Each phase—and how it was applied to this project—is described below.

Figure 2-1. The RTI Trinity Sight™ Methodology


RTI Trinity Sight
Integrated analysis of the time, space, and nature of potential threats
Questions and challenges
Identify operational questions
Identify challenges in answering questions
Data collection and fusion
Collect event data related to time, event and nature
Fuse datasets
Create information pool
Operationally relevant preprocessing
Inventory data and data quality
Select variables
Extract structured data from text
Prepare structured data for use
Identification, characterization and modeling
Filter data
Analyze general trends
Characterize data and relationships
Apply models and visualize results
Generate hypotheses
Security-specific evaluation
Verification and validation of analysis
Verification and validation of hypotheses
Operationally actionable output
Initial products
Ongoing products
Iterative feedback and control

Trinity Sight™ was introduced in McCue (2006) and was built on top of the generic analysis methodology Actionable Mining and Predictive Analysis for Public Safety and Security (AMPA-PSS) (also in McCue [2006]), which fused the CIA Intelligence Process (Air War College, 2007) and Cross-Industry Standard Process for Data Mining (CRISP-DM) (Chapman et al., 1994). The updated version of Trinity Sight™ used for this project has been augmented with key features from the RAND Corporation's Atypical Signal Analysis and Processing architecture (ASAP) (Hollywood et al., 2004).

2.1 Questions and Challenges

The first phase identifies the operational questions that the data analysis will seek to answer, as well as identifying the obstacles to answering those questions. For this project, the operational question was to identify instances of potential terrorist preoperational surveillance and probing. Initially, our focus was on personal surveillance—individuals taking photos, video, or notes about a site. Later, based on follow-up discussions with MPD officials, we broadened our analysis to include suspicious packages and bomb threats, both of which can be used in preoperational probing efforts to determine how civilians or law enforcement personnel react to planted items or threats. For example, Grant (2006) has reported that insurgents in Iraq have use hoax improvised explosive devices to learn how U.S. forces respond to them.

We also sought to include "approach" probing, in which people attempted to explore restricted areas or ask suspicious questions of site personnel. McCue (2006), for example, noted that increased approach attempts were an indicator of increasing surveillance efforts around a facility of interest. However, the 911 CFS data contained no reports of "approach" probing, other than a few calls about "Middle Eastern" individuals asking for directions to a landmark like the White House—itself a key finding we discuss later in this report.

2.2 Data Collection and Fusion

The second phase entails collecting data about suspicious incidents, including information that can be used to analyze the time, space, and information of the incidents. The MPD initially provided us a copy of the records of 911 calls forwarded to the MPD between October 2005 and September 2006. Each record contained fields for the time and date of the event, fields providing the address or cross-street and geospatial location (in Spatial Data Transfer Standard (SDTS) coordinates), and fields providing the general type of the call and the comments typed by the 911 operator during the call. After initial meetings, we were first provided with the records of 911 calls submitted to the MPD between October 2005 and June 2007, and later with the records of 911 calls forwarded to Washington, D.C., Fire and Emergency Services (DCFEMS) between October 2005 and June 2007, for about 1.4 million call records in total. Call records were provided as flat files in SPSS format. After our in-progress review meeting with the MPD, we were also forwarded the MPD's internal files on hazardous materials (HAZMAT) and suspicious package responses, both of which were formatted in Excel spreadsheets describing several hundred incidents. The latter files contained time and location fields, but had much less detail on the nature of the incidents; the suspicious package file had only brief descriptions, while the HAZMAT file did not have any descriptive information.

2.3 Operationally Relevant Preprocessing

This phase inventories the quality of the data, identifies the key fields and variables for analysis, and prepares the data for analysis by ensuring consistent data formats, consolidating records, removing records with missing or invalid data, and reformatting data in formats that can be read by analysis programs. For projects that involve large amounts of free-text data, this phase includes performing text mining to extract structured data such as names, dates, and addresses.

For this project, the main preprocessing challenge was consolidating the data. CFS data were delivered to RTI in separate sets of SPSS files. The first set of files contained structured data about each CFS, and the second set of files contained the related unstructured text comments for the CFS records. A total of eight files, representing 1,107,075 CFS (Table 2-1) were delivered for analysis over the course of the project.

Table 2-1. Type of Files Received and Time Period Covered

File Type	Time Period Covered	Date Received
CFS—MPD	October–December 2005	November 2006
CFS—MPD	January–September 2006	November 2006
CFS—MPD	October 2006–June 2007	July 2007
CFS—DCFEMS	October 2005–June 2007	September 2007
Comments—MPD	October–December 2005	November 2006
Comments—MPD	January–March 2006	November 2006
Comments—MPD	April–June 2006	November 2006
Comments—MPD	July–September 2006	November 2006
Comments—MPD	October 2006–June 2007	July 2007
Comments—DCFEMS	October 2005–June 2007	September 2007

CFS = call for service; DCFEMS = DC Fire and Emergency Services; MPD = Metropolitan Police Department.

The structured CFS data files each contained 23 variables, which are summarized in Table 2-2. A full codebook is located in Appendix A.

The comments data files each contained three variables, which are summarized in Table 2-3. The structure of the comments files were such that each unique CFS record could have multiple related comment records (see Table 2-4 for an example) such that, when all comment records for a particular call are combined, a complete transaction of the comments are typed during the call. The comments field contained basic information (e.g., a short description of the reason for the call, administrative information) about each call, with the amount of detail varying by call.

Table 2-2. CFS Data File Variables

Variable	Description
agid	responding agency
sdts	date-time stamp
year	year
month	month
moday	month and day stamp (e.g., 1001 = October 1)
time	time of the call
hour	hour of the day the call was received
eid	unique identifier for a call for service
case_num	a case number (CCN number) is issued whenever an offense/incident report is taken
address	physical address where call originated; a blank address indicates the call occurred at an intersection
xstreet	Cross-street or intersection
eapt	apartment number/building floor/suite number/miscellaneous text description
ecompl	commonplace (e.g., name of apartments or building)
psa	police service area the call originated from
tycod	type of call
typ_eng	English version of the call type code (consistent with variable “tycod”)
cfscat	calls for service category
rcfscat	recoded calls for service category to reduce the number of categories
sub_tycod	indicates whether the event was in progress, just occurred, etc.
prority	numeric priority of the call
xc	geo-coded x coordinate
yc	geo-coded y coordinate
dispo	disposition/result of the call

Table 2-3. Comments Data File Variables

Variable	Description
sdts	call date-time stamp
eid	unique identifier for a call for service
comm	case notes and comments typed by the dispatcher

Table 2-4. Sample Comment Records for a Single CFS

eid	Comments
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18
5223332	** >>>> by: FICTICIOUS NAME on terminal: d08
5223332	** LOI search completed at 01/01/06 00:35:20
5223332	** Case number R2006000027 has been assigned
5223332	** >>>> by: FICTICIOUS NAME on terminal: d08
5223332	\NUMBERS FOR MP HAS R E T U R N---D1335

The CFS data files were combined into one single file prior to variable recoding. The date-time stamp variable (*sdts*) was stored as a string variable in the original files, which required that it be parsed into its distinct month, date, year, hour, minute, and second elements in order to use these elements to create date and time variables that would be recognized as such by the analysis software. For example, a value of 20051006122126ED stored in the *sdts* variable represents October 6, 2005, at 12:21:26 Eastern Daylight time. The parsing was completed using the SUBSTRING function in SPSS to extract specific position ranges from the *sdts* variable that corresponded with each element of the date-time stamp variable. For example, the following code, COMPUTE Year = (SUBSTR(*sdts*,1,4)), extracts positions 1 to 4 of the *sdts* field and stores it in the newly created *year* variable. Using the previous example, 2005 would be extracted with this code.

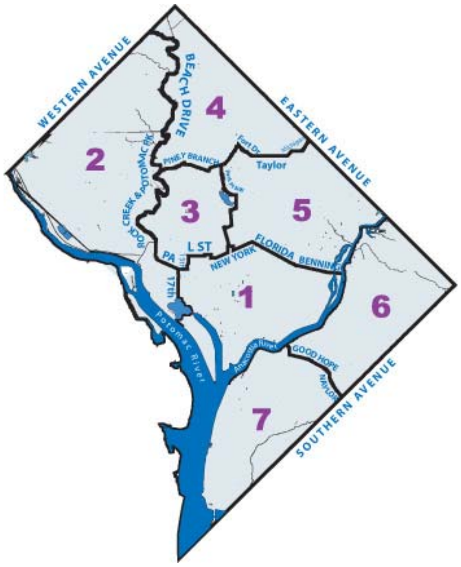
The newly created date field was then used to create a categorical variable representing the day of the week that the call occurred. This was achieved by copying the date field into a new field that displayed the date as the day of the week (e.g., Mon, Tue) and then performing a string conversion to a newly created string variable. The string conversion is necessary because this function copies the actual three-letter abbreviation of the week instead of the date itself to this new field, thus making a categorical variable.

The parsed hour field was used to create a time block variable with the following values: mid–4am, 4am–8am, 8am–12pm, 12pm–4pm, 4pm–8pm, and 8pm–mid. Calls were assigned to these time blocks using the following rules:

- If hour between 00 and 03, time block = mid–4am
- If hour between 04 and 07, time block = 4am–8am
- If hour between 08 and 11, time block = 8am–12pm
- If hour between 12 and 15, time block = 12pm–4pm
- If hour between 16 and 19, time block = 4pm–8pm
- If hour between 20 and 23, time block = 8pm–mid

Finally, a new variable representing the seven police districts in Washington, D.C., was created (Figure 2-2), using the police service area (*psa*) variable as the first digit of each three-digit *psa* that represents the district.

Figure 2-2. Washington, D.C., Metropolitan Police Department Districts



The comments data files contained multiple comment records for each unique CFS (Table 2-4). In order to obtain a complete comments record for each CFS, the multiple comments needed to be concatenated into one single record. The concatenation was completed using the LAG function in SPSS. This function compares the unique identifier for the current record to the unique identifier for the previous record; if the unique identifiers are the same, the comment variable from the previous record is appended to the current record such that, when the last unique identifier for a given CFS is reached, a single record contains all of the comments for the CFS in question. The final comment record containing all comments for a given CFS is also flagged to identify complete records. These flagged records were then saved to a new file that now contains a single record for each CFS with all comments. Figure 2-3 shows the results of this concatenation process. Prior to this concatenation, the length of the comments variable was increased to 2,000 so that no comments were truncated during concatenation.

It is important to note that the comment records had to be concatenated without reordering the original file to ensure that the comments were concatenated in the same order that they were typed during the course of the call, because within each set of comment records for a given call, there was not a variable designating the order of the comments (e.g., a sequential number). Following this recoding, the concatenated comment field could then be appended to any CFS analysis files by matching on the common identifier between both sets of files, the *eid* variable.

Figure 2-3. Color-Coded Comment Concatenation Sample

eid	Comments
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18 ** >>>> by: FICTICIOUS NAME on terminal: d08
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18 ** >>>> by: FICTICIOUS NAME on terminal: d08 ** LOI search completed at 01/01/06 00:35:20
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18 ** >>>> by: FICTICIOUS NAME on terminal: d08 ** LOI search completed at 01/01/06 00:35:20 ** Case number R2006000027 has been assigned
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18 ** >>>> by: FICTICIOUS NAME on terminal: d08 ** LOI search completed at 01/01/06 00:35:20 ** Case number R2006000027 has been assigned ** >>>> by: FICTICIOUS NAME on terminal: d08
5223332	** Event I20050732945 has been reopened at: 01/01/06 00:35:18 ** >>>> by: FICTICIOUS NAME on terminal: d08 ** LOI search completed at 01/01/06 00:35:20 ** Case number R2006000027 has been assigned ** >>>> by: FICTICIOUS NAME on terminal: d08 \NUMBERS FOR MP HAS R E T U R N---D1335

2.4 Identification, Characterization, and Modeling

Data analysis takes place during the identification, characterization, and modeling phase. In general, data analysis begins with filtering—using rules to exclude the bulk of the available data from the analysis. In this project, for example, filtering was critical to exclude the vast majority of the 1.3 million CFS records.

The next step is usually characterization, or reviewing the records (manually or by using software), to see if they fit into various categories or groups. Primary examples include identifying groups of records close to each other in time and space, dividing records into groups representing similar observed behavior, and evaluating how suspicious the records are. This step also includes identifying relationships between records, either by being in the same time, space, and nature groups, or by having details strongly implying that the same people appeared in multiple records.

The third step in this phase applies models and visualizes the results, which entails creating a series of charts and plots to visualize the data. These visualizations could include bar or pie charts to show the distribution of observations by category, trend charts to determine if certain types of observations are increasing (and thus worth further attention), and location plots to find geographic clusters of locations. This step also includes drilling down, or examining incidents of interest in detail. In addition to examining the records themselves, drilling down includes backsweeping, or searching the data sets for records potentially related to the incidents of interest.

The final step explicitly generates hypotheses about the analysis results—identifying those incidents of interest worth further investigation and expressing why those incidents may be of interest. In addition to stating the hypothesis, this step includes explicitly marshaling evidence for and against the hypothesis, as well as a current assessment of the hypothesis's likelihood. As an example, the final chapter of this report contains a table of hypotheses for those clusters of incidents that most likely represent preoperational surveillance, all of which include significant uncertainties.

2.5 Security-Specific Evaluation

This phase includes both verification and validation of the results—namely, are the identified clusters of interest actually worth investigating?—and of the analysis to date. The reviews in this phase frequently lead to new operational questions to answer unresolved issues, incorporation of additional data, and follow-up analysis.

2.6 Operationally Actionable Output

The final phase of RTI Trinity Sight™ produces analysis products that support decision making in counterterrorism and anticrime efforts, including batch products that summarize the results of the research effort. Ideally, they also include setting up processes to replicate the analysis on a regular basis in order to create a stream of updated analysis products that can support day-to-day decision making.

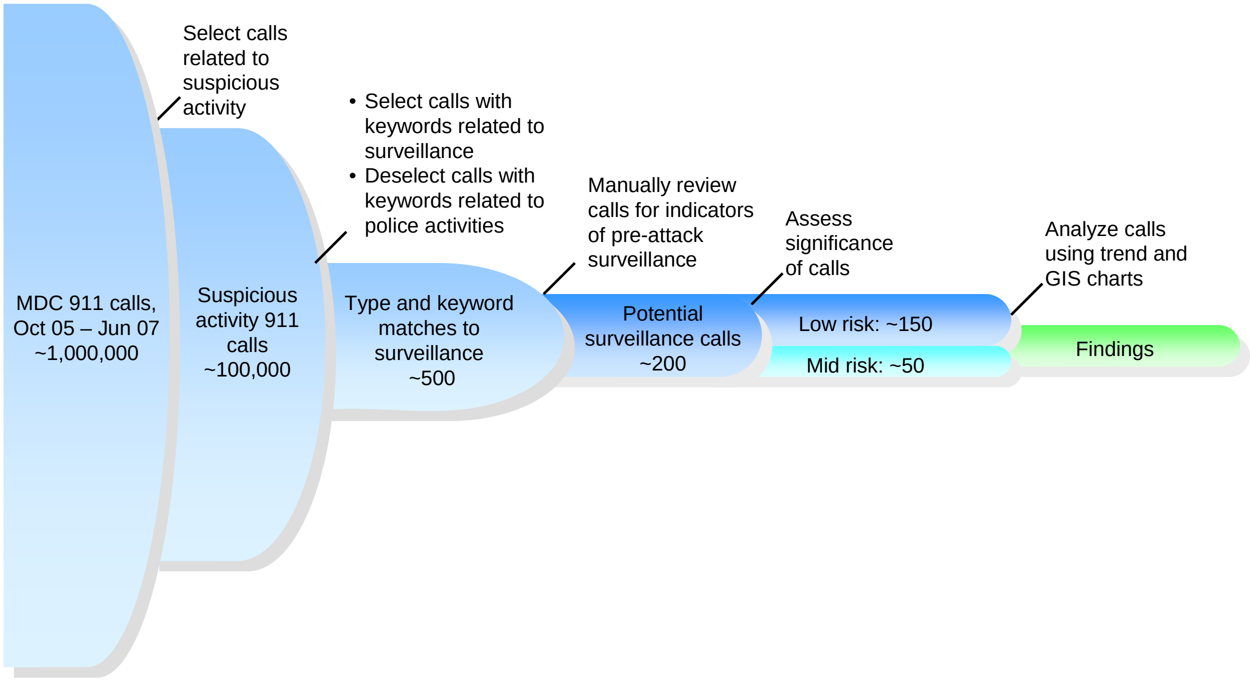
Analysis of Potential Surveillance Incidents

The first analysis we performed using 911 call data specifically searched for target surveillance, which includes behavior such as photographing the target, studying it through binoculars, or writing detailed notes about it. This analysis expanded on the earlier work of McCue (2006), which characterized instances of potential surveillance around a single building of interest.

3.1 Methods

The first phase of the methodology filtered the 911 CFS records to identify those potentially related to preoperational surveillance of a target. Figure 3-1 summarizes the filtering process, starting with all 911 calls forwarded to the MPD from October 2005 through June 2007. As noted, there were more than 1 million such calls.

Figure 3-1. Filtering 911 Call Records to Identify Potential Surveillance Reports



MDC 911 calls,
Oct 05 – Jun 07
~1,000,000
Select calls related to suspicious activity
Suspicious activity 911 calls
~100,000
• Select calls with keywords related to surveillance
• Deselect calls with keywords related to police activities
Type and keyword matches to surveillance
~500
Manually review calls for indicators of pre-attack surveillance
Potential surveillance calls
~200
Assess significance of calls
Low risk: ~150
Mid risk: ~50
Analyze calls using trend and GIS charts
Findings

GIS = geographic information system; MDC = Metropolitan DC.

The first step was to filter records by type. Using the existing call type field, we selected and extracted all suspicious person, suspicious package, suspicious vehicle, "investigate the trouble," and "other" records in the call data.[1] This created a population of about 100,000 calls, including about 14,000 suspicious person/vehicle calls, and about 85,000 investigate the trouble/other calls.

The second step was to filter the records based on content. We first reviewed about 500 suspicious person and suspicious vehicle records to identify and characterize reports potentially related to terrorist surveillance. Only a small portion of records appeared to be potentially relevant, and all found related to individuals taking pictures, video, or notes. We thus extracted a subset of records containing key strings related to surveillance, as follows:

- Photography: photo, camera, picture
- Video: video, taping, film, camcorder
- Note-taking: note, write, typing
- Visual aids: binocular, telescope, lense

Two hundred and eleven suspicious person/vehicle records and 730 investigate the trouble/other records included one or more of these keywords. Upon further review, many of the latter related specifically to police activities, especially taking photos of prisoners or of crime scenes. We thus omitted records containing the following keywords:

- Key words related to taking photos at crime scenes: CSS (Criminal Support Services, tasked to take photos), needs a picture, for photos, scene
- Key words related to taking photos of prisoners being transferred: warrant, extradite, missing

We then manually reviewed the remaining records (about 500) to identify those specifically related to surveillance of public places and infrastructure. We eliminated records containing references to "ordinary crime," such as casing of individuals, homes, and vehicles, and containing references to security cameras. This left us with 166 records on suspicious person/vehicle calls and 11 records on investigate the trouble/other calls, for a total of 177 potential surveillance calls.

The third step was to characterize the records along several dimensions: time, location, and nature. The MPD call records already included time and date fields; to these, we added 4-hour time block, day of week, and quarter.

Location was more complicated to define. Some records had a specific address; others listed a nearest cross-street; and others listed a place name, such as "White House" or "14th Street Bridge." Most records came with State Plane Coordinate System (SPCS) coordinates, which provided x/y-coordinates in

[1] We initially just selected suspicious person, suspicious vehicle, and suspicious package records. During in-progress review meetings with MPD staff, it was noted that potential surveillance calls might be coded as investigate the trouble, or other as well, so those were added to the analysis.

meters.[2] We labeled locations in three ways: by specific target name (if applicable), by target type, and by general area or neighborhood. We also created a hybrid labeling that combined the most common specific targets and target types with geographic areas for otherwise "unspecified locations," such as generic office buildings and residences.

We then looked for clusters of incidents at or near the same location. To do this, we used a simple heuristic, ordering the calls by x-coordinate and then by y-coordinate, and flagged records with the same x/y-coordinates. We then reviewed groups of "nearby" records to determine if records with slightly different coordinates in fact applied to the same location. We similarly ordered the records by cross-street and looked for clusters. Finally, we ordered the records by location name (if available) and flagged clusters of records for the same location.

We next looked for clusters of events in both time and space. To do this, we first ordered the events by their hybrid labeling, then ordered the events by date. We then read adjacent groups of records to see if there were clusters of events occurring in the same area in short succession (within a month or so).

For nature, we first characterized each call by whether the surveillance method reported related to photography, videography, using binoculars, or taking notes. In McCue's (2006) analysis of a single building, videography was seen as posing a much more significant risk than photography, because video equipment was more expensive. However, we ended up not incorporating the type of surveillance into our risk analysis. For many of the calls, the comments reported a person "taking pictures or taping" the location (i.e., they could not clearly tell whether a person was taking pictures or video). Furthermore, the price of video equipment for at least brief video has become inexpensive enough (commonly included on cameras and cell phones) that the distinction no longer appears strongly meaningful.

Instead, we created a risk rating framework that allocated points to records along several different dimensions, including:

- how atypical the behavior reported in the call (as noted in the comment field) was compared with standard tourism, work, and "ordinary criminal" behavior;
- how attractive the location would be to a terrorist;
- whether the call was part of a cluster of calls for the same target, such that there was some confidence that the same people were responsible for the reported behavior; and
- whether a police report about the incident had been filed, showing that the responding officer found something "worth reporting."

Greater points equaled a greater risk that the call actually represented potential preoperational surveillance. The framework was based initially on our experience with prior counterterrorism research

[2] SPCS is described on the U.S. Geographic Survey's Web page: "Spatial Address Encoding," at http://mcmcweb.er.usgs.gov/sdts/SDTS_standard_nov97/part1an3.html.

and was modified after consultation with other RTI and MPD subject matter experts. Table 3-1 shows the complete risk rating framework.

Table 3-1. Risk Rating Framework for Potential Surveillance Events

Dimension	Score	Description
1. Atypicality of reported activities	Unusual:1 point	Could be explained by ordinary work, tourism, or criminal behavior. Examples include photographing office buildings, lesser-known landmarks, and airplanes.
	Highly atypical: 2 points	Not readily explainable, especially if behavior is risky. Examples include photographing highways, railroads, and other public infrastructure.
	Threatening: 4 points	Matches known pre-attack signatures. Examples include using large numbers of cell phones (or discarding them), attempted trespassing, and asking probing questions.
2. Attractiveness of target	Attractive: 1 point	Well-known landmark (and hence well monitored) or opportunity for significant casualties. Examples include high-density office and residential buildings, well-known Washington, D.C., landmarks, and Metrobus.
	Highly attractive and atypical: 2 points	Not normally photographed and could result in massive casualties or disruption to Washington, D.C. Examples include highway bridges and overpasses, chemical facilities, and Metrorail.
3. Membership in a cluster	Moderate confidence: 1 point	Moderate confidence that the calls could be due to the same group of individuals because they are reasonably close in space, time, and descriptions.
	High confidence and atypicality: 2 points	Atypicality score of at least 2, and high confidence that the calls are due to the same individuals because they are very close in space, time, and description.
4. Presence of police report	Police report: 2 points	Call record includes a police report number.
Total	10 points maximum	

As shown, a call can receive up to 10 points. We broadly categorized the risk rating a call received into one of three categories: 0 to 3 points is equivalent to low risk, with the call likely reporting on an activity with a conventional explanation; 4 to 6 points is equivalent to moderate risk, with the call representing an increased risk of representing potential surveillance; finally, 7 or more points is equivalent to high risk. Calls in the high risk category would specifically match a known threat profile. As will be seen, no call was in the high risk category.

3.2 Characterization of Potential Surveillance Calls, by Time

Figure 3-2 shows the results of characterizing the potential surveillance calls by time, comparing the time block and day of week between potential surveillance calls and the approximately 14,000 suspicious person and vehicle calls. The differences between day of week are comparatively small and may be due to statistical noise resulting from the fairly small number of potential surveillance calls. However, the numbers of calls by time block are very different, with potential surveillance calls concentrated during the day and suspicious person and vehicle calls concentrated at night.

Figure 3-2. Potential Surveillance Calls and Suspicious Person/Vehicle Calls, by Day of Week and Time of Day

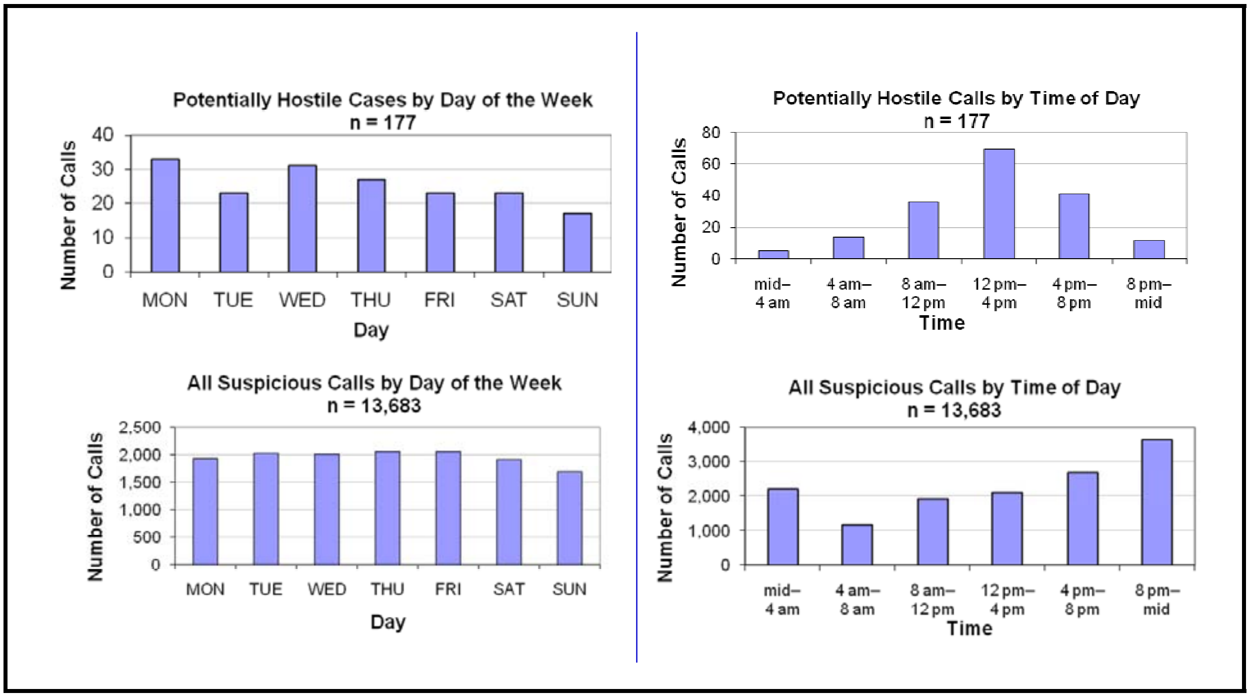


Figure 3-3 shows the line chart of potential surveillance calls by month. The monthly totals fluctuate around an average of eight calls.

Figure 3-3. Potential Surveillance Calls, by Month

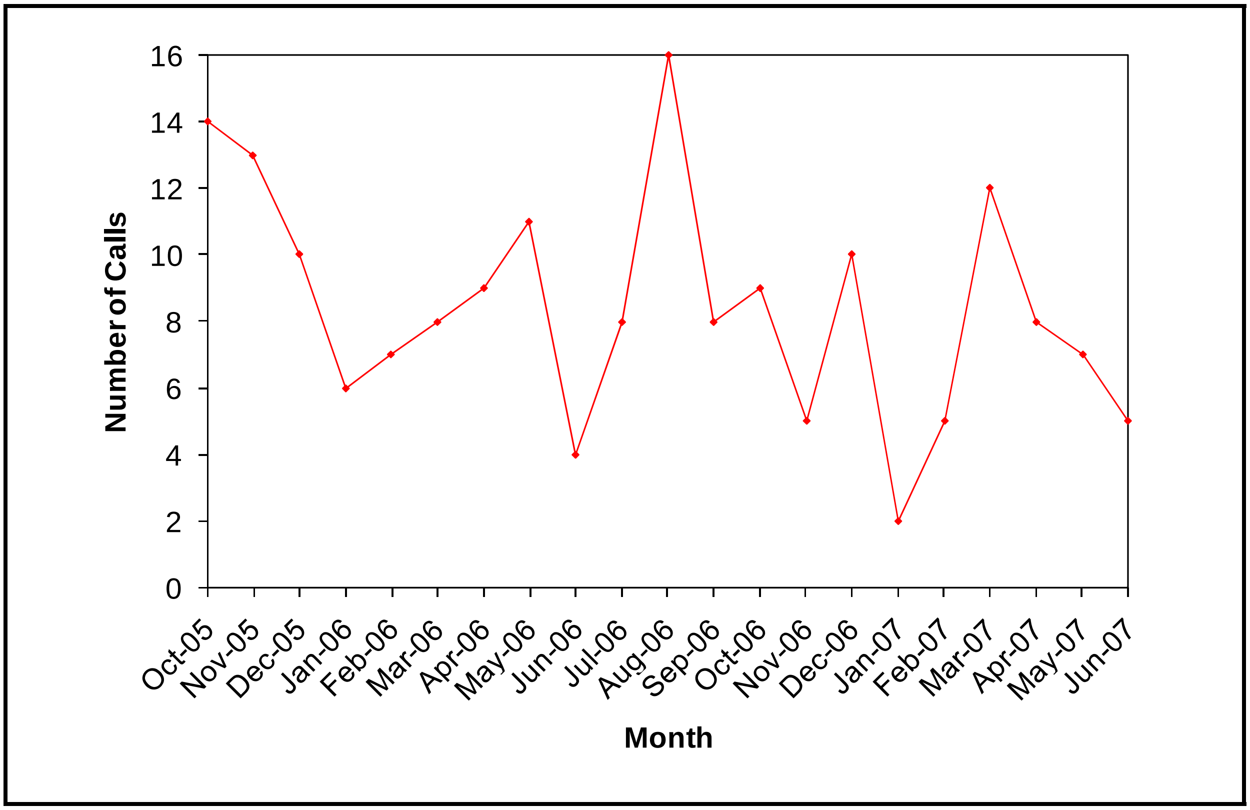
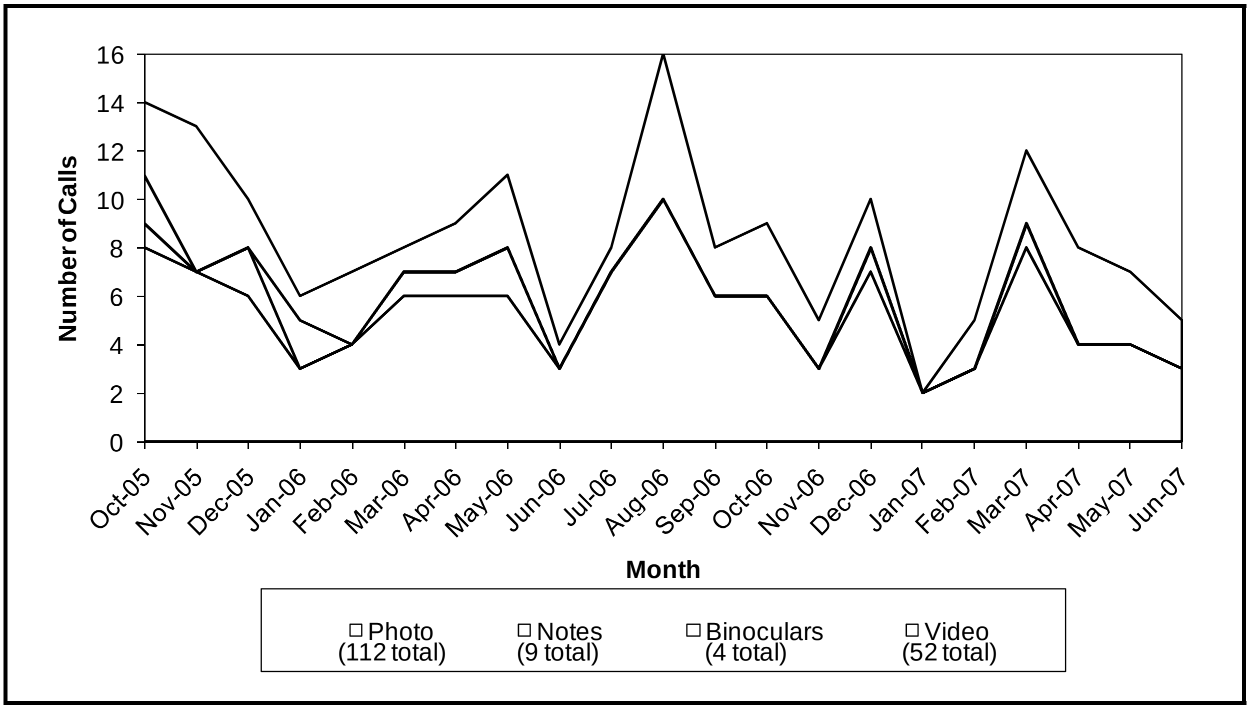


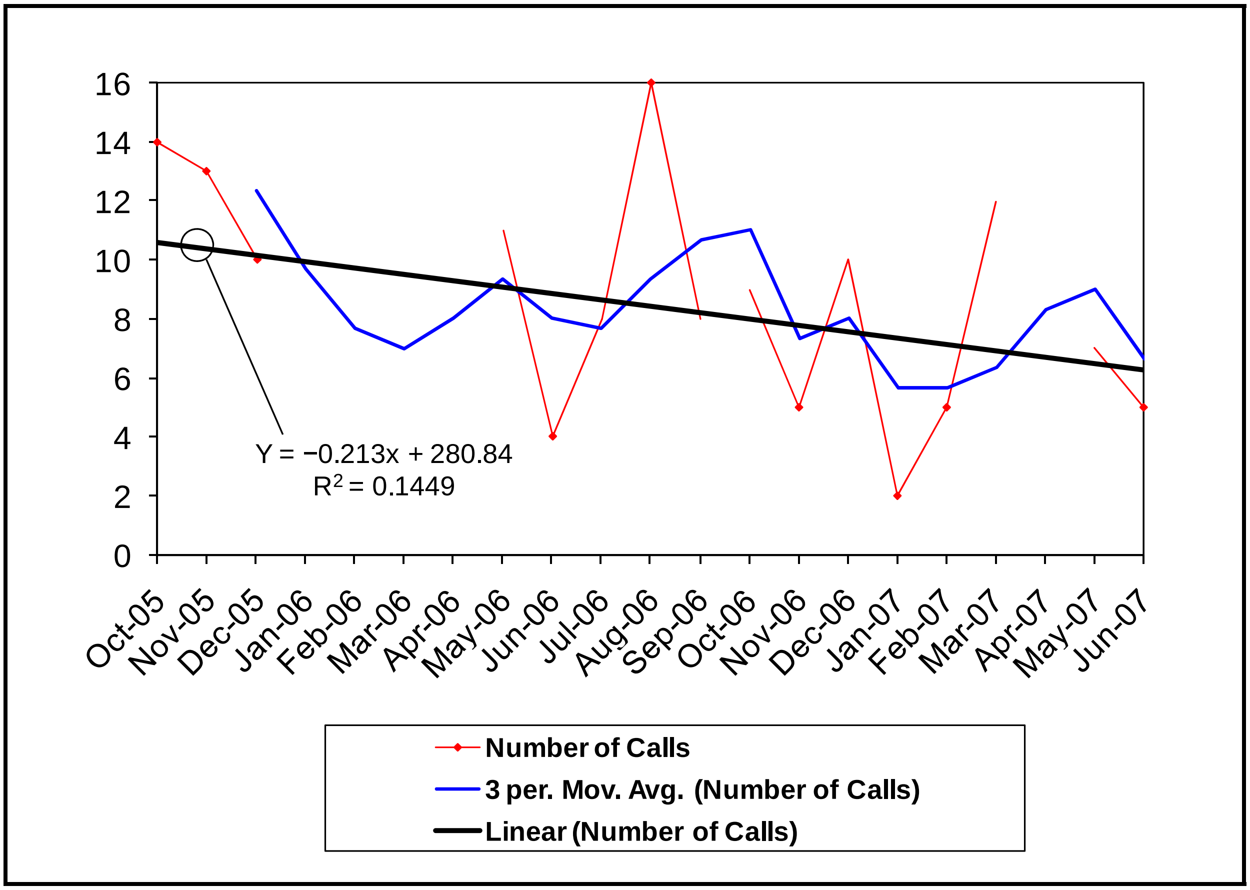
Figure 3-4 breaks down the calls by type of surveillance employed: photography, videography, taking notes, or using binoculars. If the call comment was unclear about whether photos or video were being taken, we assumed photography. The figure shows no significant changes between the types of surveillance employed.

Figure 3-4. Potential Surveillance Calls, by Month and Type of Surveillance



Finally, Figure 3-5 adds a 3-month moving average and a linear trend line to the line chart of potentially suspicious calls. The trend line shows some evidence that the number of calls has been decreasing somewhat, from approximately 10 per month around October 2005 to 6 per month around June 2005. The moving average shows some evidence of seasonality, with substantially reduced calls in winter months. Given the seasonality and significant month-to-month variation in calls, it is unclear whether the trend line reflects a real trend or is an artifact of seasonality and random noise.

Figure 3-5. Moving Average and Trendline for Potential Surveillance Calls



3.3 Characterization of Potential Surveillance Calls, by Location

Figure 3-6 compares the numbers of potential surveillance calls and suspicious person/vehicle calls by police service area. As shown, potential surveillance calls are tightly concentrated in downtown areas, while suspicious person/vehicle calls are distributed throughout Washington, D.C.

Figure 3-6. Potential Surveillance Calls and Suspicious Person/Vehicle Calls, by Police Service Area

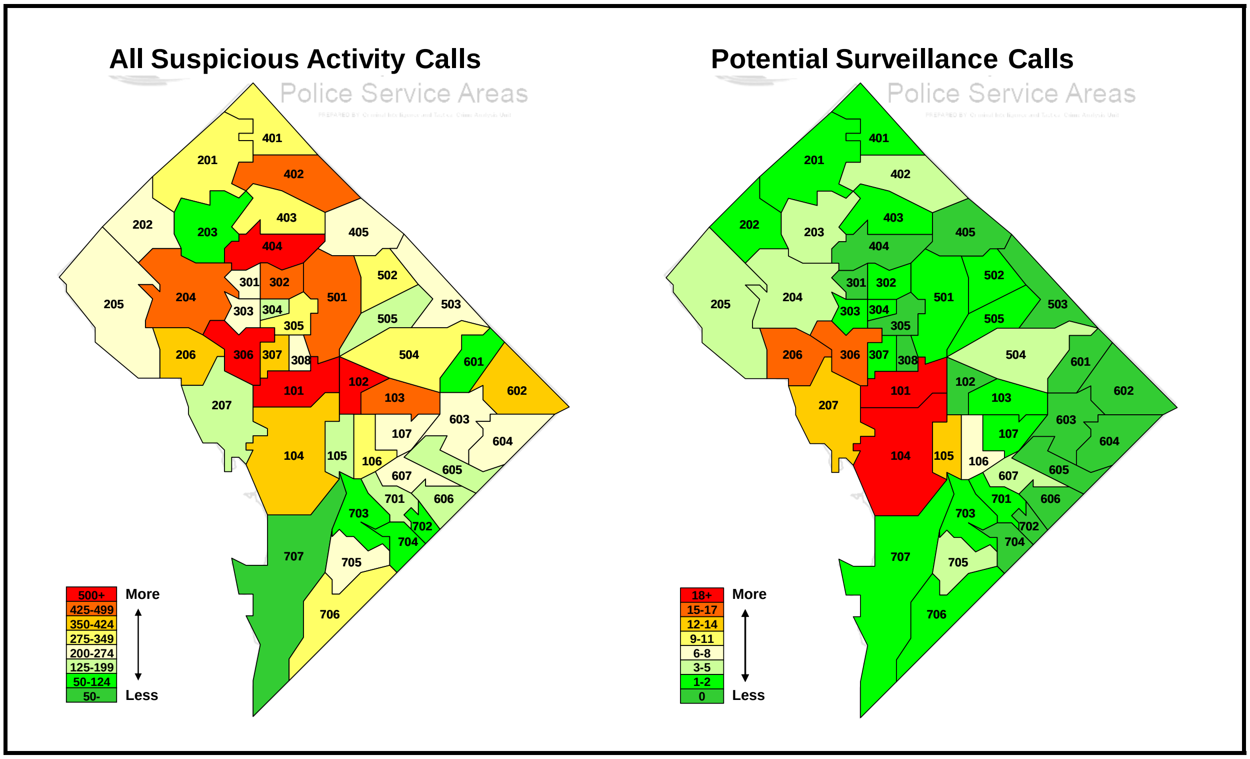


Figure 3-7 characterizes the potential surveillance calls by the hybrid listing described earlier, combining named locations, major types of locations, and geographic areas. As shown, a large proportion of calls concerned Washington, D.C.'s highways, especially the I-395 system. Military locations, including the Bolling Air Force Base/Naval Station and Navy Yard areas, were also named regularly. Several other Washington, D.C., locations were also named, including the Pepco Power Plant in Northeast Washington, D.C., a section of railroad in Northeast Washington, D.C., and Sibley Memorial Hospital. Other potential surveillance calls were distributed throughout various Washington, D.C., neighborhoods, concentrated in the downtown area.

Figure 3-7. Potential Surveillance Calls, by Location

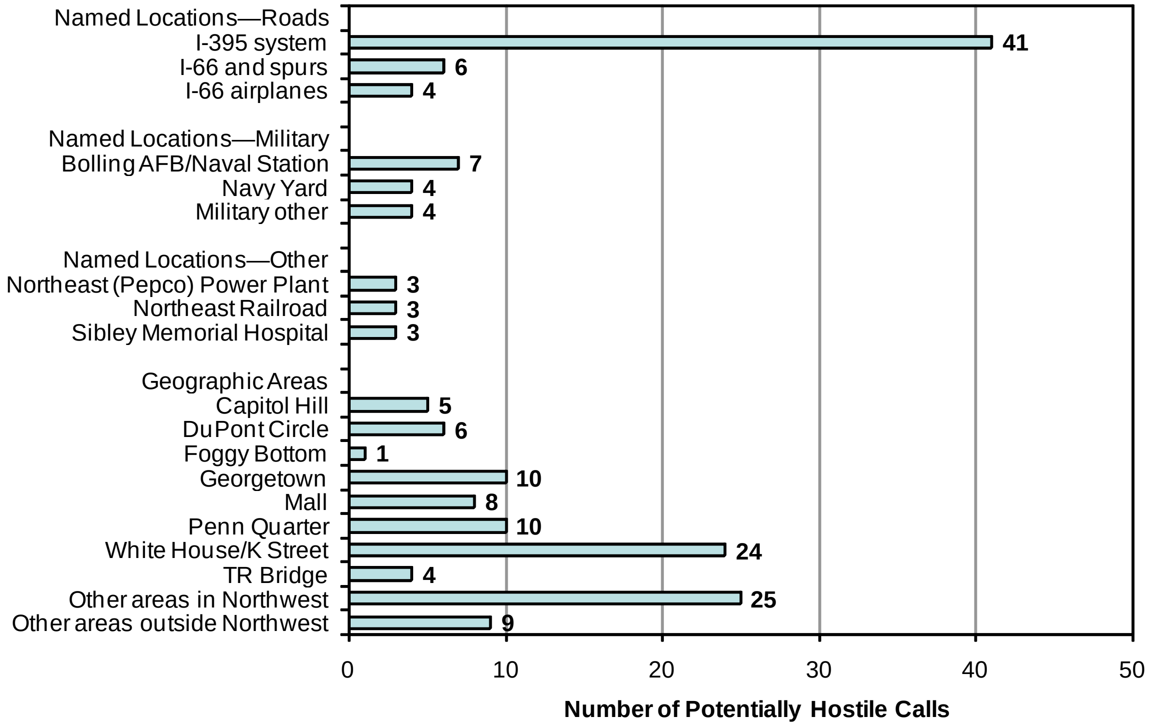
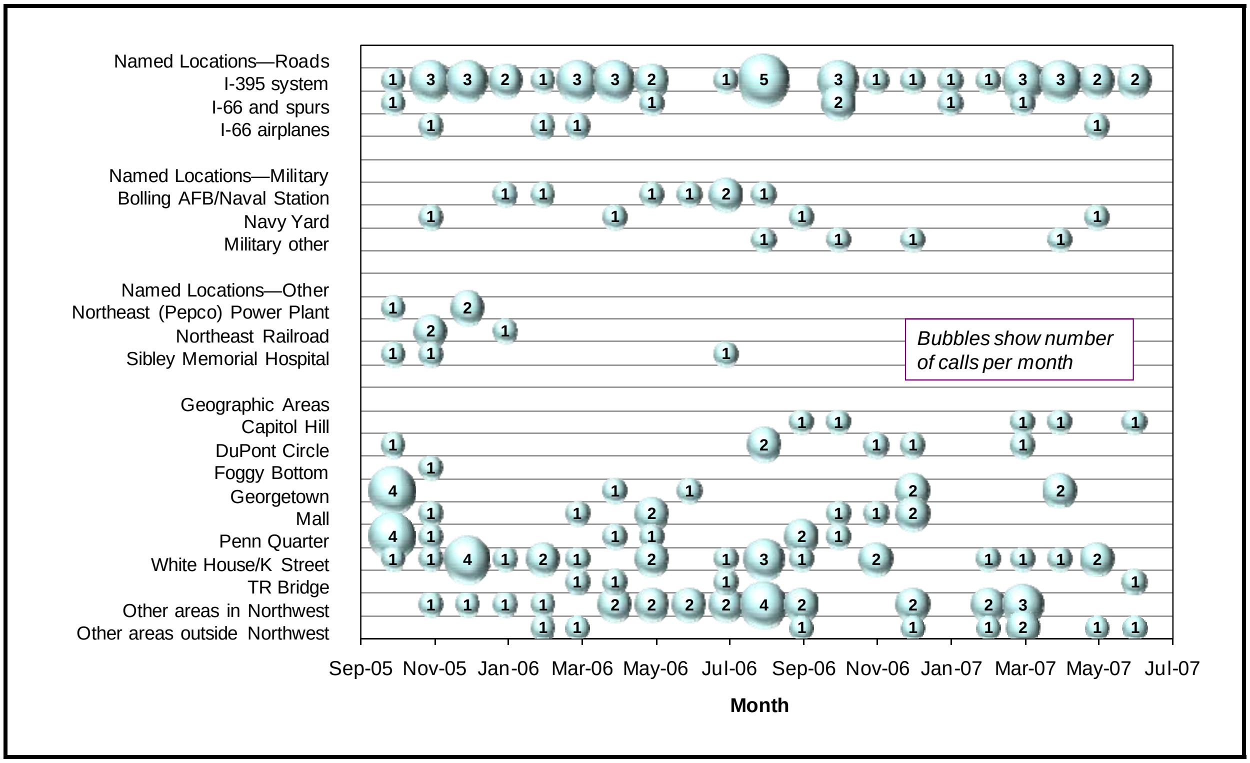


Figure 3-8 shows potential surveillance calls by both time (by month) and by location (by hybrid listing). The size and numbers within each bubble show the number of calls per month. In general, the dates of the calls for most locations are fairly evenly scattered, with few obvious trends or spikes. The exceptions are for the three "named locations" (the Pepco power plant, the Northeast Washington, D.C., railroad, and Sibley Memorial Hospital); these tend to be concentrated in late 2005.

Figure 3-8. Potential Surveillance Calls, by Time and Location



Bubbles show number of calls per month

3.4 Characterization of Potential Surveillance Calls, by Nature

Figure 3-9 shows the distribution of potential surveillance calls by assessed risk, on the aforementioned 0 to 10 scale. As shown, no calls scored higher than 6. There were no reports of specifically threatening behavior, nor were there any police reports filed, for any potential surveillance call.

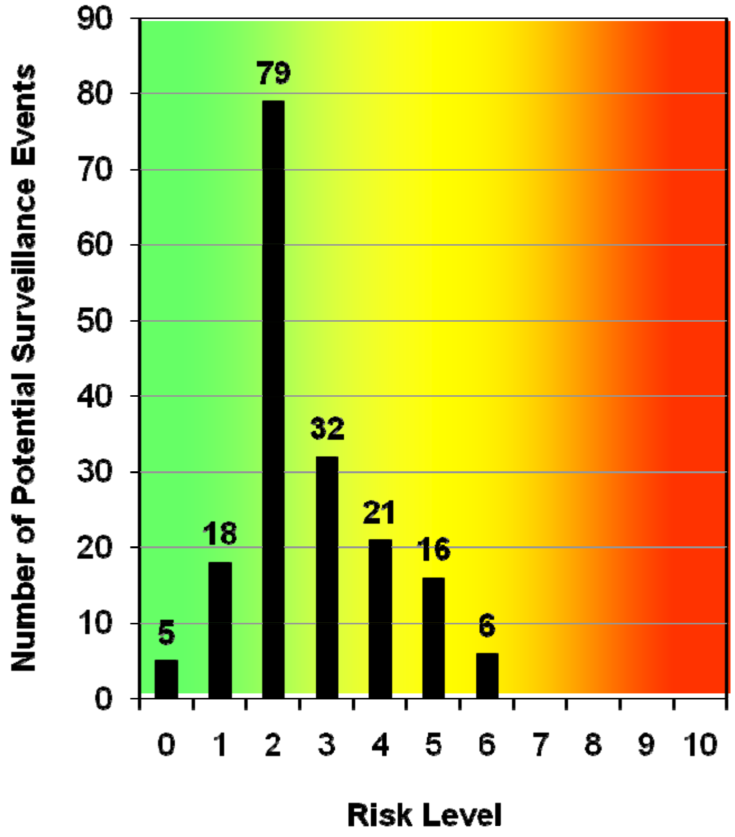
Six events scored 6. These calls were inconsistent with ordinary behavior, were for a highly attractive target, and were part of a high-likelihood cluster (i.e., strong possibility that all reports were of the same people) of similarly atypical observations.

Sixteen events scored 5. These calls had similar risk characteristics as those scoring a 6, but were part of a medium-likelihood cluster (i.e., much lower probability that the same people were responsible for all observations) or the target was not highly attractive.

Twenty-one events scored 4. These calls were similar to those scoring a 5, but were not part of a cluster or the target was not highly attractive.

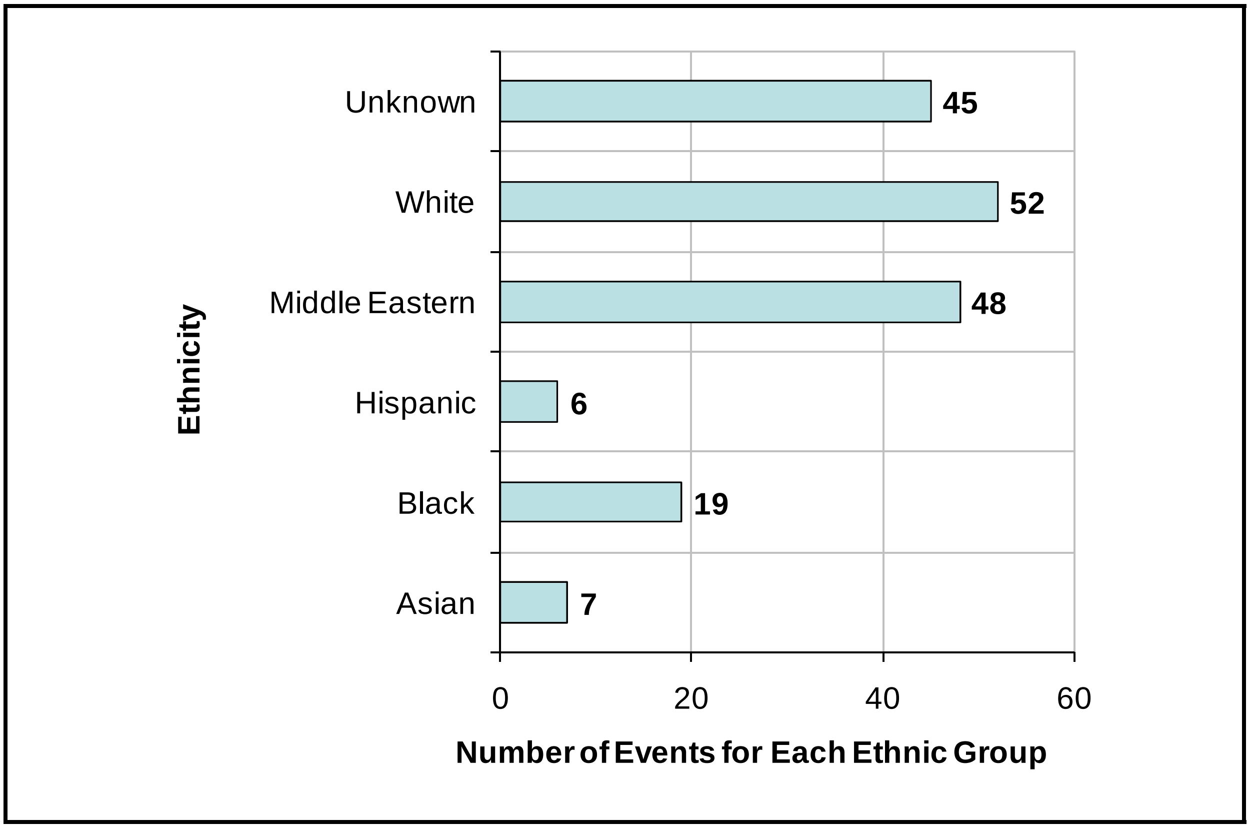
The remaining, large majority of calls were rated as 3 or less. These are comparatively unlikely to represent actual preoperational surveillance.

Figure 3-9. Potential Surveillance Calls, by Risk



As a final check, we considered the reported ethnicities of the suspects, if available, to ensure that our analysis is not simply detecting large numbers of “Middle Eastern” persons engaged in what would otherwise be normal behavior, such as photographing landmarks. Figure 3-10 shows the result. While the number of “Middle Eastern” persons is overrepresented, white persons were reported most frequently. We suspect that there is some overreporting of “Middle Eastern” simply based on callers’ likely suspicions, so the call analysis methods are doing a reasonable job of selecting potential surveillance calls based on behavior as opposed to ethnicity.

Figure 3-10. Ethnicities of Persons Reported in Potential Surveillance Calls

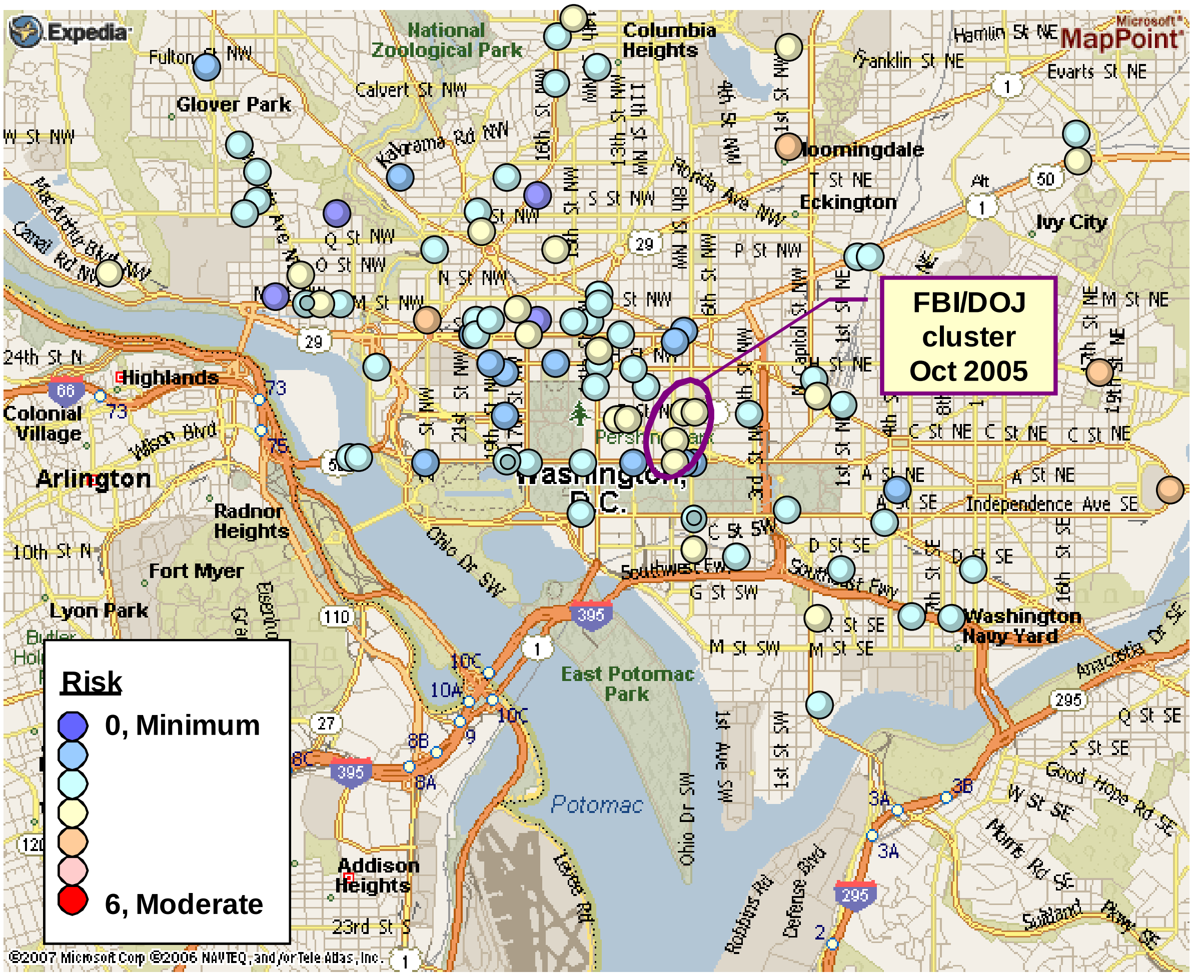


3.5 Clusters of Interest

We now consider location plots of the potential surveillance calls. The following plots show the location of the calls; the color shows the assessed risk from 1 to 6 (recall that there were no calls scoring higher than 6). The plots also highlight clusters of interest. The plots were created by graphing the calls' SPCS coordinates using Microsoft Excel's x-y plot feature, then manually fitting the plots to background maps of Washington, D.C., downloaded from Microsoft Expedia's mapping feature.

To provide a baseline of what a "normal" amount of suspicious activity looks like, Figure 3-11 maps call locations in downtown Washington, D.C., other than military and highway locations. The figure shows a fairly wide dispersion of calls, with some concentration in the K Street/White House areas. The only cluster of note involved four calls related to the DOJ and FBI buildings, in October 2005. However, given the age of the calls (almost 2 years old) and the comparatively low risk of the calls, this cluster does not seem to be high risk. In particular, three of the four calls were for photography of the DOJ and FBI buildings, which are both landmarks. The fourth reported a person surveying the FBI building from the rooftop of an adjacent building with binoculars; the observed person was probably part of a security detail.

Figure 3-11. Call Locations for the Downtown Washington, D.C., Area

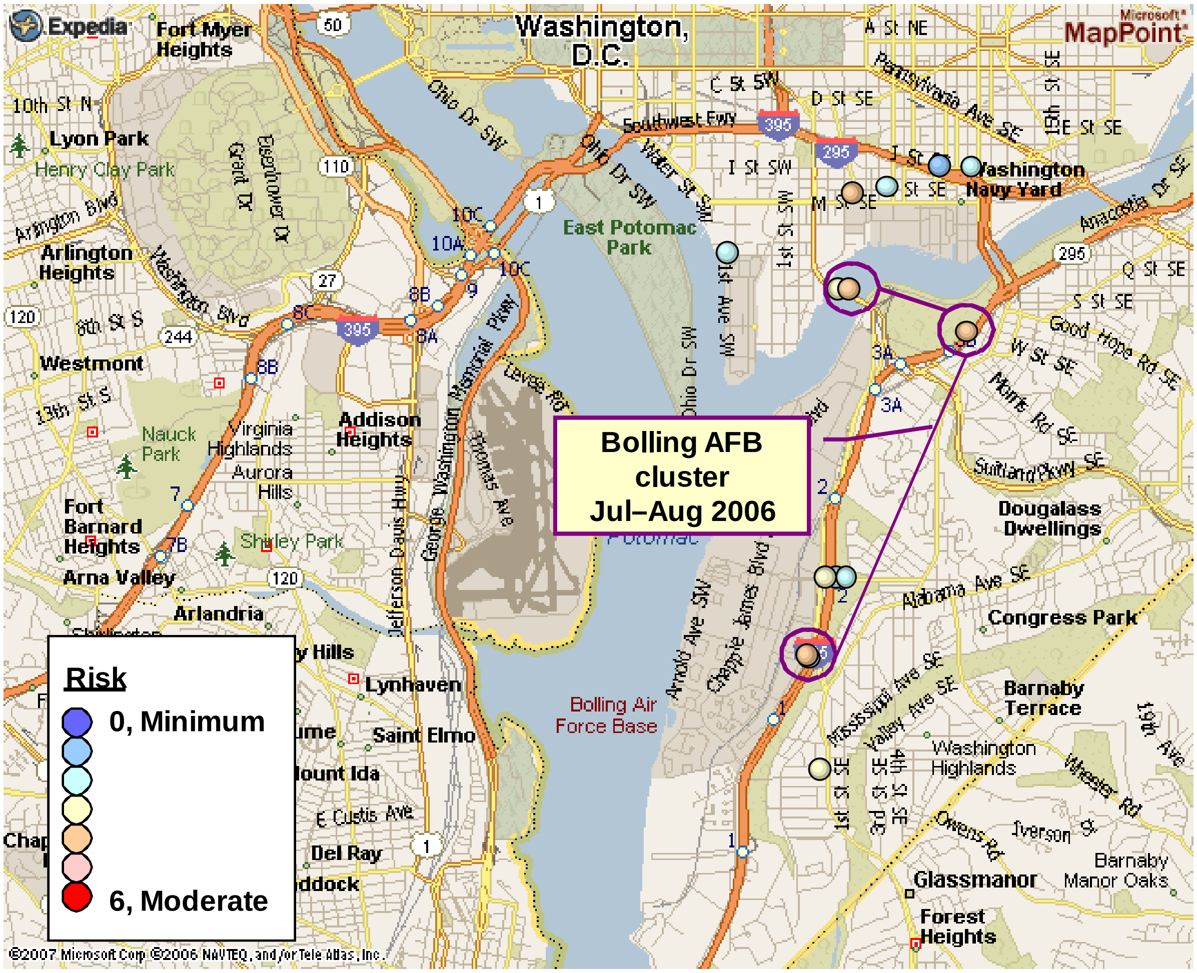


FBI/DOJ cluster Oct 2005

Source: Microsoft Expedia.

Figure 3-12 maps call locations in downtown Washington, D.C., for military locations. In contrast to Figure 3-11, this location plot does show some evidence of clustering, with three potentially related incidents around the Bolling Air Force Base (AFB)/Naval Station area in July and August 2006. The cluster likely contains a reporting error; the calls for the Frederick Douglass Bridge and for South Capitol Street and I-295 likely represent the same incident. Even though the “South Capitol and I-295” call was plotted near the entrance to Bolling AFB, this call was within 15 minutes of the call for the Frederick Douglass Bridge, and it would be easy for “South Capitol and I-295” to mean the Douglass Bridge or ramp from South Capitol Street onto I-295 (the start of Suitland Parkway). Furthermore, a cluster of two to three incidents, with some question about where the incidents actually were and what was being surveyed as a result, does not indicate a significant threat.

Figure 3-12. Call Locations for Military Facilities



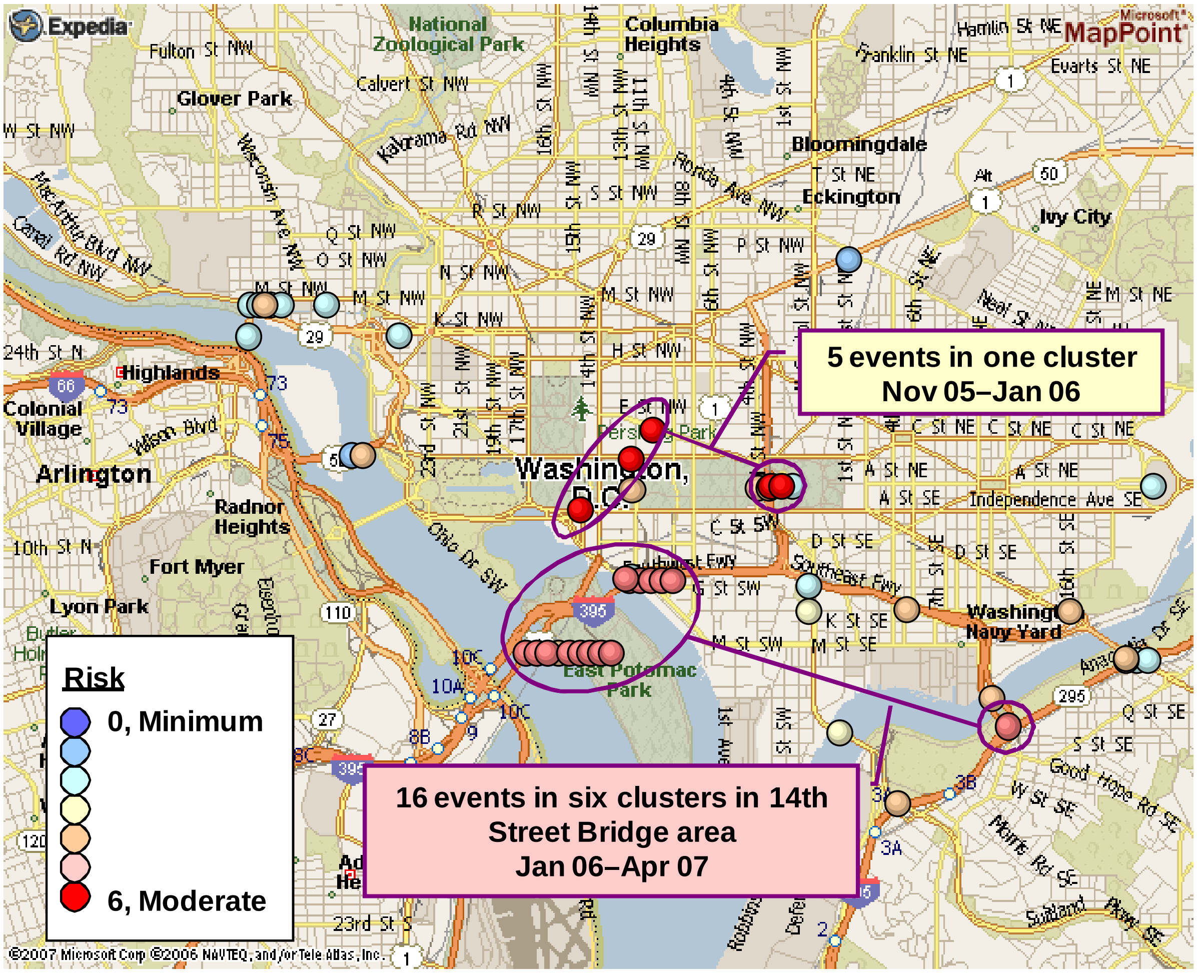
Bolling AFB cluster Jul–Aug 2006

AFB = Air Force Base.

Source: Microsoft Expedia.

Figure 3-13 maps call locations for Washington, D.C., highways. This figure is very different from the previous two, showing strong indications of clustering. The assessed risk levels were also higher, as these call locations tended to be highly atypical (photographing traffic and road or bridge infrastructure, with some risk to self while stopped on the side of the road), and highly attractive (disrupting these highways would have a major impact on Washington, D.C.'s ability to get people in and out of the city).

Figure 3-13. Call Locations for Washington, D.C., Highways



5 events in one cluster
Nov 05–Jan 06

16 events in six clusters in 14th Street Bridge area
Jan 06–Apr 07

Source: Microsoft Expedia.

As shown, there were two major sets of clusters. The first of these, shown as red dots (risk level 6) concerned a man taking pictures of traffic coming out of various northern exits from I-395 from November 2005 through January 2006. Given the closeness in time and similar descriptions, there is a fairly high likelihood that the same man was involved. Table 3-2 provides the date, location, and comment fields for the five linked incidents. It should be noted that the risk level implied from this cluster is not great, as the last call in this cluster was in January 2006.

The second set of clusters, and likely more significant, concerns individuals taking pictures of traffic or infrastructure on the 14th Street Bridge or in the Maine Avenue overpass area immediately north of the bridge. As shown in Figure 3-13, there were 16 such incidents in 6 clusters.

Table 3-2. Incidents of Taking Pictures on I-395's Northern Exits

Date	Location	Comment Field[3]
11/15/2005	10th St NW & D St NW	W/M 20'S BROWN HAIR HEAVY SETBLACK JKT BLUE JEANS......HE IS TAKING PICTURES OF THE OVER PASS ** LOI search completed at 11/15/05 18:36:08
12/16/2005	Tunnel—3rd St—Northbound	A W/M WITH A PUFFY TAN WINTER COAT IS TAKING PICTURES FROM THE 1ST OVERPASS OF THE TUNNEL,POSSIBLY D ST TAKING PICTURE OF CARS & THE TUNNEL ITSELF ** LOI search completed at 12/16/05 11:07:36 NFI
12/22/2005	15th St SW & Independence Ave SW	LOF… MALE WEARING DARK COLORED CLOTHING WITH A TV CAMERA….LOOK AROUND AND TAKING PICTURES OF THE TRAFFIC ** LOI search completed at 12/22/05 17:31:17 PLEASE HAVE UNITS TO CANVAS THE AREA
12/24/2005	Tunnel—3rd St—Northbound	CALLER STATES AND IRANEAN LOOKING MALE WAS TAKING PICTURES OF THE TUNNELL ** LOI search completed at 12/24/05 13:20:21
1/17/2006	12th St NW & Constitution Ave NW	W/M IN ALL BLACK ,,,BLACK HAT ...BLACK BAG SUBJ IS VIDEOING VEHS COMING OUT OF THE TUNNEL HE IS TAPING VEH'S AS THE COME OUT,, N/F ** LOI search completed at 01/17/06 15:46:37

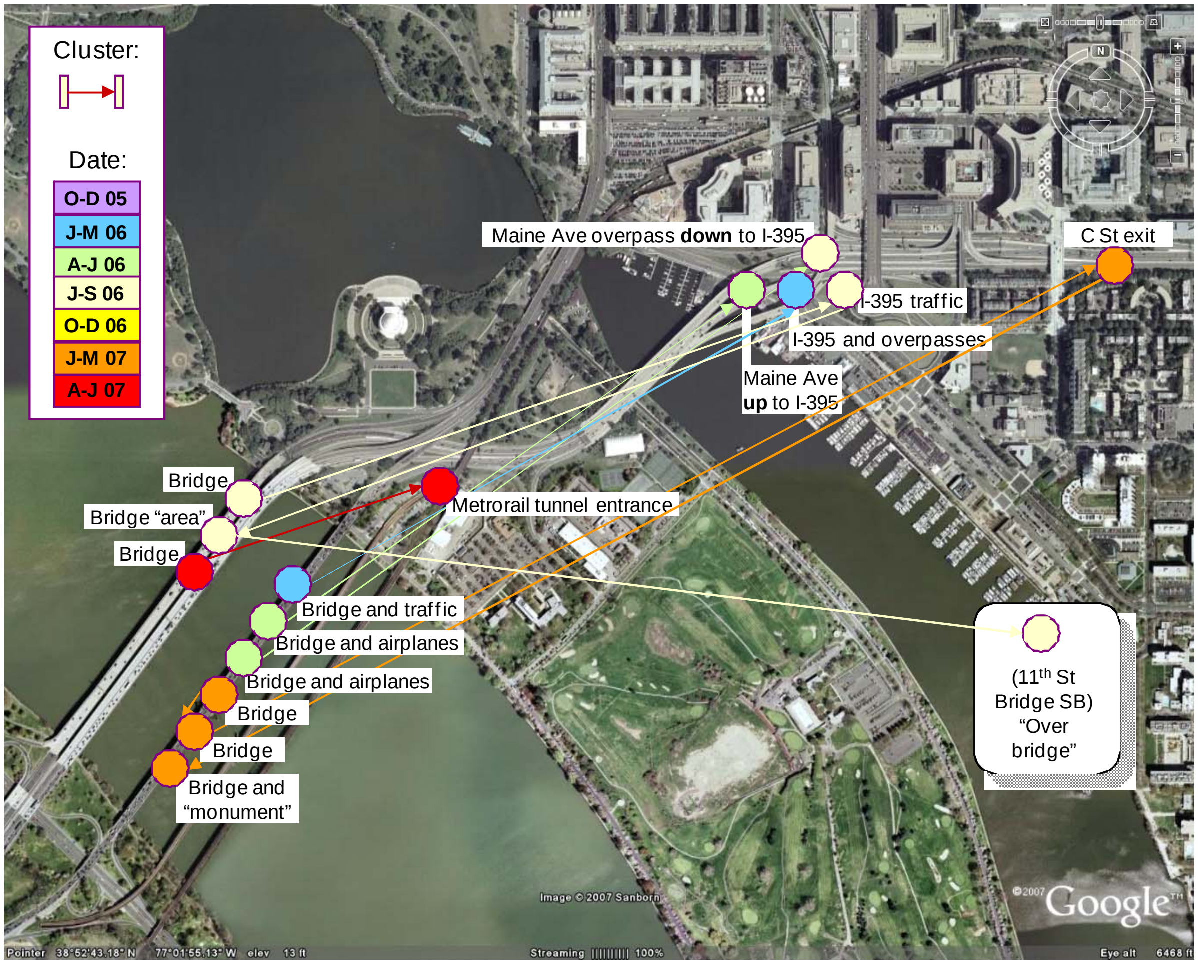
Source: 911 call data provided by the MPD.

Figure 3-14 drills down on these 16 incidents, showing the locations, links with other events in the same cluster, and quarter in which the incidents occurred. The locations for the 14th Street Bridge are staggered to show details, because the records did not provide specific locations on the bridge. Incident locations were plotted manually on an overhead photo of the 14th Street Bridge from Google Earth. The 14th Street Bridge incidents do tend to note that the individual was taking pictures of airplanes and monuments as well as traffic, so tourism may be a possibility, despite the personal risk to the picture taker and the fact that the bulk of the calls were on the northbound span (the southbound span has a pedestrian bridge). During our in-progress review, MPD officials specifically stated that cars do stop on the 14th Street Bridge to take pictures of planes landing at Regan National Airport.

The Maine Avenue overpass incidents, however, appeared to focus on highway infrastructure and traffic. They also effectively covered major features of this area, with one incident focused on the underside of bridge infrastructure, one focused on traffic from the top of the overpass, and several focused on the traffic flows from the sides of I-395. Also of note is the incident reporting filming of the Metrorail tunnel entrance near the 14th Street Bridge.

[3] We reprinted the exact text in the comment fields with the exception of leading spaces, leading periods, and administrative notes.

Figure 3-14. Detailed View of the 14th Street Bridge and Maine Avenue Overpass Incidents



Source: Google Earth.

Table 3-3 provides the cluster, date, location, and comment fields for the 16 incidents. The license plate numbers referenced in the comments have been altered for privacy reasons.

Returning to Figure 3-13, there was one additional group of incidents—those for the Key Bridge near Georgetown. However, we did not rate these as being of significant risk for several reasons. First, most of these calls related to people taking pictures from the local Key Bridge Exxon station, which reduced personal risk. Second, most calls specifically referred to people taking pictures of airplanes overhead, as opposed to traffic or bridge infrastructure. Third, the calls were spread out over time.

Table 3-3. Incidents for the 14th Street Bridge and Maine Avenue Overpass Area

Cluster	Date	Location	Comment Field
1	1/23/2006	14th Street Bridge	LOF... BLACK OR DARK BLUE PT CRUISER WITH MD TAG.,.. TWO GUYS TAKING PICTURES OF THE TRAFFFIC AND THE BRIDGE,, MD TAG ....AAA111 HEADED NORTH ON THE BRIDGE,,
	3/1/2006	I-395 NB at Maine Ave (on I-395)	LOF....2 ASIAN MALES TAKING PICTURES OF THE HIGHWAY AND THE OVER PATHS
2	4/15/2006	14th Street Bridge	DRIVING A LIGHT BEIDGE HONDA/NO TAG NUMBER AVAIL/DK SKINNED MALE/FIREIGNER/PARKED ON RT SIDE OF BRIDGE/COMPL STATES SUBJ WAS TAKING PICTURES PF AIRPLANES AND THE BRIDGE
	4/16/2006	12th Street SW & Maine Ave SW (under I-395)	MALE UNDERNEATH BRIDGE STRUCTURE TAKING PICTURES. MALE WEARING RED SHIRT AND KHAKI COLORED PANTS.
3	5/28/2006	14th Street Bridge NB	2 MIDDLEEASTERN MALES , FILMING THE BRIDGE WITH A CAM CORDER DC TAG # BBB222, SILVER CORILLA //NORTHBOUND// NFI// AND FILMING AIRPLANES
	7/7/2006	I-395 SB at Maine Ave (on overpass)	3 MIDDLE EASTER MALES VIDEO TAPING THE BRIDGE MAINE AVE LOOKING DOWN ONTO I395
4	8/12/2006	14th Street Bridge NB	LOF....LT BLUE FORD EXPEDITION W/MD TAGS STARTS W/CCC.... THE DRIVER IS VIDEO TAPING AS HE WAS DRIVING.....N/F LAST SEEN HEADING INTO DC
	8/21/2006	I-395 NB at Maine Ave (on I-395)	LOF: W/M DARK COLOR SHIRT, UNK PANTS...TAPING TAFFIC ON I395 COMPL STATES HE NEAR OVERPASS FOR MAIN AVE...SUBJ WAS ON FOOT
	8/24/2006	14th Street Bridge	LOF BURGUNDY FORD EXPLORER CC STATES SHE SAW O/M, LSW WHITE TANKT OP, BLUE SHORTS TAKING PICTURES OF THE AREA SUBJS APPEARED TO BE ON 395 SIDE HE FACIGN THE VA SIDE WHEN HE WAS TAKING PICTURES IT ALSO APPEARED A SUBJS HAD A CAST ON ARM VEH PARKED ON THE SHOULDER
	8/26/2006	I-295 SB on 11th St Bridge	LOF...TAN BRONCO......MALE WEARING A ORANGE HAT CALLER STATED THAT HE WAS TAKING PICTURES OVER THE BRIDGE
5	1/23/2007	14th Street Bridge NB	LOF MALE WITH A CAMERA STANDING ON THE BRIDGE INBOUND
	2/28/2007	14th Street Bridge NB	COMPL STATED THAT SUBJ TAKING PICTURE IN THE NORTH BOUND SIDE OF THE BRIDGE.... LOF GRAY OLD MODEL HONDA
	3/2/2007	I-395 NB at Maine Ave (on I-395 itself)	SUBJECT TAKING PICTURES............CALLER UNABLE TO GIVE LOOKOUT........CALLER STATES THAT THE SUBJECT IS NEAR THE C ST EXIT...... 18:16:24 SUBJECT HAS A CAMERA ON A TRIPOD............
	3/9/2007	14th Street Bridge NB	2 MIDDLE EAST PERSON SHOOTIG PICTURE OF GEORGE WASHINGTON BRIDGE AND THE MONUMENT .....FILMING THE AREA ..... SUBJ HEADING TO WASHINGTON, DC....... SUBJ HAS LIGHT GRAY DDD444 VA TAG VEH.......VEH MAKER UNK........ L/S HEADING TO DC....

(continued)

Table 3-3. Incidents for the 14th Street Bridge and Maine Avenue Overpass Area (continued)

Cluster	Date	Location	Comment Field
6	4/6/2007	14th Street Bridge SB	2 MIDDLE EASTERN LOOKING MALE TAKING PICTURE OF THE BRIDGE SUBJECT IN A SILVER COLOR MITS MONT LATE MODLE TAG NUMBER EEE555 TAG STATES UNKNOW COLOR OF TAG BLUE AND ORANGE VEH LAST SEEN GOING TOWARD VA
	4/11/2007	I-395 NB at Maine Ave (near entrance to Metrorail Tunnel in Potomac Park)	NEAR POTOMAC PARK VIDEO TAPING WHERE THE SUBWAY GO UNDERGROND LOF W/M DARK GREEN SWEATER UNKNOWN PANTS DESCRIPTION

Source: 911 call data provided by the MPD.

Outside of the downtown area, there was one cluster of incidents worth mentioning, which involved two incidents involving potential surveillance of Sibley Memorial Hospital. The incidents may involve the same woman, who in one case was taking pictures of Sibley Memorial's chemical facility. Table 3-4 provides details about these two incidents. As with the man taking pictures near I-395's northern exits, the risk of this cluster is reduced by its age; both incidents took place in October and November 2005.

Table 3-4. Incidents of Taking Pictures at Sibley Memorial Hospital

Date	Location	Comment Field
10/1/2005	5900 MacArthur Blvd NW	** LOI search completed at 10/06/05 12:04:26 COMPL STATES FEMALE DRIVING A CHAMPAIGNE COLOR MERCURY SABLE WITH MD TAG# MJD286 A TAKING PICTURES OF THE BUILDING.
11/1/2005	5201 Little Falls Rd NW	SOP. OBSERVED LADY TAKING PICTURES OF CHEMICIAL AREA ** LOI search completed at 11/11/05 13:08:07 COMPL. WILL MEET POLICE AT GATE// LOF. W/F 110LBS//5'3// GLASSES SUBJ. WAS IN BLACK SUV PASSENGE// WEARING WHITE SHIRT// BLUE JEANS//

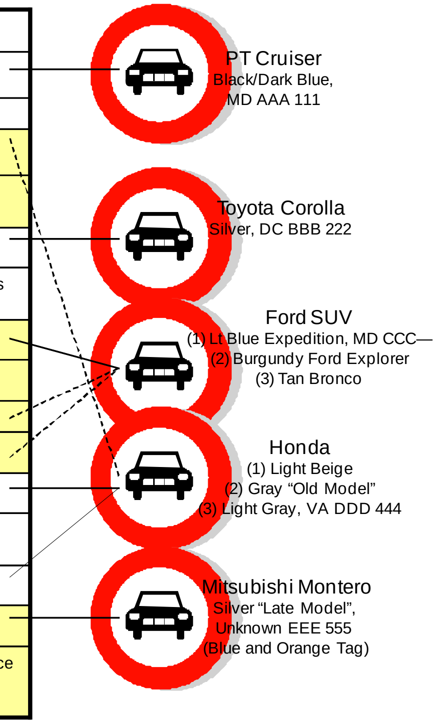
Source: 911 call data provided by the MPD.

3.6 Findings Supporting Follow-Up Investigations

Some of the 911 call records directly support follow-up investigations. In particular, a number of comment fields for calls on the 14th Street Bridge provided at least partial license tag information, along with descriptions of vehicles, suggesting that the same vehicle might have been in multiple incidents. (There were no tags provided for calls for the Maine Avenue overpass area.) Figure 3-15 matches vehicle descriptions and tags to incidents; solid lines are likely matches and dashed lines are uncertain matches (for example, match of general vehicle type but different color or model). The actual tag data has been obscured for privacy reasons.

Figure 3-15. License Tag Data and Model Descriptions from Potential Surveillance Calls

Cluster	Date	Location	Target
1	1/23/2006	14th Street Bridge	Traffic and bridge
	3/1/2006	I-395 NB at Maine Ave (on I-395)	Highway and overpass
2	4/15/2006	14th Street Bridge	Airplanes and the bridge
	4/16/2006	12th Street SW & Maine Ave SW (under I-395)	Underside of bridge structure
3	5/28/2006	14th Street Bridge NB	Bridge and airplanes
	7/7/2006	I-395 SB at Maine Ave (on overpass)	I-395 traffic from the overpass
4	8/12/2006	14th Street Bridge NB	Bridge and traffic
	8/21/2006	I-395 NB at Maine Ave (on I-395)	I-395 traffic
	8/24/2006	14th Street Bridge	“Area”
	8/26/2006	I-295 SB on 11th St Bridge	“Over the bridge”
5	2/28/2007	14th Street Bridge NB	Bridge
	3/2/2007	I-395 NB at Maine Ave (on I-395 itself)	Traffic from camera on tripod
	3/9/2007	14th Street Bridge NB	Bridge and monuments
6	4/6/2007	14th Street Bridge SB	Bridge
	4/11/2007	I-395 NB at Maine Ave (near entrance to Metrorail Tunnel in Potomac Park)	Potomac Park subway entrance



Source: 911 CFS data provided by MPD.

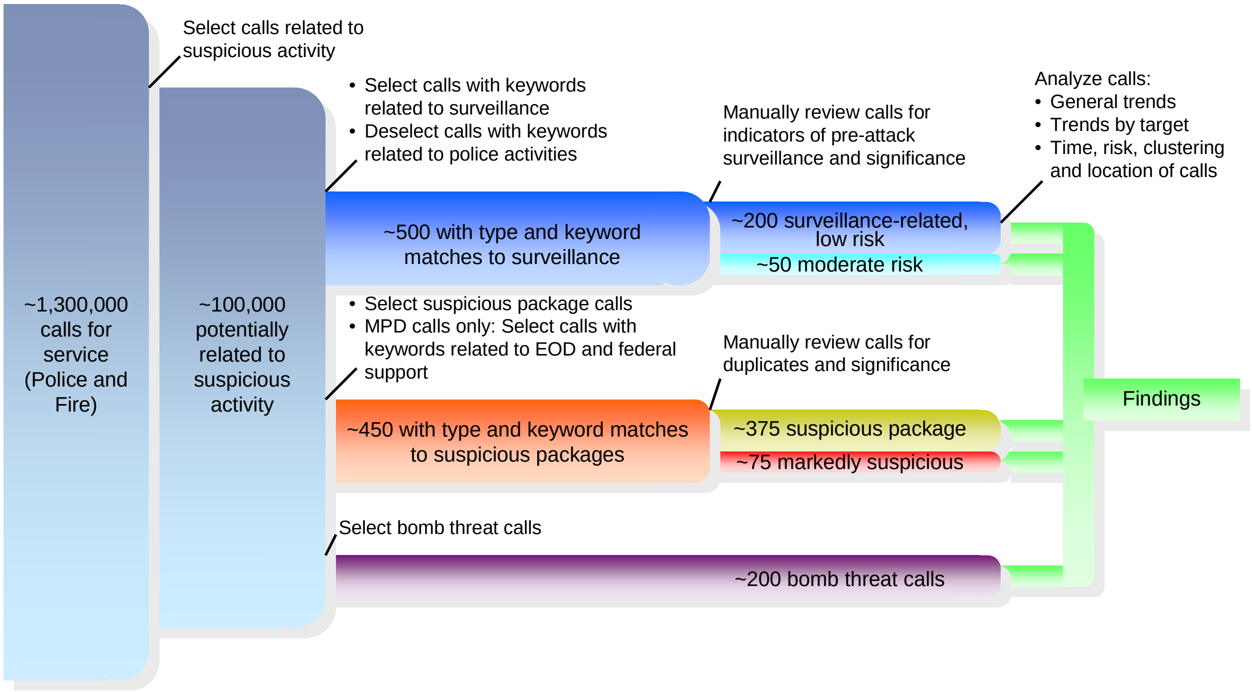
Analysis of Potential Preoperational Incidents

The second analysis examined multiple types of calls potentially related to preoperational activity. These include the aforementioned potential surveillance calls, bomb threat calls, and suspicious package calls.

4.1 Methods

The processes largely duplicated those used for potential surveillance calls on multiple types of calls. Figure 4-1 summarizes the processes employed.

Figure 4-1. Methods for Analyzing Multiple Types of Calls


~1,300,000 calls for service (Police and Fire)
Select calls related to suspicious activity
~100,000 potentially related to suspicious activity
• Select calls with keywords related to surveillance
• Deselect calls with keywords related to police activities
~500 with type and keyword matches to surveillance
Manually review calls for indicators of pre-attack surveillance and significance
~200 surveillance-related, low risk
~50 moderate risk
• Select suspicious package calls
• MPD calls only: Select calls with keywords related to EOD and federal support
~450 with type and keyword matches to suspicious packages
Manually review calls for duplicates and significance
~375 suspicious package
~75 markedly suspicious
Select bomb threat calls
~200 bomb threat calls
Analyze calls:
• General trends
• Trends by target
• Time, risk, clustering and location of calls
Findings

EOD = explosive ordnance demolition; MPD = Metropolitan Police Department.

For this analysis, we worked with two sets of 911 calls—those forwarded to the MPD and those forwarded to DCFEMS. We examined multiple types of 911 CFS from October 2005 through June 2007 to find the counterterrorism-relevant calls, including the following:

- Potential surveillance calls (presented earlier). These calls were strictly in the MPD set.
- Bomb threat calls. These had a unique type code and were directly extracted. Again, these calls were strictly in the MPD set.

- Suspicious package calls. The bulk of these were in the MPD data set, where they all had a specific type code. A smaller number were in the DCFEMS data set, where they had one of multiple type codes.

Because bomb threat calls were directly extracted (there were comparatively few of these), most filtering work was done on suspicious package calls. We first reviewed about 100 MPD suspicious package comments in the MPD data set. Only a small portion of these records appeared to be genuinely suspicious, relating to cases in which explosive ordnance demolition (EOD) teams or another government agency was called in, a bomb-sniffing dog detected explosives, or a case number was assigned. Therefore, to filter the over 1,500 suspicious package calls in the MPD data set, we extracted calls containing key strings Case, EOD, K9, FBI, SECRET (for Secret Service), or CAPITOL (for Capitol Police).

There were many fewer suspicious package calls in the DCFEMS data set, which appeared to relate to calls in which the specialized fire department teams were called in. We therefore extracted calls with types of HAZMAT—Suspicious Package, HAZMAT—Suspicious Letter, or HAZMAT—White Powder. While the DCFEMS calls did have other HAZMAT types, upon review, these others related to routine chemical spills or leaks and did not appear relevant.

We then manually reviewed the records, eliminating drills and cases where the package was clearly not suspicious after examination; the most frequent disqualifier was “Good Intent,” or descriptions of a person returning to pick up a forgotten package. We also looked for duplicates between MPD and DCFEMS records, because the MPD informed us that suspicious package calls can have two records if handled by both agencies. We identified 47 duplicate cases, 17 of which took place around the White House.

We used a simple two-level framework to characterize the risk level of the remaining packages. We characterized about one-sixth of the packages as “markedly suspicious.” These were packages that appear to have been deliberately planted or mailed or have another significant reason to suspect them. Markedly suspicious packages included one or more of the following descriptions in their comment fields:

- Suspect seen deliberately leaving the package
- Assemblies of material taped or glued together
- Covered with postage or tape
- Protruding or taped wires or fuses
- Wrapped in plastic (This category refers to a package tightly wrapped in sheets of plastic, not items in plastic bags.)
- Ticking, alarmed, or otherwise making suspicious noises
- Reported as looking like ordnance or a bomb
- Stains or leaks

- Concerning messages: “to” public figures, or “strange” messages
- Contains white powder (This category refers specifically to instances when white powder was placed directly in an envelope or package or specifically left in an area. It does not refer to instances of someone just happening across “white powder” on the ground.)
- Contains inflammable gas or liquid
- Identified as suspicious by a bomb-sniffing dog
- Identified as suspicious by a chemical/biological agent sensor
- Person made threats about packages later found
- Molotov cocktail
- Details about the package unspecified, but resulted in a major response or linked to other suspicious packages

Other suspicious package calls generally lacked much description or information about the results of the investigation. While many calls noted that the package had been “cleared,” this was insufficient to say that the package was definitely benign (e.g., left by accident, fell off a vehicle) because the fact the package contained no explosives did not mean it was not placed for threatening or probing purposes. Of all the suspicious package calls, only one appears to have been an actual weapon—a single Molotov cocktail.

The filtering processes resulted in a total of 850 calls, including 218 bomb threats, 79 markedly suspicious packages, 376 suspicious packages, 43 potential surveillance calls of moderate risk (rated 4 to 6) and 134 potential surveillance calls of low risk (rated 0 to 3). Following the filtering processes, we graphed the numbers of incidents by type of location and prepared trend charts to identify those types of location seeing recent increases in activity. We also identified clusters of incidents at individual locations.

4.2 Characterization of Markedly Suspicious Packages

It is worth examining the markedly suspicious packages in some detail. Figure 4-2 breaks down the number of suspicious packages by type. By far the largest number of incidents concerned packages with white powder in them, distantly followed by reports of people deliberately leaving packages. There were also significant numbers of hits by bomb-sniffing dogs, packages with strange or threatening messages, and packages with what looked like wires or fuses. There were only one or two examples of other types of markedly suspicious packages.

Out of the markedly suspicious packages, we have extracted the 10 that we believe are most suspicious. These are described in Table 4-1.

Figure 4-2. Breakdown of Markedly Suspicious Packages

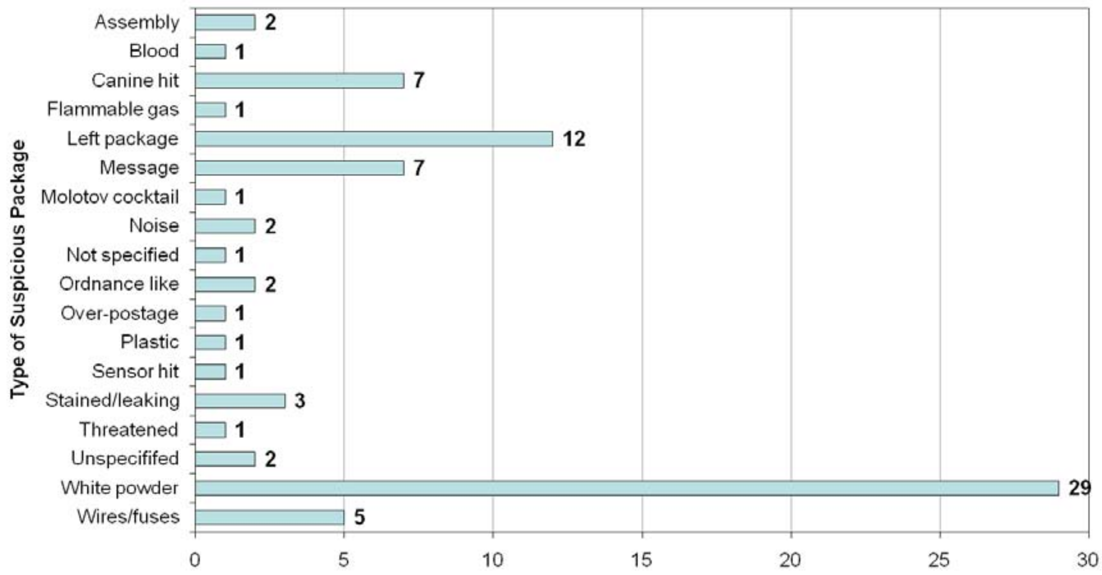


Table 4-1. Ten "Extremely Suspicious" Packages

Date	Location	Summary
10/10/2005	Connecticut Ave & McKinley Ave NW	Man deliberately left suitcases at M&T Bank, CVS, and bus stop
11/30/2005	740 15th St NW	Received letter with "blood looking substance" in it
5/04/2006	DC Armory	Bottle wrapped in black tape with brown cord coming from bottom
9/22/2006	Post Office (3370 V St NE)	Envelope with white powder and anthrax threats
10/11/2006	IRS (1111 Constitution Ave NW)	Book bag deliberately left by driver of gold van
12/06/2006	DC Public Health Commission (1875 Connecticut Ave NW)	6-inch pipe with wires wrapped around it
12/08/2006	Related events: Fairchild Building (50 E St SW) and Union Station	Fairchild Building call unspecified, but resulted in HAZMAT team having to "suit up" to investigate it; linked with "something else" around Union Station. Presumably the two other suspicious package calls at Union Station on 12/8/2006.
1/5/2007	Iraq Chancery (1801 P St NW)	Molotov cocktail
1/22/2007	Congressional Offices (430 S Capitol St SE)	Multiple nested envelopes; inner white envelope contained a pill bottle (handled similar to white powder envelope)
6/01/2007	Psychiatric Institute of Washington (4228 Wisconsin Ave NW)	Caller overheard man on Metrobus talk about planting explosives in bathrooms at this location; "call type changed from 1089 to suspicious package"

Source: 911 call data provided by the MPD.

Of these 10 packages, the most notable are the Molotov cocktail at the Iraq Chancery and the package at the Fairchild Building. The Molotov cocktail was the only genuine explosive weapon reported in all of the suspicious package data. The package at the Fairchild Building was the only incident that was linked to other suspicious package calls (two at Union Station).

4.3 Characterization of Calls, by Type of Location

Figure 4-3 shows the total numbers of calls by quarter. Except for a significant drop in activity between January and March 2006, the figure shows a slight but steady decline in activity between October 2005 and June 2007. There have been no major changes in the proportion of each type of call.

Figure 4-3. Calls, by Quarter

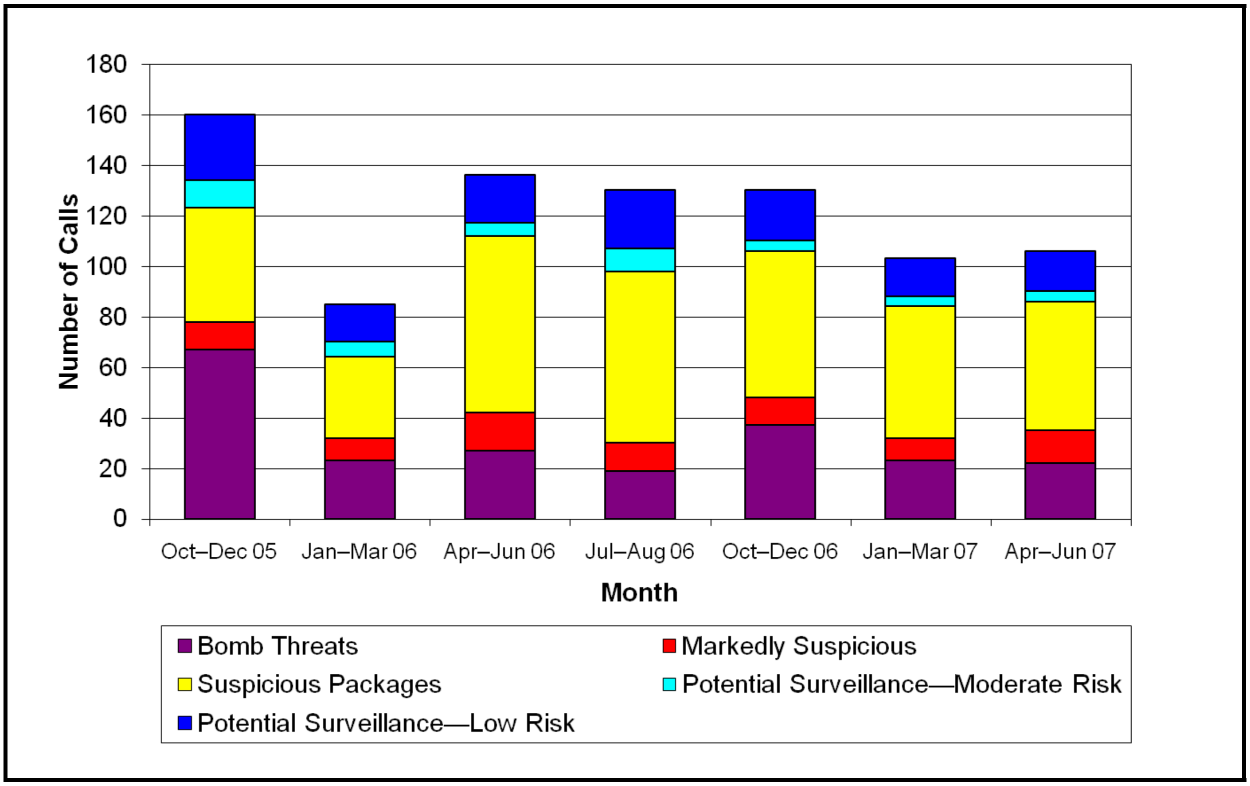
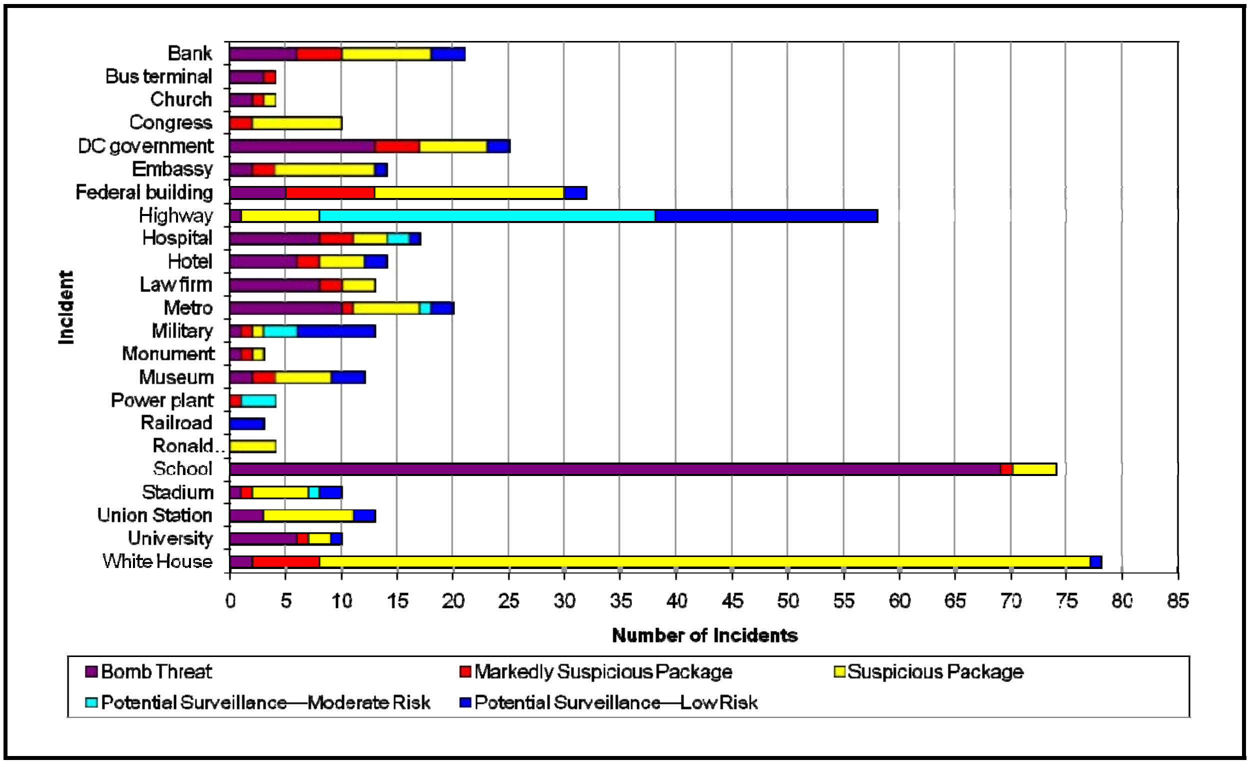


Figure 4-4 shows the numbers of potential surveillance, bomb threat, and suspicious package calls by type of location. Here, we focus on locations with a definite type, including infrastructure, government buildings, public facilities, and landmarks. Standard office buildings, residences, unspecified locations, and packages left out in the open are not included in Figure 4-4; altogether, these "generic" locations accounted for 69 bomb threat calls, 35 markedly suspicious packages, 205 suspicious packages, 3 potential surveillance calls of moderate risk, and 82 potential surveillance calls of low risk.

Figure 4-4. Incidents, by Type of Location



The graph is dominated by three location types: highways, schools, and the White House, each of which in turn is dominated by a single call type. Most highway calls were for potential surveillance, most school calls were for bomb threats, and most White House calls were for suspicious package calls. With the latter, the calls recorded MPD and DCFEMS routinely being called to assist the Secret Service with packages on or near White House grounds, the bulk of which seem to have been left by accident. The few markedly suspicious package calls related to hits by bomb-sniffing dogs.

Also of interest are the types of locations with 10 or more calls, including the following:

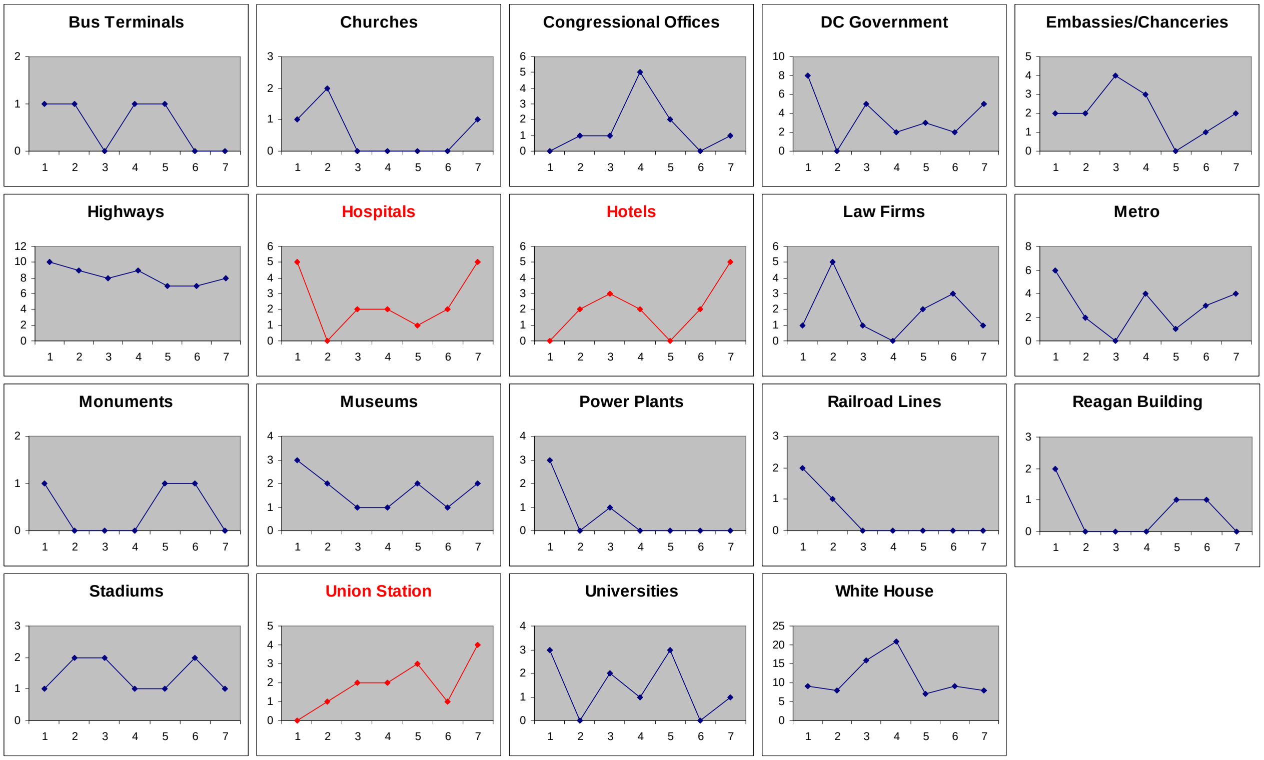
- banks
- congressional buildings (Note that the number of calls for congressional buildings was far less than it was for the White House; we assume this is due to the Capitol Police handling the bulk of incidents themselves.)
- Washington, D.C., government buildings, including government centers, fire stations, police stations, and courthouses
- embassies
- federal buildings
- hospitals

- hotels
- law firms
- Metro, including Metrorail and Metrobus
- military facilities
- museums
- stadiums and convention centers
- Union Station
- universities

All of these tended to have a mixture of calls and, in most cases, were fairly distributed across different locations. For example, for hotel calls, only one hotel (Renaissance Mayflower) had more than one call. We examine clusters of incidents at specific locations within these categories in the next section.

Figure 4-5 shows a panel of trend charts for each type of location, by quarter. Only three types have seen increases in calls: hotels, hospitals, and Union Station. The wide distribution of hotel calls tends to lower the significance of the increase in hotel calls. The hospital calls were concentrated at three hospitals, Providence, Sibley Memorial, and Washington Hospital Center. Hospital and Union Station calls will be examined in the next sections.

Figure 4-5. Trend Charts for Each Type of Location



4.4 Clusters of Incidents

Figures 4-6 through 4-9 list all locations that had more than one call. The first figure lists locations with multiple calls for banks, Washington, D.C., government, embassies, and federal buildings. Of note are two markedly suspicious packages at ATI Afribank (one of which was a white powder envelope), four bomb threats against the DC Public Safety Communications Center, and the aforementioned concentration of suspicious package calls at the White House.

Figure 4-6. Clusters of Incidents for Banks, DC Government, Embassies, and Federal Buildings

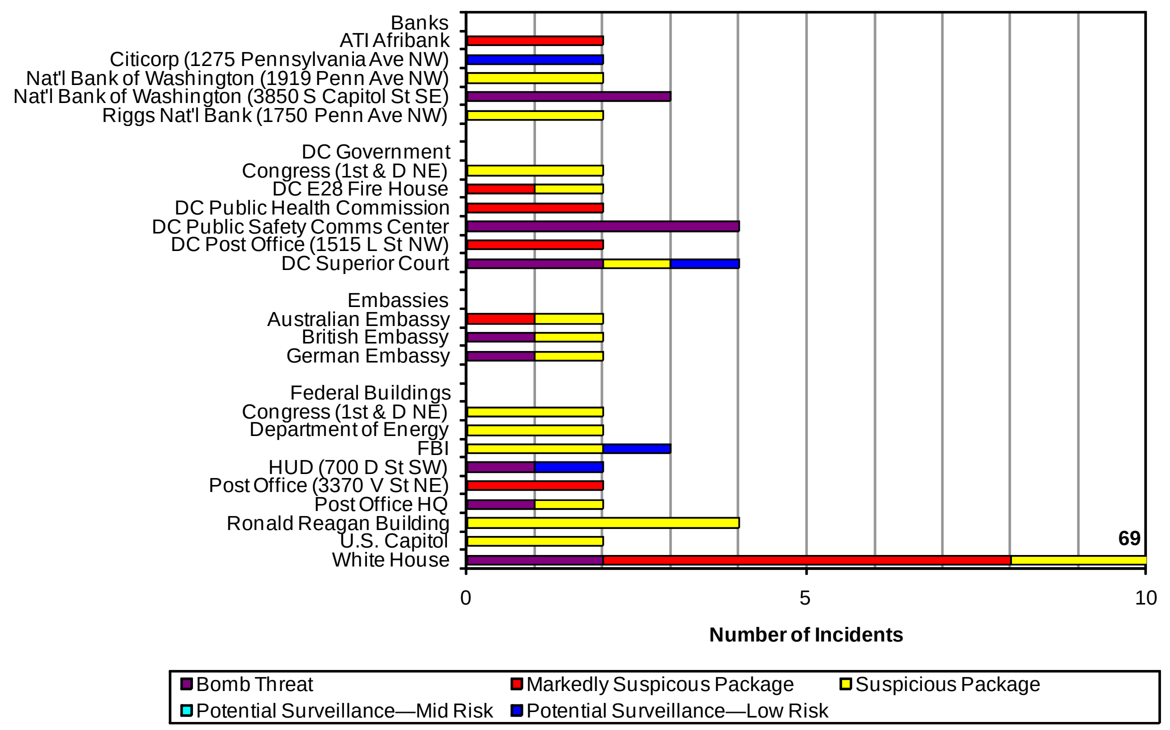


Figure 4-7 lists multiple call locations for highways, hospitals, hotels, and law firms. The large number of potential surveillance calls for highways was discussed in Section 3, as were the potential surveillance calls for Sibley Memorial Hospital. Of note are the concentrations of bomb threats at Providence Hospital and Washington Hospital Center, with the latter also having a markedly suspicious package addressed to "Department of Justice." Two law firms have seen significant numbers of calls, with Venable LLP seeing five bomb threats. As noted, the Renaissance Mayflower is the only hotel to have more than one call; the markedly suspicious package was for an item that looked like it had a fuse attached to it.

Figure 4-7. Clusters of Incidents for Highways, Hospitals, Hotels, and Law Firms

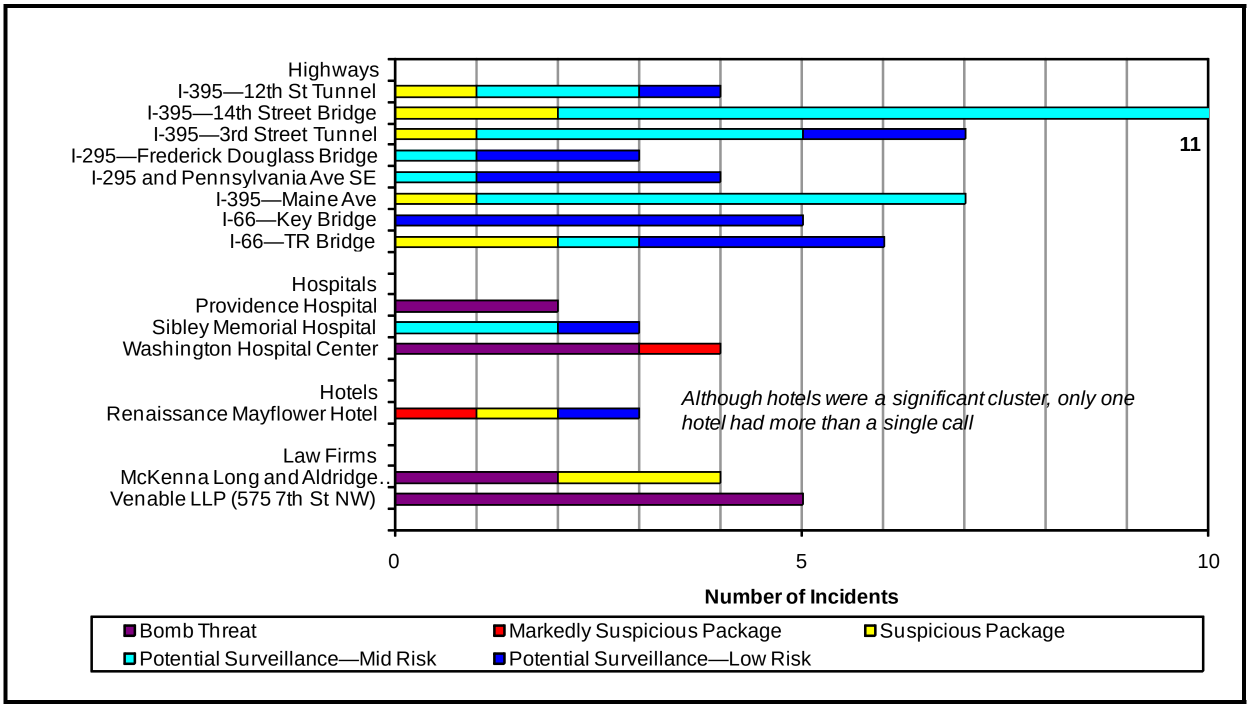
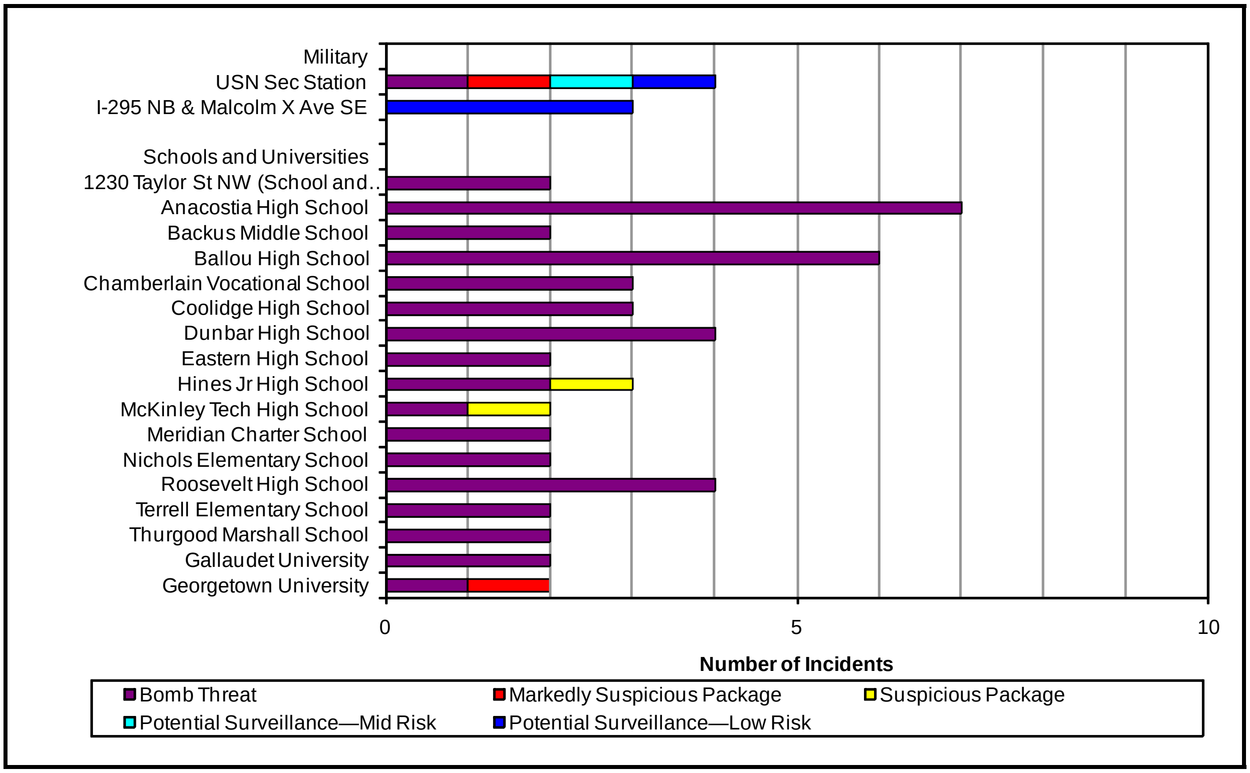


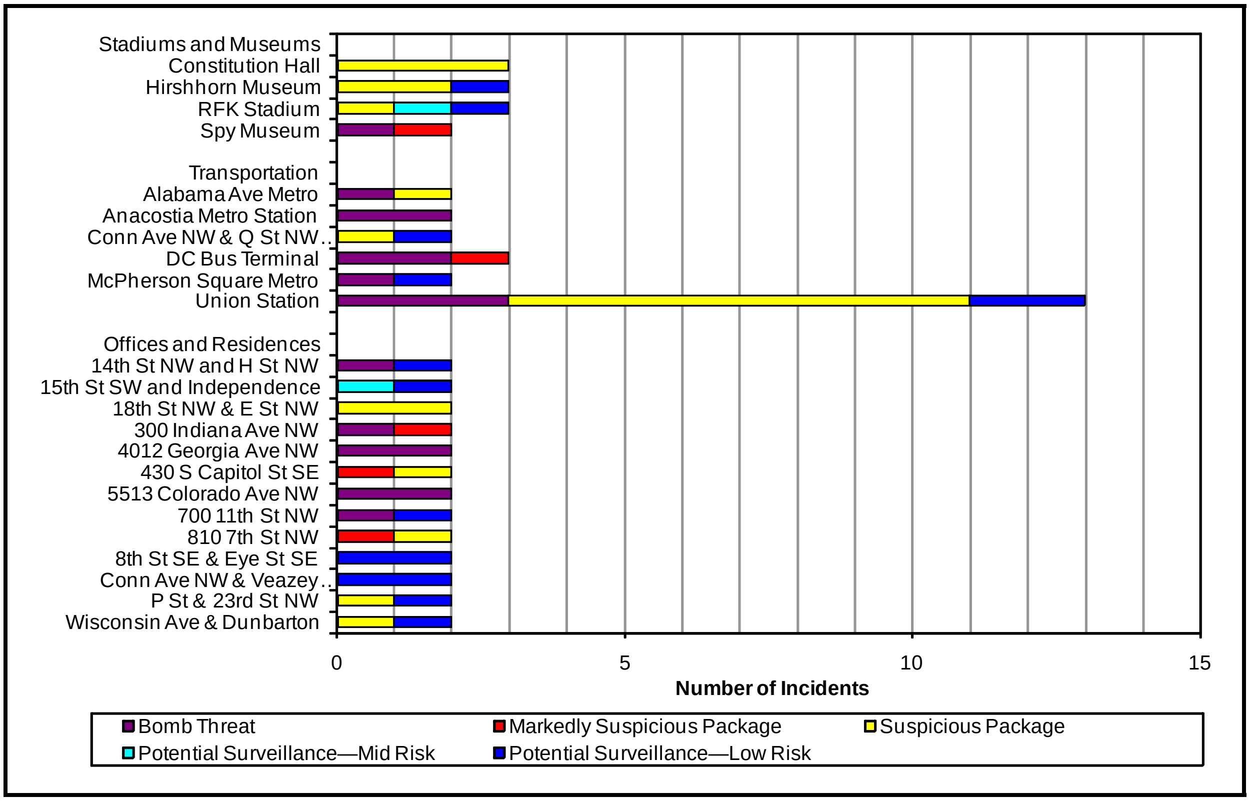
Figure 4-8 lists multiple call locations for military facilities, schools, and universities. This figure clearly shows the dominance of bomb threat calls for schools. Many of the comment fields for these calls imply that the calls are being made by children, likely students at the schools.

Figure 4-8. Clusters of Incidents for Military Facilities, Schools, and Universities



Finally, Figure 4-9 lists multiple call locations for stadiums and museums, transportation-related locations, and otherwise unspecified offices and residences. The figure is dominated by the calls at Union Station, which include a mix of suspicious package calls, potential surveillance calls, and bomb threats.

Figure 4-9. Clusters of Incidents for Stadiums, Museums, Transportation Locations, Offices, and Residences



Given both the number and trend of calls for Union Station, we drilled down on these calls to get more detail. Table 4-2 summarizes the calls for Union Station. While many of these calls appear to be left luggage or crank calls, some appear to be of concern. Of particular interest are two suspicious package calls linked to a highly suspicious package call for the Fairchild building, mentioned earlier. Also of note is a report of an older male taking pictures of buses at Union Station.

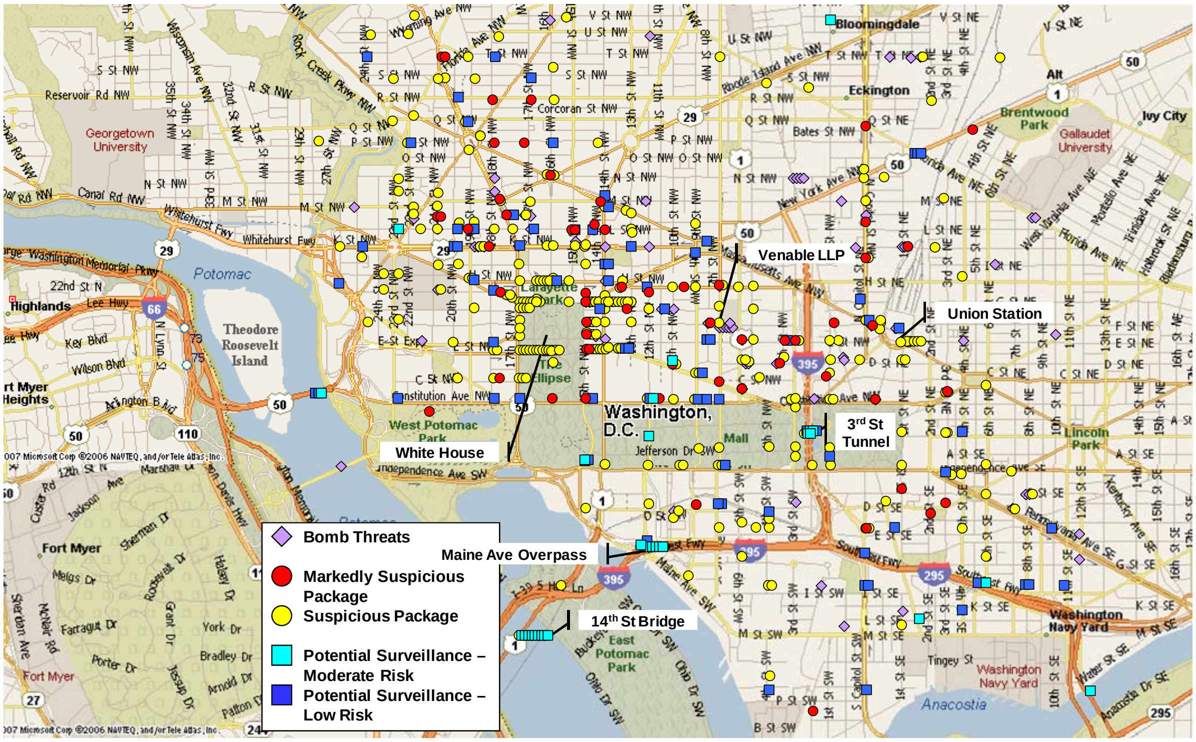
Table 4-2. Calls for Union Station

Date	Call Type	Summary
3/3/2006	Suspicious package	Six unspecified packages (handled by Capitol Police)
4/4/2006	Bomb threat	Bomb threat from possibly intoxicated person
4/21/2006	Suspicious package	Two pieces of luggage left unattended
8/10/2006	Suspicious package	Unspecified
9/21/2006	Suspicious package	Briefcase left unattended
10/23/2006	Potential surveillance	Black Escalade videotaping Thurgood Marshall Judiciary Building from Union Station parking area
12/8/2006 (two calls)	**Cluster of suspicious packages**	**Two calls for unspecified packages in support of Capitol Police. Appears linked to Fairchild Building (50 E St SW) call that resulted in HAZMAT team needing to "suit up"**
3/3/2007	Bomb threat	Male: "There is a bomb threat in Union Station"
4/10/2007	Bomb threat	Male caller stated "he don't like police—bomb planted in bottom of Union Station where the food at"
4/23/2007	**Potential surveillance**	**Older male taking pictures of buses**
5/10/2007	Suspicious package	Black suitcase left unattended
6/12/2007	Suspicious package	Unspecified

Source: 911 call data provided by the MPD.

Finally, Figure 4-10 provides a map of all calls for downtown Washington, D.C. The mapping technique is the same used in the last chapter—Microsoft Excel plots of the calls' SPCS coordinates manually fitted onto a Microsoft Expedia map of the downtown area. Calls having the same address are shifted slightly to the east so that multiple calls for the same location appear as a stack of points. Figure 4-10 calls out those locations with the greatest numbers of calls (five or more at a single location): the White House, 14th Street Bridge, Maine Avenue overpass, Union Station, and Venable LLP.

Figure 4-10. Plot of All Calls in the Downtown Washington, D.C., Area



Source: Microsoft Expedia.

Other than highlighting the clusters of incidents previously discussed, Figure 4-10 does not show any new major clusters of activity. The earlier pattern of having incidents fairly well distributed throughout the downtown area, with heavier concentrations around the K-Street/White House area, applies to all calls, as well.

Locations of Interest

The prior analyses highlight certain areas of interest that have a higher number of relevant incidents, markedly suspicious incidents, or both. In Table 5-1, we identify "locations of interest" meeting one or more of the following criteria:

- Having five or more potential surveillance, suspicious package, or bomb threat incidents. We make exceptions for suspicious packages at the White House and bomb threats against schools; these events were too frequent to be able to differentiate actual risks from continuous calls about trash and left personal effects (White House) or student pranks (schools).

- Having two potential surveillance risks of moderate risk (rated as 4 to 6) or two markedly suspicious packages. The exception to the latter were post offices, as packages with white powder or other markedly suspicious attributes appeared to have been for unspecified addressees rather than the post office.

- Having a cluster of incidents within one of the three of 23 types of locations that have actually seen increases in activity between 2005 and 2007—hospitals, hotels, and Union Station.

- Having highly atypical incidents outside of the above criteria. These include the one suspicious package that was actually a weapon, the two locations with four bomb threats outside of schools, and the one set of linked suspicious packages.

Within Table 5-1, locations are listed by the number of incidents, in reverse order.

Table 5-1 is set up as a table of hypotheses in that it lists the locations of interest along with arguments for and against hypotheses that particular locations are actually the target of preoperational activities. The table also includes a column for actions, or the next steps to test whether the hypotheses are correct. The primary action for all incidents is "Backsweep for related incidents." Introduced in Hollywood et al. (2004), backsweeping refers to extracting information related to locations of interest that were filtered out previously. For this report, we extracted all suspicious person/vehicle, suspicious package, and bomb threat 911 call records for the locations of interest. We did not consider "investigate the trouble" and "other" calls, given the very low numbers of these calls potentially relevant to counterterrorism.

Table 5-1. Initial Table of Hypotheses for Locations of Interest

Location	Arguments for	Arguments against	Actions
1a. I-395: 14th Street Bridge and Maine Avenue Overpass	▪ 16 potential surveillance calls in six clusters ▪ Appears highly atypical; some personal risk involved ▪ Disruption to this area would have major consequences	▪ Stopped cars more likely to be noticed ▪ Could be tourism of airplanes and Washington, D.C., landmarks, especially on 14th Street Bridge	Backsweep for related events
1b. I-395: Maine Avenue Overpass (in isolation)	▪ 6 potential surveillance calls that sweep area from multiple perspectives ▪ Seemingly lacks tourism explanations	▪ Stopped cars and people more likely to be noticed ▪ Could be tourism or work related	Backsweep for related events
1c. I-395 northern exits	▪ 5 seemingly related calls of a man taking pictures of traffic	▪ Incidents are old—last was January 2006	Backsweep for related events
2. Union Station	▪ 13 incidents, 5 in 2007 ▪ Seen increased activity ▪ Only instance of linked suspicious packages (twice at Union Station, once at Fairchild Building)	▪ Natural location to leave luggage ▪ Some bomb threats appear to be crank calls	Backsweep for related events
3. Bolling AFB/ Naval Station	▪ 7 potential surveillance calls	▪ Stopped cars and people more likely to be noticed ▪ Calls covered a large area; significant uncertainty in what was actually being surveyed	Backsweep for related events
4. Venable LLP	▪ 5 bomb threat calls	▪ Bomb threats have limited preoperational value ▪ Threats may be from disgruntled clients	Backsweep for related events
5. DC Public Safety Service Center	▪ 4 bomb threat calls	▪ Bomb threats have limited preoperational value	Backsweep for related events
6. Sibley Memorial Hospital	▪ 3 potential surveillance calls; 2 in one cluster involving chemical plant	▪ Surveillance activity not repeated recently	Backsweep for related events
7. Mayflower Hotel	▪ 3 incidents, including a markedly suspicious package and a person taping the hotel (including the loading dock) in June ▪ Seen increased activity for hotels	▪ Incidents do not appear directly related	Backsweep for related events

(continued)

Table 5-1. Initial Table of Hypotheses for Locations of Interest (continued)

Location	Arguments for	Arguments against	Actions
8. Washington Hospital Center	▪ Markedly suspicious package addressed to “Department of Justice” (April 07), followed by a bomb threat (June 07) ▪ Seen increased activity for hospitals	▪ Not clear if incidents have preoperational value	Backsweep for related events
9. ATI Afribank	▪ 2 markedly suspicious packages, 1 involving white powder, 1 leaking oil	▪ Incidents do not appear directly related	Backsweep for related events
10. DC Public Health Commission	▪ 2 markedly suspicious packages, 1 involving brown powder, 1 a pipe with wires wrapped around it	▪ Incidents do not appear directly related	Backsweep for related events
11. Iraq Chancery	▪ Molotov cocktail—only weapon found ▪ Natural target because of war	▪ Only one incident	Backsweep for related events

Table 5-2 shows the results of backsweeping through the suspicious person/vehicle, suspicious package, and bomb threat calls. While backsweeping did find additional incidents for many locations of interest, in most cases the incidents were low risk, including suspicious packages that were likely trash or left luggage, or potential surveyors who were probably vagrants rather than surveyors. The notable exception was on the 14th Street Bridge, where backsweeping produced three additional markedly suspicious incidents. Two of these involved activities on the Potomac River, and the third involved two people in one of the bridge control towers, “wearing all black with black skull caps.”

Table 5-2. Results of Follow-Up Actions

Location	Results
1a. I-395: 14th Street Bridge and Maine Avenue Overpass	▪ Found 11 incidents on 14th Street Bridge – Markedly suspicious package: shackles with attached line hanging from bridge (10/31/2005) – Potential surveillance, mid risk: two people in tower on bridge, wearing all black (4/26/2006) – Potential surveillance, mid risk: two rowboats tied to bridge, with rowers “doing work” (1/2/2007) – 4 potential surveillance, low risk – 4 suspicious packages
1b. I-395: Maine Avenue Overpass (in isolation)	▪ 1 new potential surveillance, low risk ▪ 2 new suspicious packages
1c. I-395 northern exits	▪ 1 potential continuation of cluster—man w/bags “messing with something” behind barrier in 3rd Street Tunnel (3/25/2006) ▪ 5 new potential surveillance, low risk, appear unrelated to cluster ▪ 12 new suspicious packages
2. Union Station	▪ Markedly suspicious package: 1 canine hit on a vehicle (12/2/2006) ▪ 1 new potential surveillance, low risk ▪ 10 new suspicious packages
3. Bolling AFB/Naval Station	▪ 7 new potential surveillance, low risk ▪ 1 new suspicious package
4. Venable LLP	▪ 2 additional bomb threat calls
5. DC Public Safety Service Center	▪ No new calls
6. Sibley Memorial Hospital	▪ No new calls
7. Mayflower Hotel	▪ 1 new suspicious package
8. Washington Hospital Center	▪ 2 new suspicious packages
9. ATI Afribank	▪ No new calls
10. DC Public Health Commission	▪ No new calls
11. Iraq Chancery	▪ No new calls

Finally, Table 6-3 updates Table 6-1 with the results of the follow-up activities. We have reordered the locations of interest to reflect the numbers of incidents discovered during backsweeping. Under Actions, we assign one of two recommendations: (1) focus for those locations we believe warrant follow-up monitoring and analysis efforts and (2) increase attention for those locations warranting increased attention but not dedicated focus efforts.

Table 5-3. Revised Table of Hypotheses for Locations of Interest

Location	Arguments for	Arguments against	Actions
1a. I-395: 14th Street Bridge and Maine Avenue Overpass	▪ 32 incidents in all, 22 on bridge itself ▪ 16 potential surveillance calls for taking pictures and filming in six clusters; some personal risk involved ▪ Other notable calls for – Two persons wearing black clothes and black skull caps in one of the bridge towers – Persons "working" on the bridge from rowboats; call comments read that neither DC nor Arlington knew why they were there – Leaving shackles with a line connected to them hanging from the bridge ▪ Disruption to this area would have major consequences	▪ Stopped cars and people more likely to be noticed ▪ Could be tourism of airplanes and Washington, D.C., landmarks, especially on 14th Street Bridge	Focus
1b. I-395: Maine Avenue Overpass (in isolation)	▪ 10 calls for just this area ▪ 6 potential surveillance calls that sweep area from multiple perspectives ▪ Seemingly lacks tourism explanations	▪ Stopped cars and people more likely to be noticed ▪ Could be tourism or work related	Focus
1c. I-395 northern exits	▪ 29 calls for northern tunnels and related on-ramps—16 potential surveillance, 13 suspicious package ▪ 5 seemingly related calls of a man taking pictures of traffic; one potentially related call of a man with bags "messing with something" in the 3rd Street Tunnel	▪ Stopped cars and people more likely to be noticed ▪ Many packages could be trash or fallen luggage ▪ Incidents from cluster are old—last was March 2006	Increased attention
2. Union Station	▪ 26 incidents, 9 in 2007; seen increased activity ▪ Only instance of linked suspicious packages (twice at Union Station, once at Fairchild Building, 12/8/2006)	▪ Over half are for suspicious packages; natural location to leave luggage ▪ Some bomb threats appear to be crank calls	Focus
3. Bolling AFB/Naval Station	▪ 14 potential surveillance calls in this area	▪ Stopped cars/people more likely to be noticed ▪ Uncertainty in what was actually being surveyed; reports covered a wide area ranging from the 11th Street Bridge to the Naval Research Laboratory	Increased attention

(continued)

Table 5-3. Revised Table of Hypotheses for Locations of Interest (continued)

Location	Arguments for	Arguments against	Actions
4. Venable LLP	▪ 7 bomb threat calls	▪ Bomb threats have limited preoperational value ▪ Threats may be from disgruntled clients	Increased attention
5. Washington Hospital Center	▪ 6 calls total; includes markedly suspicious package addressed to “Department of Justice” (April 07), followed by a bomb threat (June 07) ▪ Seen increased activity for hospitals	▪ Not clear if incidents have preoperational value	Focus
6. Mayflower Hotel	▪ 4 incidents, including a markedly suspicious package and a person taping the hotel (including the loading dock) in June ▪ Seen increased activity for hotels	▪ Incidents do not appear directly related	Focus
7. DC Public Safety Service Center	▪ 4 bomb threat calls	▪ Bomb threats have limited preoperational value ▪ 3 of the calls occurred in October–November 2005	Increased attention
8. Sibley Memorial Hospital	▪ 3 potential surveillance calls; 2 in one cluster involving chemical plant	▪ Surveillance activity not repeated recently	Increased attention
9. ATI Afribank	▪ 2 markedly suspicious packages, 1 involving white powder, 1 leaking oil	▪ Incidents do not appear directly related	Increased attention
10. DC Public Health Commission	▪ 2 markedly suspicious packages, 1 involving brown powder, 1 a pipe with wires wrapped around it	▪ Incidents do not appear directly related	Increased attention
11. Iraq Chancery	▪ Molotov cocktail—only weapon found ▪ Natural target because of war	▪ Only one incident	Increased attention

As shown in Table 6-3, we have identified four locations of interest for which we believe follow-up monitoring and analysis are warranted. Our primary rule for selecting these locations is that they have seen multiple incidents of genuinely atypical activity that has continued recently.

- **I-395 West End (14th Street Bridge and Maine Avenue Overpass).** There is reason to believe that many of the potential surveillance events in this area—especially on the 14th Street Bridge itself—were really tourism, despite elevated personal risks. Still, the atypical nature of some of the incidents does constitute some cause for concern. The incidents near Maine Avenue appeared to be directed at traffic and infrastructure rather than tourism, and did cover the area from different perspectives. The incidents found through backsweeping—two involving people on the bridge piers and one involving people dressed in black in a control tower—are also of concern.

- **Union Station.** The number of suspicious packages alone does not constitute cause for concern, as Washington, D.C.'s main train station is a natural place to accidentally leave luggage. Similarly, some of the bomb threats appear to be crank calls (one caller threatened to blow up the food court because he did not like the food). However, the number of incidents at Union Station has been increasing steadily over time—the only named location for which this is the case (incidents elsewhere have been on an overall decline). There is also a strong mix of incidents at this location, including bomb threats and potential surveillance incidents, in addition to suspicious packages. Furthermore, Union Station is the only named location that has seen a set of linked suspicious packages.

- **Washington Hospital Center.** This has seen six incidents, including one markedly suspicious package addressed to the "Department of Justice," three bomb threats, and two discoveries of white powder. Three incidents occurred in 2007; as noted, the overall number of incidents at hospitals has been increasing.

- **Renaissance Mayflower Hotel.** As noted earlier, hotels have seen an increasing number of suspicious incidents, and this was the only hotel named more than once. There have been four incidents here, three of which (including a person filming the hotel's rear and loading dock) occurred in May and June 2007.

The other locations of interest warrant some increased attention, but not as much as these four. While there were many incidents for the I-395 northern exits, especially the tunnels, many appeared to be vagrancy, stopped vehicles (or walkers from stopped vehicles), or fallen packages. The cluster of incidents relating to a man filming traffic on these exits is of concern, but ended in early 2006. The Bolling AFB/Naval Station has seen 14 potential surveillance calls, but these were widely dispersed around a large area, and it was frequently unclear exactly what was being surveyed, if anything. Venable LLP's seven bomb threats appear likely to be due to disgruntled clients. Three of the four bomb threats to the Public Safety Communications center appeared in 2005; the last one was in mid-2006. The incidents of a woman filming Sibley Memorial's facilities were of concern, but have not been repeated recently. ATI Afribank's suspicious packages are also of concern, but appear unrelated and are separate by almost a year. Finally, the discovery of a Molotov cocktail at the Iraqi chancery is of high concern—it was the only genuine explosive weapon reported—but this was the only incident at the chancery.

6

Discussion and Recommendations

Attempting to identify suspicious behavior indicative of something far more sinister often resembles looking for the proverbial needle in the haystack. Behaviors can be misinterpreted by citizens, officers, or security personnel, resulting in an unknown number of false-positive reports. Yet, calls by citizens about suspicious activity could also represent an important source of information on potential terrorist threats. Unfortunately, the use of 911 data has been largely unexplored in terms of its potential utility to homeland security.

A jurisdiction's 911 CFS data represent an underutilized resource for collecting information on suspicious behaviors reported by citizens, particularly those reports that are potentially related to terrorist pre-planning activities. The ability to identify, model, and characterize possible hostile surveillance provides direct operational benefits including the ability to reveal potential vulnerabilities or areas of interest to likely terrorists, including the times and locations of pre-planning activity.

In large part, the limited use of CFS data is due to the intensive pre-processing and analysis required for extracting useful information, which can consume time and manpower resources that police departments cannot afford to expend. A related challenge concerns analyzing large volumes of data on suspicious activity and then prioritizing a small proportion of these cases for follow-up. CFS data also typically contain calls on a wide range of behaviors, including activities related to illegal drug activity; criminal casings of people, places, or things; and loitering, making it difficult to distinguish between certain types of events.

The objectives of this study were to (1) apply an analytic method to a data source commonly available to law enforcement in order to verify if operationally relevant findings related to counterterrorism could be produced, (2) document and capture this process so that it can be incorporated into standard operating procedures within law enforcement agencies or fusion centers, and (3) assess the usefulness of CFS data in counterterrorism planning and prevention activities.

We believe this project demonstrated that a relatively simple analytic approach could be used to produce operationally relevant findings from 911 calls. The number of cases identified as potentially related to preoperational terrorist activities represented only a small proportion of all suspicious calls (fewer than 200 calls out of approximately 1.3 million). As part of this process, we developed a method for evaluating the risk level of both incidents and clusters of incidents. While we found no strong evidence of preoperational activities in progress, we did find 11 locations of interest worth further attention, along with evidence for and against preoperational activities actually taking place at those locations.

This study did have several limitations that should be discussed in more detail. First, because Washington, D.C., is a unique location, the results may not be generalizable to other jurisdictions. For instance, Washington has many landmarks that are associated with tourist attractions, which could complicate distinguishing between potential terrorist surveillance activity and innocuous tourist activity that has been mistaken as threatening by citizens calling 911. Washington is also home to numerous law enforcement agencies that receive suspicious activity reports, including the MPD, Capitol Police, FBI, and surrounding police departments. Having so many agencies in the region likely explains certain gaps in reports for specified areas across the city. In other words, the presence of multiple agencies can actually make it more difficult to capture all reported suspicious activity because these agencies lack access to each other's data sources. For example, reports of suspicious activity on the Metro transit system may have been reported directly to Metro police personnel but not registered through 911. As such, in order to validate and refine the developed methodology, it is important that future research test the methods used in this study by applying them to other jurisdictions that have different characteristics and vulnerabilities.

The CFS data are also limited in that call type and call comments are dependent on what is reported by the initial caller and responding officer and then entered by the 911 dispatcher. Call types are not always updated; a call initially identified as "suspicious person" could have turned out to be a burglary in progress. Similarly, comments frequently are not updated with investigative results. For example, very few of the potential surveillance call comments stated whether the officer actually found the suspects in question and whether they were truly engaged in suspicious behavior or were just tourists or other innocent bystanders. In addition, one class of calls that we expected to find was missing from the CFS data—probing behavior. This class would include reports of individuals aggressively approaching locations that could be potential targets (this would include trespassing), or asking probing questions about personnel or security measures. We reviewed numerous suspicious person and unauthorized entry (trespassing) records to try to find reports of probing behavior, but found none. We believe that these incidents are collected by entities not represented by the 911 CFS data or are simply not recorded.

Finally, the power of CFS analysis to identify confirmed cases of terrorism is limited in that we are not able to confirm what an incident truly represents using CFS data alone. For example, does a person exhibiting suspicious behavior represent a tourist or a terrorist? The question is difficult because in many cases the behavior is similar and not easily distinguishable by an individual who just happens to notice and report the behavior. Individuals reporting the behavior also introduce bias into the data because their reporting of an event is based on their own internal scale of behaviors that they perceive to be suspicious or innocuous. Thus, two individuals who observe the same behavior and may reach different conclusions about whether it should be reported to law enforcement. Individuals may also be sensitized to reporting incidents that are associated with areas that they consider sensitive. They may also be more likely to report behavior if the individual is of a specific ethnicity (e.g., "Middle Eastern" or "Arabic"), although our analysis did not reveal an overwhelming ethnic bias.

6.1 Recommendations

Ultimately, improved collection and analysis of suspicious activity data from CFS data can allow law enforcement agencies to integrate previously underutilized data sources into their analytic practices, to identify potential signs of terrorist pre-planning activity in specific jurisdictions, and to identify operationally relevant information that can be used to directly support follow-up investigations. Analyzing these data can produce results that were previously unknown or they can reinforce and illuminate existing counterterrorism activities. For instances where the information was not previously known, it can serve as a trigger to collect more detailed data to verify if there is actual terrorist activity taking place. For situations where the results confirm or negate existing beliefs about assets most threatened by a potential terrorist attack, adjustments can be made to counterterrorism strategies. Findings from calls for service analysis can also be used to establish a baseline level of suspicious activity in jurisdictions.

We have a number of recommendations to improve the data analysis processes used in this project and to help implement the processes elsewhere. These recommendations pertain to data collection, data formatting, automation, and publicity and training.

6.1.1 Data Collection

As discussed above, we were unable to find any reports of aggressive approaches or questioning in the data. We recommend working with security officers at major office buildings, landmarks, and infrastructure facilities, especially those named as locations of interest, to incorporate their suspicious activity reports related to probing behavior.

We recommend adding a field to records allowing responding officers to report the results of their investigation. Of particular interest are reports that a particular call did end up being suspicious, and why it was suspicious, even in situations that did not warrant making an arrest or opening a case. Potential surveillance incidents would be situations that did not fit standard patterns of tourism, work or “ordinary crime”—for example, finding a person who really was trying to survey bridge infrastructure as opposed to just taking pictures of airplanes and the Washington, D.C., skyline. Suspicious packages would be items that did not fit standard patterns of litter or left personal effects. Examples might include luggage that contained nothing or deadweight rather than clothing or papers, or luggage left in areas decidedly away from normal places to forget it (especially if the person had to trespass to get the luggage there).

It may be the case that Washington, D.C., government does not want to add an additional field directly to the 911 database. Washington, D.C., already maintains separate databases on DCFEMS HAZMAT calls and MPD’s responses to certain suspicious package calls; an alternate recommendation would be to add the results comments to these databases and set up a new, similar database tracking results for potential surveillance and probing calls.

In either case, we recommend having the separate databases add a field linking their records to one of the identification fields in the 911 calls database, which will allow direct joins between the databases. We were able to match 911 call records with HAZMAT and suspicious package records manually through matching times and addresses, but this took a significant amount of time.

6.1.2 Data Formatting

As noted in Section 2, RTI’s Trinity Sight™ methodology focuses on the time, location, and nature of suspicious incidents. We have identified certain key fields that need to be present to support the analysis. The first set includes core fields needed to be able to extract and process call records. These need to be collected on every CFS; fortunately, we find it likely that most 911 systems would maintain these fields (they are all present in Washington, D.C.'s 911 records). These include the following:

- Time: date and time of call
- Location: address, grid coordinate, and name (filled out if applicable for landmarks and notable buildings)
- Nature: type of incident and call comments

The second set includes fields directly supporting data analysis. These fields only need to be added for those records extracted from the main database. These include the following:

- Type of incident
- Risk level of incident
- Type of location
- Area of location, such as a neighborhood
- Name of location. This is needed to provide a consistent naming scheme for landmarks and notable buildings, because "name" field in the main 911 database will not be filled out the same way by all operators.
- Hybrid location type. This combines the most relevant location type areas and names, supporting creation of a single bar chart summarizing incident locations.
- Status. This records whether a record is (1) entirely new, (2) previously in the main database but not previously extracted, (3) previously reviewed but discarded, or (4) reviewed and found to be relevant for counterterrorism purposes. This field supports comparing previously analyzed records with new call records, which is important when implementing this process to analyze incoming call records regularly.

To ensure compatibility with other law enforcement systems, these fields should be translatable into XML format, consistent with the Department of Justice's new National Information Exchange Model and Law Enforcement ISP Exchange Specification, described at www.niem.gov (DOJ and DHS, 2007).

6.1.3 Automation

Comprehensive automation of the call analysis methodologies is a subject for future research. However, there are some comparatively simple tasks that could be automated using Visual Basic programming in Microsoft Access and Excel. These include providing analysts with simple window inputs for the following:

- Filtering: Set up and retain complicated, multiple keyword queries to perform filtering.

- Querying and sorting: Extract and display records by multiple value matches for all fields listed in the previous section. Sort records by any combination of fields. Save both common queries and edited tables of results.

- Reviewing: Allow analysts to either assign a value for the derived fields from a menu (ensuring consistency) or create a new value (for records with unique characteristics).

- Charting: Export a table of records to panels of bar charts, panels of trend charts, or color-coded location plots.

- Clustering: Have the computer suggest clusters by time and location value or by time and grid coordinate nearness.

6.1.4 Training and Technical Assistance

Finally, we recommend setting up training and technical assistance programs in three areas. The first concerns the general public; it would be useful to post signs requesting the public to report certain types of suspicious activity, especially in locations of interest. The second concerns security staff at major landmarks and notable buildings. As noted earlier, aggressive approach and questioning behavior was absent from the 911 call records. We suggest an outreach effort to security staff in downtown Washington, D.C., areas, providing them with examples of approach and questioning behavior, and asking that they report it. The third concerns officers and emergency personnel responding to potential surveillance and would ask them to report on genuinely suspicious results from their investigations.

6.2 Future Research

This study represents a first step in applying 911 CFS data to homeland security and counterterrorism efforts. We have identified a number of areas for future research.

- **Automation.** Automation of most analysis steps would allow the data to be analyzed efficiently and perhaps more effectively, on a recurring basis. We have already identified some near-term tasks that could be automated using Visual Basic programming. On a more advanced level, we recommend studying the use of text mining software for filtering, classifying, and clustering records; RTI is about to start an Internal Research & Development that will examine the value of text mining software. We also recommend studying the use of full GIS packages, such as the ArcGIS, to determine if there are more effective ways to visualize locations and identify clusters than simple location plots. Finally, we recommend developing an integrated tool supporting analysis through a single interface rather than requiring analysts to manually translate data between tools.

- **Expansion to Metropolitan Regions.** Terrorists do not abide by jurisdictional boundaries; in the case of the National Capitol Area, many potential targets are located outside of the District of Columbia. We recommend expanding the processes described in this section to cover the entire metropolitan region. In addition to identifying locations of interest outside Washington, D.C., it may be possible to identify patterns of suspicious activity cutting across jurisdictional boundaries. We also recommend the continued refinement of the developed 10-risk rating framework using to classify and prioritize the selected cases of interest.

- **Application to Crime Prevention.** Finally, the approaches taken in this study have relevance to traditional crime prevention. By utilizing 911 CFS data, it should be possible to both identify and predict small-area upswings in crime, as well as better understand what types of crime are precursors to more violent crime.

This project has demonstrated that CFS data can be a useful data source for counterterrorism planning. The techniques used for “filtering out the noise” of the 911 call data were straightforward and did not require complex analyses or software tools. Ultimately, these processes can allow local law enforcement agencies to (1) integrate previously underutilized data sources into existing analytic practices, (2) identify potential signs of terrorist preplanning activity in specific jurisdictions, and (3) identify operationally relevant information that can be used to directly support follow-up investigations. The failure to incorporate these data into counterterrorism planning could result in missed opportunities for prevention as some of the incidents of interest reported by citizens may go otherwise undetected. While suspicious activity data do not, in themselves, represent tactical or strategic intelligence, the process of evaluating suspicious activity data is an essential first step in transforming raw information into actionable output.

Jurisdictions interested in experimenting with this project’s methodology in the near term can review Appendix C, which provides a near-term implementation guide. On a larger scope, CFS data analysis can serve an important role in a fusion center, providing the center with specific locations of interest to investigate and informing ongoing investigations with confirming or disconfirming information. Appendix D discusses a larger architecture for fusing homeland security data and shows how the methodology presented here would fit into that architecture.

In summary, we believe that CFS data can be useful in counterterrorism planning activities. There are currently limited data sources that can be used to assess a jurisdiction’s relative risk of terrorism and establish a baseline level of pre-planning terrorist activity. Utilizing CFS data, this activity level could be monitored on an ongoing basis and used to take a proactive approach to terrorism prevention rather than a purely reactive approach that is based on combing data to support an incoming tip. Furthermore, analyzing these data can produce results that were previously unknown or they can reinforce and illuminate existing counterterrorism activities. In instances where the information was not previously known, it can serve as a trigger to collect more detailed data to verify if there is actual terrorist activity taking place. For situations where the results confirm or negate existing beliefs about assets most threatened by a potential terrorist attack, adjustments can be made to counterterrorism strategies.

.

References

The 9/11 Commission. (2004). The 9/11 commission report.

Air War College. (2007). *Gateway to intelligence.* Retrieved from http://www.au.af.mil/au/awc/awcgate/awc-ntel.htm#humint

Al-Qaeda (n.d.). *Training manual. Eleventh lesson—Espionage (1) Information-gathering using open methods.* Retrieved from http://www.disastercenter.com/terror/Al_Qaeda_Manual_ELEVENTH_LESSON.htm

Barkun, M. (1997). Religion and the racist right; The origins of the Christian Identity movement. Chapel Hill, NC: The University of North Carolina Press.

Bureau of Justice Assistance (BJA). (2005). *Intelligence-led policing: The new intelligence architecture* (NCJ 210681). Washington, DC: U.S. Department of Justice.

Carter, M. (2004). Why feds believe terrorists are probing ferry system. *The Seattle Times.* Retrieved July 10, 2007, from http://seattletimes.nwsource.com/html/localnews/2002058959_ferry10m.html

Chapman, P., Clinton, J., Kerber, R., Khabaza, T., Reinartz, T., Shearer, C., et al. (1999). *CRISP-DM 1.0: Step-by-step data mining guide*. Miami, FL: CRISP-DM Consortium, SPSS. Retrieved from www.crisp-dm.org

CNN.com (2004, August 3). *Officials: Arrest in Pakistan led to orange alert.* Washington, DC: CNN. Retrieved from http://www.cnn.com/2004/US/08/02/terror.threat/index.html

De Becker, G. (1997). *The gift of fear*. New York: Little, Brown and Company.

Eddy, M. (2007, September 6). *Germany searching for 10 terror suspects.* New York: AP News.

Grant, G. (2006). Behind the bomb makers. *Defense Technology International*, pp. 30–32.

Goldfayne, A. (2007). Software logs Chicago 911 call data, makes it searchable. FireRescue 1 News. Available at http://www.firerescue1.com/print.asp?act=print&vid=287387

Harris, S. (2007, April). Shadow hunters. *National Journal*.

Hollywood, J., Snyder, D., McKay, K., & Boon, J. (2004). *Out of the ordinary: Finding hidden threats by analyzing unusual behavior* (MG-126-RC). Santa Monica, CA: RAND Corporation. Retrieved from http://www.rand.org/pubs/monographs/2004/RAND_MG126.pdf

Jarboe, J.F. (2002). The threat of eco-terrorism. Testimony before the House Resources Committee, Subcommittee on Forests and Forest Health. Available at http://www.fbi.gov/congress/congress02/jarboe021202.htm.

Jonas, J., & Harper, J. (2006). Effective counterterrorism and the limited role of predictive data mining. *Policy Analysis, 584*.

Kelling, G. L., & Bratton, W. J. (2006). Policing terrorism. *Civic Bulletin, 43*.

Koh, D. (2008). City tries to address overuse of 911 system. Baltimore Sun. Available at http://www.baltimoresun.com/news/local/bal-ambulance0508,0,3664267.story.

Krebs, V. (2006). *Social network of the 9-11 terrorist network*. Retrieved from http://www.orgnet.com/hijackers.html

Maguire, M. (2000). Policing by risks and targets: Some dimensions and implications of intelligence-led crime control. *Policing and Society*, *9*, 315–336.

Masse, T., O'Neil, S., & Rollins, J. (2007). *CRS report for Congress RL34070. Fusion centers: Issues and options for Congress* (Order code RL34070). Prepared for members and committees of Congress.

McCue, C. (2005). Data mining and predictive analytics: Battlespace awareness for the war on terrorism. *Defense Intelligence Journal, 13*, 47–63.

McCue, C. (2006). *Data mining and predictive analysis: Intelligence gathering and crime analysis* (pp. 94-100). Burlington, MA: Butterworth-Heinemann.

Medina, C. A. (2001). The coming revolution in intelligence analysis: What to do when traditional models fail. *Studies in Intelligence, 46*(3), 23–28.

Pendelton, S. (). Technology Acquisition Project Case Study: North Miami Beach, Florida, Police Department. Available at http://www.ilj.org/publications/CaseStudies/miamibeach.pdf.

Russell, R. L. (2004). Intelligence failures. *Policy Review, 123.*

Safe Cities Project. (2006). *Hard won lessons: The new paradigm—merging law enforcement and counterterrorism strategies.*

Sherman, L., & Weisburd, D. (1995). General deterrent effects of police patrol in crime "hot spots:" A randomized, controlled trial. *Justice Quarterly*, *12*(4), 625–648.

Smith, B.L. & Damphousse, K.R. (2002). American Terrorism Study: Patterns of Behavior, Investigation and Prosecution of American Terrorists. Final report to the National Institute of Justice.

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. Final report to the National Institute of Justice.

STRATFOR. (2005a, September 30). *The terrorist attack cycle: Selecting the target.* Austin, TX: Strategic Forecasting, Inc. Retrieved from http://www.cptmi.org/html/_stratf_the_terrorist_attack_cycle2.html

STRATFOR. (2005b). *Vulnerabilities in the terrorist attack cycle.* Austin, TX: Strategic Forecasting, Inc. Retrieved from http://www.stratfor.com/products/premium/read_article.php?id=256319

Tufte, E. (1997). *Visual explanations*. Cheshire, CT: Graphics Press.

U.S. Department of Homeland Security (DHS). (2007). *Preparedness Directorate Office of Grants and Training: FY 2007 Homeland Security Grant Program—Supplemental resource: Fusion capability planning tool.* Washington, DC: U.S. Department of Homeland Security. Retrieved from http://it.ojp.gov/topic.jsp?topic_id=209

U.S. Department of Homeland Security (DHS) & Federal Bureau of Investigation (FBI). (2005). *Terrorist tactics: Analysis of the surveillance notes concerning certain US financial buildings*.

U.S. Department of Justice (DOJ). (2006). Analyst's toolbox: A toolbox for the intelligent analyst. Prepared by the U.S. Department of Justice's Global Just Information Sharing Initiative Intelligence Working Group. Retrieved from http://www.it.ojp.gov/documents/ analyst_toolbox.pdf

U.S. Department of Justice (DOJ) & U.S. Department of Homeland Security (DHS). (2005). *Fusion center guidelines: Developing and sharing information and intelligence in a new world*. Retrieved from http://www.fas.org/irp/agency/ise/guidelines.pdf

U.S. Department of Justice (DOJ) & U.S. Department of Homeland Security (DHS). (2007). *National information exchange model*. Retrieved from www.niem.gov

Walsh, W. (2001). CompStat: An analysis of an emerging police managerial paradigm. *Policing: An International Journal of Police Strategies & Management, 24*(3), 347–362.

Warner, B., & Pierce, G. (1993). Reexamining social disorganization theory using calls to the police as a measure of crime. *Criminology, 31*(4), 493–517.

Appendix A: Call for Service Datafile Variables

agid = responding agency; values are “MPD” and “TRU” (MPD = Metropolitan Police Department, TRU = Telephone Reporting Unit); Telephone Reporting Unit (TRU) calls are typically placed when a complainant prefers to file a report over the phone.

sdts = combined date-time stamp (e.g., **20051006122126ED** = October 6, 2005 at 12:21:26 Eastern Daylight Time)

year = year

month = month

moday = combined month and day stamp (e.g., 1001 = October 1)

time = time of call represented in military time

hour = hour of the day represented in 24 hour time (e.g., 00 = midnight)

eid = unique identifier for a call for service. A “call for service” is defined as any call that requires some sort of police action.

case_num = a case number (CCN number) is issued whenever an offense/incident report is taken. Not all records will have a narrative report.

address = actual physical address where call originated. If the address is blank, that means the call occurred at an intersection.

xstreet = Cross-street or intersection. When there is no address, the event occurred at an intersection.

eapt = apartment number/building floor/suite number along with some miscellaneous text descriptions

ecompl = commonplace (e.g., Empire Apartments, Riggs Bank)

psa = police service areas. Represents the “beat” boundaries; 46 total covering the whole city.

tycod = call type code. Abbreviation for type of call (e.g., UPSN = unconscious person).

typ_eng = English version of the call type code (consistent with variable “tycod”). This is missing in some cases but can be inferred from “tycod” variable.

cfscat = calls for service category

rcfscat = recoded calls for service category to reduce the number of categories. Some of the records have the field RCFSCAT = 10. Don't necessarily ignore these; they are just new codes that have not yet been added to my value list for call type.

sub_tycod = indicates whether the event was in progress, just occurred, etc.

priority = priority (0 means officer in trouble, priority 1 is the next most serious)

xc = x coordinate for geo-coding

yc = y coordinate for geo-coding

dispo = disposition; result of the call

- ACA: Accidental alarm
- ADV: Advised
- ASSNCASE: CCN number assigned
- CANCELEV: Cancelled event, no dispatch necessary
- CLOSED: Closed accept, which means . . .?
- CU: Complainant Uncooperative
- DOA: Dead on arrival
- DMV: DMVs issued
- DUPNCAN: Duplicate CCN
- GOA: Gone on arrival
- INB: Information notebooked
- INS: Insufficient Information
- NCOM: No complainant
- NMA: Notification made
- NOF: Nothing found
- NOI: Notice of infraction
NOS: Numbers only (when a crime occurred a while ago, and the officer just needs a CCN for his/her report) ??
- NRT: No report taken

- RT: Report taken
- SECURE: Secure the scene?
- SOW: Sent on way
- TRU: Event closed by Telephone Reporting Unit
- UGE: Unable to gain entry
- UTN: Unable to notify

Appendix B: Additional Analysis of 2007 Incidents

Following in-progress reviews, the MPD sent us copies of two internal databases to expand our analysis beyond 911 calls. These included Washington, D.C.'s internal spreadsheet recording hazardous packages and the MPD's internal spreadsheet recording suspicious packages. Both covered incidents from January through June 2007. The hazardous package spreadsheet contained no details besides links to files on the MPD's network (we did not have access to these). The suspicious package spreadsheet contained brief, one-line summaries.

B.1 Methods

The methods used parallel those for analyzing multiple types of 911 calls. The first step was consolidating the new spreadsheets with the previously analyzed call records into a single spreadsheet. The two new spreadsheets covered January through June 2007, so we similarly extracted the calls from this period. We then manually compared the call records to the events on the spreadsheets. There was no clear pattern of overlap; some call records had matching records in the new databases, while other records were unique. We thus have three kinds of suspicious package incidents: the aforementioned markedly suspicious packages, suspicious packages with multiple records, and suspicious packages with only a single record.

The new spreadsheets contained date and address fields, but did not have SPCS coordinates. Thus, we used Google Earth to plot locations because Google Earth can provide geolocations for a table of addresses. To do this, we created a single field for each location. For the new spreadsheets, this field was simply the address. For the 911 call records, this field could be the address, cross-street, or landmark name, depending on what was present; addresses were selected if available.

Mapping into Google Earth generally worked well, but had limitations. The major shortfall was that Google Earth's address database did not register locations on highways; instead, we had to find alternate addresses near these locations. Some alternate addresses were reasonably close, while others, notably for bridges, were not. The shortfall was compounded by the fact that the names for the bridges do appear on Google's maps. A few addresses for residences could not be geolocated at all.

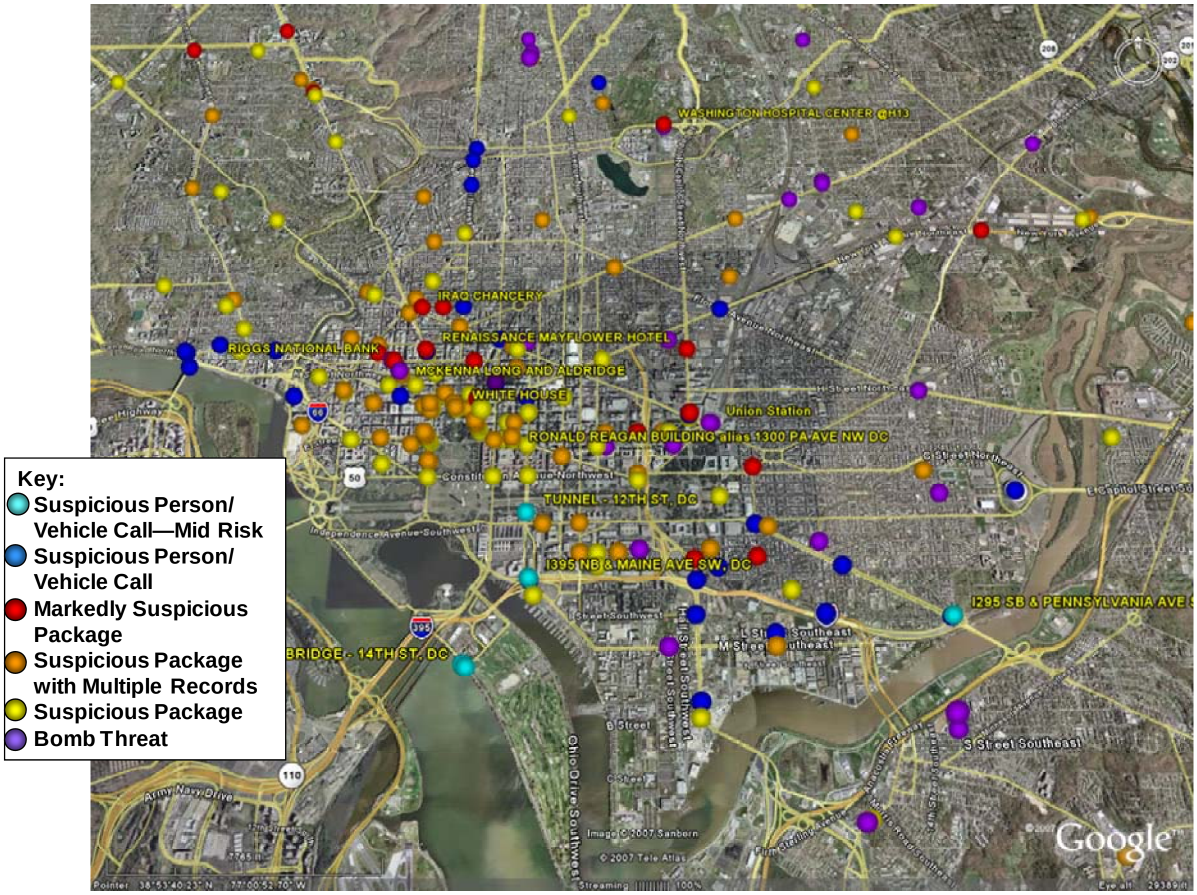
A second shortfall was that Google Earth does not automatically show duplicates of the same location—an important indicator for this analysis because duplicates generally indicate clusters of incidents. For this analysis, we manually adjusted the altitude of the duplicate locations so that they would appear as stacked disks.

As in previous chapters, we also prepared bar charts characterizing the observations by type of location and specific location, and then we drilled down on clusters of significant numbers of incidents.

B.2 Location Plots

Figure B-1 shows the Google Earth plot of incidents in the downtown area. We have added the names of locations with significant numbers of incidents or with markedly suspicious incidents (such as the Iraq Chancery's Molotov cocktail). The overall pattern continues to be that seen previously; there is fairly wide dispersion of incidents, concentrated in the K Street area, with large clusters directly around the White House, on the west end of I-395, and at Union Station. Note the distance of the bridge incident plots (14th Street Bridge, Douglass Bridge, Pennsylvania Avenue) from their actual location; as mentioned, we had to find alternate addresses for these. The 14th Street Bridge plots are particularly far away, on Ohio Street.

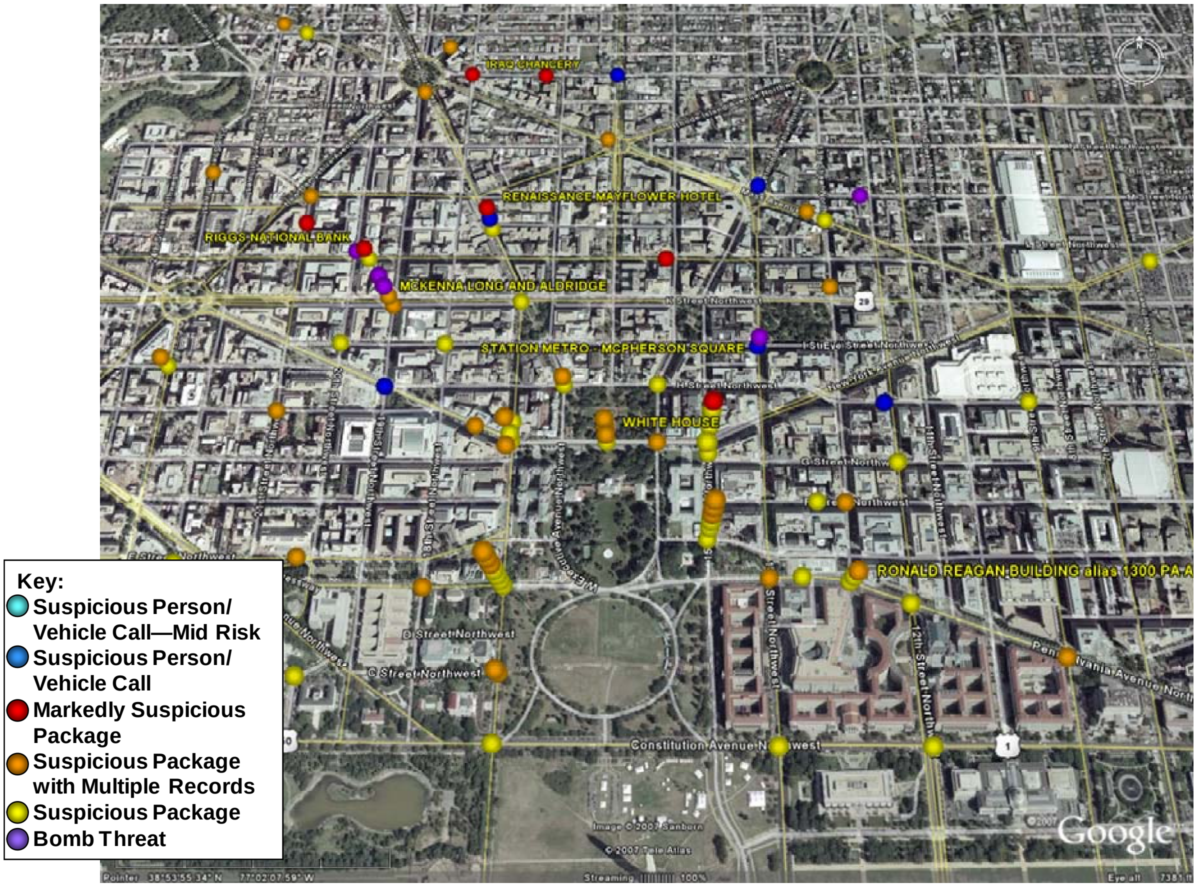
Figure B-1. Incidents in Downtown Washington, D.C., January–June 2007


WASHINGTON HOSPITAL CENTER @H13
IRAQ CHANCERY
RENAISSANCE MAYFLOWER HOTEL
RIGGS NATIONAL BANK
MCKENNA LONG AND ALDRIDGE
WHITE HOUSE
Union Station
RONALD REAGAN BUILDING alias 1300 PA AVE NW DC
TUNNEL - 12TH ST, DC
I395 NB & MAINE AVE SW, DC
I295 SB & PENNSYLVANIA AVE S
BRIDGE - 14TH ST, DC
Key:
Suspicious Person/ Vehicle Call—Mid Risk
Suspicious Person/ Vehicle Call
Markedly Suspicious Package
Suspicious Package with Multiple Records
Suspicious Package
Bomb Threat
Image © 2007 Sanborn
© 2007 Tele Atlas
Google

Source: Google Earth.

Figure B-2 provides a detailed view of incidents near the White House. The figure shows the distribution of White House events around the various entrance gates to this landmark. It also more clearly shows the various types of incidents at locations in the broader K Street/White House area.

Figure B-2. Incidents in the White House Area, January–June 2007


IRAQ CHANCERY
RENAISSANCE MAYFLOWER HOTEL
RIGGS NATIONAL BANK
MCKENNA LONG AND ALDRIDGE
STATION METRO - MCPHERSON SQUARE
WHITE HOUSE
RONALD REAGAN BUILDING alias 1300 PA A
K Street Northwest
I St/Eye Street Northwest
H Street Northwest
G Street Northwest
E Street Northwest
D Street Northwest
C Street Northwest
Constitution Avenue Northwest
Pennsylvania Avenue Northwest
New York Avenue Northwest
17th Street Northwest
18th Street Northwest
15th Street Northwest
14th Street Northwest
12th Street Northwest
11th Street Northwest
Key:
Suspicious Person/ Vehicle Call—Mid Risk
Suspicious Person/ Vehicle Call
Markedly Suspicious Package
Suspicious Package with Multiple Records
Suspicious Package
Bomb Threat
Image © 2007 Sanborn
© 2007 Tele Atlas
Google

Source: Google Earth.

B.3 Clusters of Incidents

Figure B-3 shows all locations with two or more incidents between January and June 2007. Events for the I-395 system have been divided into two pieces (western and eastern ends), and events for the White House have been divided into four pieces. Outside of these areas, the most incidents were at Union Station and the law firm McKenna Long & Aldridge.

Figure B-3. Locations with Two or More Incidents, January–June 2007

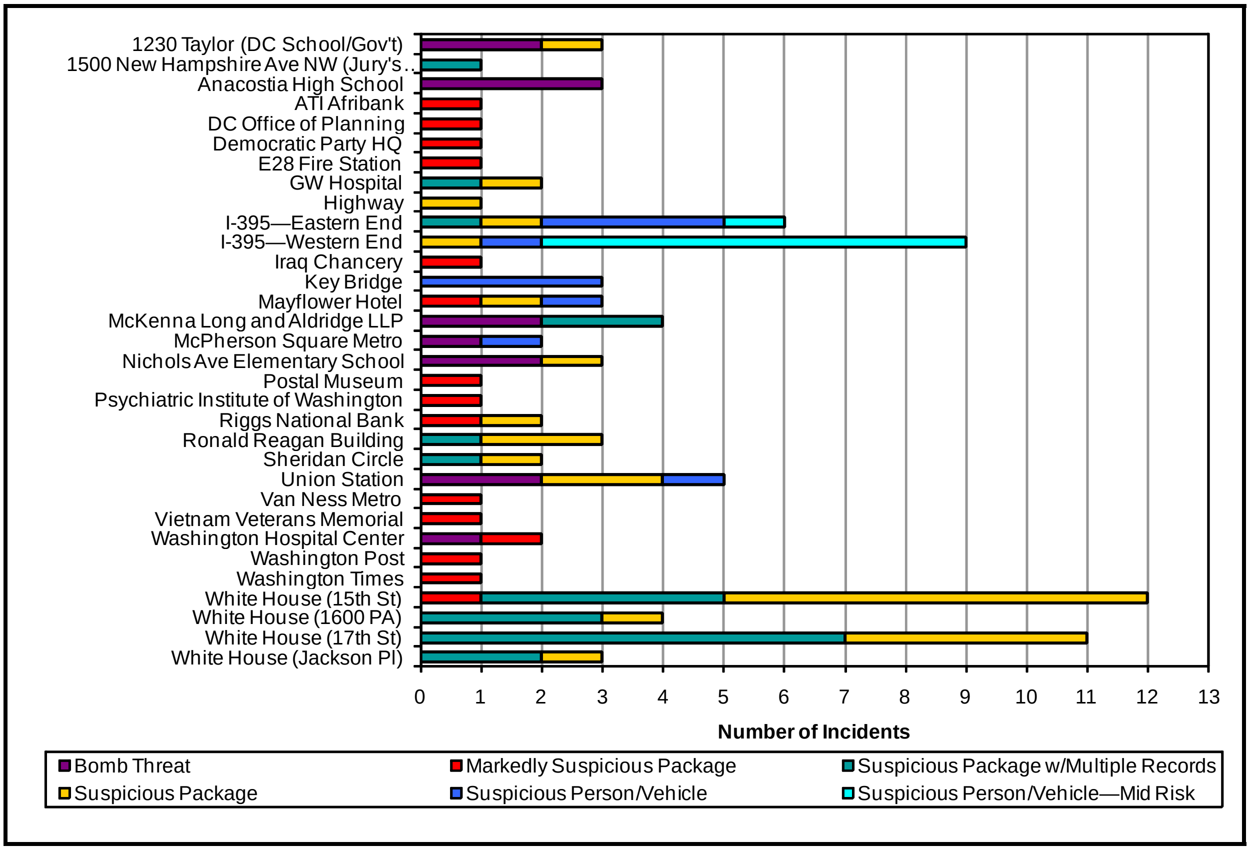
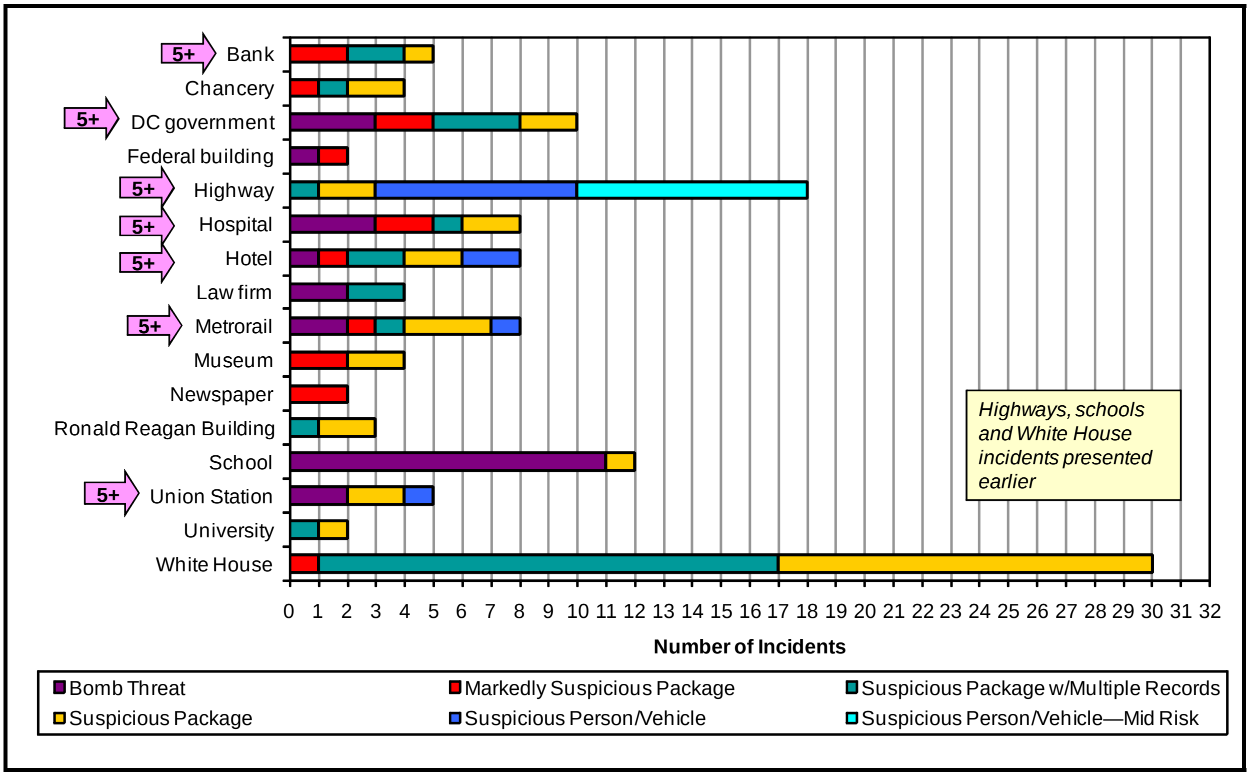


Figure B-4 characterizes the locations by type. We are interested in those types with five or more incidents between January and June 2007. These include banks, Washington, D.C. government buildings, highways, hospitals, hotels, Metrorail, Union Station, and the White House.

Figure B-4. Incidents by Type of Location, January–June 2007



Highways, schools and White House incidents presented earlier

Highway incidents have been discussed earlier in this report. Given that the school incidents are all bomb threats, most of which appear to be from students, they are not of high priority. Similarly, the White House suspicious package incidents are almost too common to be of high priority, representing frequent calls for support whenever any item is found around the White House. Below we examine the clusters of incidents for the other types of locations, plus the law firm McKenna Long & Aldridge.

Table B-1 shows incident details for the law firm, given its high number of incidents. The bomb threat note left on the copy machine is of some concern; the other incidents do not appear to be highly unusual.

Table B-1. Incidents at McKenna Long & Aldridge LLP

Date	Incident Type	Comment Field
1/25/2007	Suspicious package	SPECIAL ADDRESS COMMENT: AEDs located on site—202.496.7500 LOC......STAIRWELL NUMBER 13P LEVEL.....LOF....BLACK DUFFEL BRIEFCASE ON WHEELS......MEDIUM IN SIZE.....NOTHING APPEARS TO BE HANGING OUT FROM BAG........REPORTED IN LOCATION ABOUT 15 MINS AGO ** LOI search completed at 01/25/07 10:41:32 **
2/1/2007	Bomb threat	SPECIAL ADDRESS COMMENT: AEDs located on site—202.496.7500 DC VERIZ MIC ** LOI search completed at 02/01/07 14:08:40 ** LOI search completed at 02/01/07 14:08:51 COMPL STATES THAT THERE IS A NOTE ON THE COPY MACHINE ON THE 12TH FLR STATING THERE IS A BOMB INSIDE IT NFI CR3040 MONITORING
3/26/2007	Suspicious package	SPECIAL ADDRESS COMMENT: AEDs located on site—202.496.7500 LOBBY MR MPD REPORT A CALL FOR A BOX THAT SAYS MEDICAL AND BIO WASTE IN THE LOBBY MPD 5843
4/26/2007	Bomb threat	SPECIAL ADDRESS COMMENT: AEDs located on site—202.496.7500 2ND PART INF ,,,COMPL STATED THAT A TENANT CALL AND TOLD THE COMPL THAT SOMEONE CALL AND STATED THAT A BOMB IS IN THE BUILDING ,, ** LOI search completed at 04/26/07 10:16:56 COMPL NOT SURE WHEN ON THE WHERE THE BOMB IS

Source: 911 call data and suspicious package data provided by the MPD.

Table B-2 shows incident details for banks. Of some interest are the three events at Riggs National Banks, including two at the same location. Also of interest is the white powder package at ATI Afribank. However, none of these incidents appear linked.

Table B-2. Incidents at Banks

Date	Location	Incident Type	Comment Field
5/9/2007	ATI Afribank	Markedly suspicious package	COMPL. IS WATING IN THE LOBBY COMPL. HAS A PACKAGE W/ WHITE POWER IN IT
2/3/2007	Riggs National Bank	Markedly suspicious package	SPECIAL ADDRESS COMMENT: A.D.T. BOX 3229 COMPL. STATE THAT A MALE BROUGHT SMALL PEN ...LEFT A BLACK BAG WITH LOCK ON IT ...CALLER PUT PACKAGE OUT SIDE OF THE DOOR LOF BLK LEATHER BAG … 3061 BLOCKING N/B TRAFFIC ON 20 3063 STOPPING PED TRAFFIC E/B ON 20 ST TRAFFIC REDIRECTED FRM E/B ON L ST TO N/B ON 20 ST 3069 VOICED A LOF FOR A B/M TALL WEARING A BLK FUR L/S E/B ON L ST HE LEFT THE PACKAGE
6/29/2007	Riggs National Bank	Suspicious package	N/A
2/5/2007	National Bank of Washington (#8)	Suspicious package w/ multiple records	LOF BLACK GARAGE BAG ....NO LIGHTS OR WIRES COMING OUT OF PACKAGE ** LOI INSIDE THE BANK....SITTING ON STEPS IN STAIRWELL CALLER STATES PACKAGE HAS BEEN THERE APPROX 5 MIN CALLER IS LOC AT THE POST OFFICE LOF B/F..WEARING BLACK CAOT /GRAY PANTS AND PINK SCARF
3/13/2007	Riggs National Bank (#5)	Suspicious package w/ multiple records	INSIDE OF POST OFFICE LOBBY... BRIEFCASE UNKOWN COLOR....

Source: 911 call data and suspicious package data provided by the MPD.

Table B-3 shows incident details for hospitals. The most significant events were at the Washington Hospital; there was a suspicious package addressed to “Department of Justice,” as well as a subsequent suspicious package associated with a bomb threat. The other incidents appear comparatively routine.

Table B-3. Incidents at Hospitals

Date	Location	Incident Type	Comment Field
5/6/2007	George Washington University Hospital	Suspicious package w/ multiple records	ON THE SUBWAY SIDE /////// ****GW DISP STATED THAT THERE WAS NO LOOK OUT OR ADDL INFO ON THE PACKAGE*** ****BROWN BOX////6 X4 INCHES///TAPED UP WITH WRITTING ON THE TOP OF THE BOX.......
6/1/2007	Psychiatric Institute of Washington	Markedly suspicious package	PSYCHIATRIC INST OF WASHINGTON: CALLER STATES THAT HE HEARD A MALE ON THE METRO BUS 34/FRIENDSHIP HTS BRAGGING ABOUT PUTTING HOMEMADE EXPLOSIVES IN BATHROOMS & BEDROOMS PUT ABOUT 3 OF THEM. CALLER STATES THAT HE IS A B/M, 6'0, 180LBS, BLACK BASEBALL CAP, BLACK SHIRT, WHITE SHOES, BLUE JEANS... SUSPECT STATED THAT HE WORKED THERE & AND THEY FIRED HIM. UNKNOW IF THE SUSPECT WAS SERIOUS OR NOT.. CALLER STATES THAT THE SUSPECT WAS CLOSE TO TENELY TOWN ON THE BUS.
4/23/2007	Washington Hospital Center	Markedly suspicious package	LOF BROWN BOX WRAPPED IN CLEAR TAPE ,,,,,,,WTH WRITING SAYING DEPARTMENT OF JUSTICE SITTING ON TOP OF TRASH CAN,,,,,,,,PARKING PAVILLION 1,,,,,2 LEVEL ** LOI search completed at 04/23/07 23:31:09 COMPL STATES THEY RECEIVED CALL FROM UNKNOWN PERSON NOT ALLOWING ANY ONE TO ENTER THE AREA UNITS RESPONDING TO F/O WASH HOSP CENTER....
6/20/2007	Washington Hospital Center	Markedly suspicious package	MPS RESPOND TO SECURITU OFFICE.. ** LOI search completed at 06/20/07 04:47:21 ====UNIT 5015 REQUESTING NUMBERS FOR 10-89====
1/12/2007	Hunt Place Health Clinic	Bomb threat	BOMB THREAT REPORTED TO THE CALLER'S SUPERVISOR
3/31/2007	Providence Hospital	Bomb threat	COMPL. STATES THAT @ 1401 HRS. FEMALE CALLED THE LOC THREATEN TO BLOW THE HOSPITAL UP......2ND CALLED WAS PLACE BY A FEMAL,,,,, HOSP. SEC, HAS CHECK THE HOSP....... AND NOW REQUESTING MPD
4/3/2007	Georgetown University Hospital	Suspicious package	SPECIAL ADDRESS COMMENT: EMER. RM. PH# 202-784-2119 NEAR ENTRANCE 1 FOR HOSPITAL.........COMPL STATES THAT SHE SAW SIRING AND A BAG WITH HAZARDAS MATERIALS NEAR TREE...AND LITTLE SHELTER ,,BECNHES ON WEST SIDE CORRECTION SIRINGE

Source: 911 call data and suspicious package data provided by the MPD.

Table B-4 shows incident details for hotels. The only definite cluster is at the Renaissance Mayflower; one of these events for Jury's Washington Hotel may be outside the hotel. None of the incidents appear to be strongly linked.

Table B-4. Incidents at Hotels

Date	Location	Incident Type	Comment Field
1/13/2007	Jury's Washington Hotel	Suspicious package w/ multiple records	LOF...GRAY SUIT CASE AND BLUE LAUNDRY PACK...HAS BEEN LEFT ATTENDED FOR SOME TIME
1/24/2007	Jury's Washington Hotel	Suspicious package w/ multiple records	NEW HAMSHIRE IS SHUT DOWN...OUC MS DUNN NOTIFIED METRO NOTIFIED...D1060 EOD K-9 ON SCENE........ECRET SERV ON SCENE PARK POLICE ENROUTE EOD-73 ON SCENE 3068 OBTAINED NUMBERS FOR SUSPICIOUS PACKAGE
5/9/2007	Renaissance Mayflower Hotel	Suspicious person/vehicle	GREEN POLO WITH CREAM STRIPES.. BLUE JEANS.. SUBJ IS VIDEO TAPING THE MAYFLOWER HOTEL AND LOADING DOCK OF THE MAYFLOWER HOTEL.. REAR OF LOCATION .. N/F LOF.... MIDDLE EASTERN MALE... ON FOOT... 5'9... SLIM BUILD... MED CMPX...
5/30/2007	Renaissance Mayflower Hotel	Markedly suspicious package	17TH ST SIDE OF THE HOTEL...R/O....IN THE MOUTH OF THE ALLEYWAY RED ELC. ITEM GREEN FUSE ATTACH TOIT... THE COMPL STATED THAT IT LOOK LIKE A BOMB
2/27/2007	President Inn	Suspicious package	N/A
5/11/2007	Hyatt Regency Washington	Bomb threat	DC VERIZ MALE ON OUTSIDE ......"BOMB WILL DETENATE BEFORE 3:00" CALLER IS MARCUS CARTER .... 11:18:20 AT THE HOTEL. CALLER STATES BOMB TO GO OFF @1500 CALLER WAS A OLDER MALE CALLER IS THE MANAGER ====CR ADVISE THEY ADVISED THEY HAVE 5LBS OF C4.....DUE TO GO OFF AT 1500HRS
6/2/2007	Watergate	Suspicious person/vehicle	SPECIAL ADDRESS COMMENT: PH#—202-783-5764 H/M, WEARING A WHITE HAT, WHITE T-SHIRT, GREEN SHORTS, TAKING PICTURES OF THE WATERGATE HOTEL BROWN FANNIE PAC FILMING THE WATERGATE

Source: 911 call data and suspicious package data provided by the MPD.

Table B-5 shows incident data for Metrorail. There is one cluster of incidents at McPherson Square station. None of the incidents contain details implying relationships between them.

Table B-5. Incidents at Metrorail Stations

Date	Location	Incident Type	Comment Field
1/31/2007	Metro Station–McPherson Square	Bomb threat	STA ENT—14TH & I STS NW...VERMONT AV & I ST NW AEDs LOCATED ON SITE: KIOSK & KIOSK AT VERMONT AVE ENTRANCE CALLER SAYS THAT A FOREIGN MAN SAID THAT HE WAS GOING TO BLOW THE STATION UP NO L/O,CALLER HUNG UP TO GET ON THE TRAIN ** 10:15:19 2ND PARTY CALLER-SHOT GOT ON THE TRAIN, HE WAS LEFT BEHIND D6800 ETHIOPIAN MAN
5/16/2007	Metro–McPherson Square Metro Station	Suspicious person/vehicle	AT VERMONT AVE ENTRANCE W/M GLASSES ,,RED AND WHITE SHIRT ,,BLUE JEANS LONG HAIR ,,,WITH A HAT ON IS TAKING PICTURES ,,N/F **
1/30/2007	Metro Station–Van Ness-UDC	Markedly suspicious package	STA ENT—CONNECTICUT AV & VEAZEY ST NW ENVELOPE...FRONT OF ENVELOPE SAY ....KAMIL NAWRATEDTETIL....DO NOT TOUCH ....SITTING IN THE COMMODE IN THE MENS BATHROOM .... GO TO UDC...OFFICER WILL MEET ALSO REQUESTING BOMB DOGS REQUESTING POLICE ONLY
1/8/2007	Tunnel–Foggy Bottom—George Washington University and Farragut West	Suspicious package	STATION ENTRANCES—23RD & I STS NW...18TH & I STS NW COMPL STATES THERE IS A LIGHT GRAY COLORED BAG, LOOKS LIKE A BODY IN THE BAG...... SIZE AND SHAPE LOOKS LIKE A BODY COMPL STATES BAG IS IN THE TUNNEL NEAR THE WHITEHURST FREEWAY ** d111 ON THE EXORESSWAY AS YOU GO INTO THE TUNNEL IS A THERE'S SOMETHING WRAPPED LOOKS LIKE A SIL
4/26/2007	Rhode Island Avenue Metro	Bomb threat	MALE CALLER CALLED AND STATED THERE IS A BOMB AT THE RHODE ISLAND AVE STATION.....CALLER THEN STATEED "THAT IS ALL THAT I HAVE TO SAY" CALLER H/U
5/31/2007	L'enfant Plaza Lower Level	Suspicious package w/ multiple records	ENTRY CONTROL POINT AT THE DOT BLDG IN THE 600 BLK OF D ST SW ON MSB 4TH ENGINE RESPONDS TO THE ALTERNATE ENTRANCE AT THE HUD BLDG IN THE 700 BLK OF D ST SW IF BETWEEN LENFANT PLAZA AND PENTAGON (MUTUAL AID), CREATE MSB & NOTIFY ARL NEED BOMB SQUAD TO RESPOND......BLDG BEEN EVACUATED ** CORR 3 SUSP PACKAGE......2 INSIDE BLDG AND ONE ON THE STREET
6/21/2007	Metro Center Upper Level	Suspicious package	N/A
6/28/2007	Farragut West	Suspicious package	N/A

Source: 911 call data and suspicious package data provided by the MPD.

Table B-6 provides details on January through June 2007 incidents at Union Station. None of these calls appear to be particularly suspicious, as they relate to what appear to be crank calls and left luggage. However, the man taking pictures of buses is of some interest, especially given that two bus drivers called 911 about him.

Table B-6. Incidents at Union Station

Date	Location	Incident Type	Comment Field
3/3/2007	Union Station	Bomb threat	MALE CALLER STATED ,,,,THERE IS A BOMB THREAT IN UNION STAION AND H/U LINE ** LOI search completed at 03/03/07 21:55:23 AMTRAK POLICE NOTIFIED D5546
4/10/2007	Union Station	Bomb threat	ANI ALI INFO --------------MALE CALLER STATED --HE DONT LIKE POLICE -------------BOMB PLANTED IN BOTTOM OF UNION STATION WHERE THE FOOD AT
4/23/2007	Union Station	Suspicious person/ vehicle	W/M BLUE PANTS BLUE JACKET DARK HAIR MID LATE 40'S PRESCRIPTION GLASSES, BEEN TAKING PICTURE OF BUSES ABOUT 5'11 ** LOI search completed at 04/23/07 06:44:57 COMPL WOULD LIKE TO BE INTERVIEWED, LOCATED AT NORTH CAPITOL/G ST 2ND COMP IS DRIVING A WHITE BUS..HE IS AT N. CAP. AND G ST NE SUBJ IS NOW HEADING UP MASS TOWARDS UNION STATION VNCA
5/10/2007	Union Station	Suspicious package	LOF....BLK SUITCASE BESIDE THE TRASHCAN ON THE NORTH CORNER LEFT UNATTENDED **
6/12/2007	Union Station	Suspicious package	Field Event **

Source: 911 call data and suspicious package data provided by the MPD.

Appendix C: Methodology Implementation Guide

This appendix presents a brief guide to implementing the call analysis methodology described in this report. It is intended to help jurisdictions set up the databases and analysis methodologies needed to execute each of the four key steps of the methodology:

1. Preprocess the data
2. Filter and review the call records for relevance
3. Identify clusters of incidents
4. Prioritize clusters of incidents and search for additional information to assess whether the cluster locations are at risk

C.1 Preprocessing the Data

To effectively analyze a jurisdiction's 911 data, the following data fields need to be present for each record, and assembled into a single database:

1. Location: An address is needed at a minimum. Name fields (for landmarks) and geospatial coordinate fields are extremely useful.
2. Time: The date of the call is needed at a minimum. Time fields are very useful in assessing whether a call is a duplicate.
3. Type of call: The type field(s) should specify, at a minimum, whether the call is for a suspicious person or vehicle, a suspicious package, or a bomb threat.
4. Description: The 911 operator's typed description of the incident.

The requirements to clean and assemble the data into the above format will vary by jurisdiction; the body of the report describes what was specifically involved to prepare the MPD's 911 data.

C.2 Filtering and Reviewing the Data

Given that a major jurisdiction will have hundreds of thousands to millions of 911 call records to review, filtering and discarding most of the records is the most important step of the methodology. The first step in filtering is to select only those types of records containing suspicious activity, suspicious package, and bomb threat reports.

The second step is to perform keyword matching to further reduce the number of records. Ideally, jurisdictions will want to create a list of keywords whose presence will select the records, and a second list of keywords whose presence will result in the record being excluded. Creating this list will involve some experimentation, picking out common themes within calls of interest that can be identified through a few keywords, as follows:

1. Extract random samples of a few hundred calls out of the suspicious activity, suspicious package, and bomb threat records.

2. Manually note those calls that are potentially relevant from a homeland security perspective.

3. Note the themes making the calls relevant, and the keywords indicating the themes. One can also use subject matter expertise to attempt to guess themes and keywords that may identify relevant records.

4. Query the records using the keywords.

5. Review the extracted records (or a sample, if there are many returned records). Note which keywords were used to identify relevant records, and determine if any keywords were irrelevant, or if there are additional keywords to try. Note the themes for incorrectly selected records, and any keywords that identify these themes. Add these keywords to the "exclude" list.

6. Repeat the query using the updated selection and exclusion keywords, and repeat the process as needed to improve the keyword lists

Jurisdictions are welcome to experiment with the list of keywords that we developed over the course of this project, shown in Table C-1.

Following keyword matching, the third step is to manually review the selected records, manually removing those not related to potential surveillance or probing.

C.3 Identifying Clusters of Incidents

The methodology identifies two types of clusters: clusters of incidents at the same location (or immediate geospatial area) and clusters of incidents across the same type of location. The latter is useful in detecting potential surveillance against a type of target (e.g., systematic casing of downtown hotels).

To detect the first type of incident, the simplest approach is to sort the relevant records by address and identify clusters of incidents occurring at the same address. If the 911 database includes a name field for landmarks, one can similarly sort the names to identify clusters. A second, heuristic approach used in this project was to sort the geospatial coordinates and review nearby records to determine if they actually formed a cluster of incidents. The third approach was to use geospatial software and look for clusters visually. However, geospatial software is not necessary; at least in this project, geospatial analysis found few clusters not already identified by the simpler approaches.

Detecting clusters of incidents by type of location is harder, because it requires coding each relevant record as being of a particular type of location. Jurisdictions will need to develop a consistent list of location codes, which will take some initial experimentation. Table C-2 shows the type labels used for DC's 911 data. Some of these are specific to DC, but for most of these a major jurisdiction can use a similar label.

Table C-1. Keywords Used in Filtering Call Records

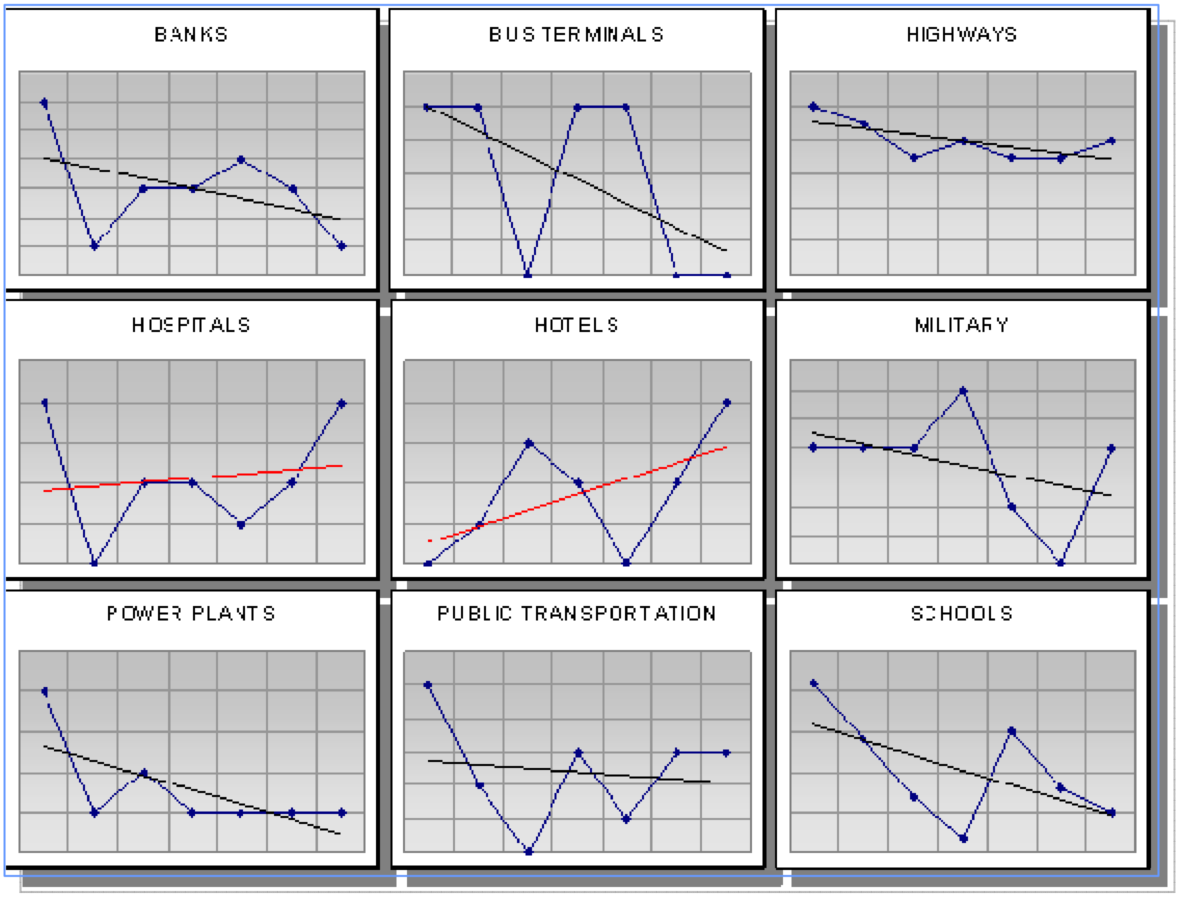
Type of call	Theme	Keywords
Potential surveillance (from "suspicious person" and "suspicious vehicle" calls)	Site photography	PHOTO, CAMERA, PICTURE
	Site video	VIDEO, TAPING, FILM, CAMCORDER
	Note-taking	NOTE, WRITE, TYPING
	Use of surveillance aids	BINOCULAR, TELESCOPE, LENS
	Photos of a crime scene (exclude)	CSS (i.e., agency tasked with taking photos of crime scenes), NEEDS A PICTURE, FOR PHOTOS, SCENE
	Photos of prisoners (exclude)	WARRANT, EXTRADITE, MISSING
Suspicious package of interest (from "suspicious package" calls)	Packages generating a major response	EOD (explosives ordnance demolition team response), K9 (bomb-sniffing dog hit)
	Packages generating a federal response (may be specific to DC)	FBI, SECRET (Secret Service), CAPITOL (Capitol Police)
	Specific types of packages	WHITE POWDER, SUSPICIOUS LETTER
	Package was left luggage (exclude)	GOOD INTENT (code for a package that was accidentally left)
Bomb threat (from "bomb threat" calls)	N/A (captured all bomb threats)	None

Table C-2. Example Location Type Labels

- Bus Terminals
- Churches
- Congressional Offices (alternate: State Government)
- DC Government (alternate: City Government)
- Embassies / Chanceries (alternate: Consulates)
- Highways
- Hospitals
- Hotels
- Law Firms (alternate: specific types of businesses, such as "Financial Firm")
- Metro (alternate: Mass Transit)
- Monuments
- Museums
- Power Plants
- Railroad Lines
- Reagan Building (alternate: Convention Center)
- Stadiums
- Union Station (alternate: Train Station, Transit Hub, Airport)
- Universities
- White House (unique to DC)

Once the records have been assigned a label, it is straightforward to use features such as Microsoft Excel's® Pivot Table to create bar graphs counting the numbers of incidents at each type of location, and sets of line graphs tracking the numbers of incidents over time. This project's reviewers have found creating a "panel" of line graphs particularly useful in permitting an analyst to rapidly focus on locations seeing increases in suspicious activity, a technique suggested by Tufte (1997).[4] As an example, Figure C-1 shows a subset of the panel of line graphs for the MPD data. Each graph plots the total number of incidents for a type of location by quarter, along with a linear trend line. Positive trends are shown in red. (The full panel is shown in Figure 4-5.)

Figure C-1. Sample Panel of Line Charts



[4] Tufte introduces the panel of line charts as a way to redesign medical charts; see Tufte, E. Visual Explanations. Cheshire, CT: Graphics Press, 1997. Pp. 110-111

C.4 Analyzing and Prioritizing Clusters

The first step in the methodology's final phase is to prioritize the incidents and clusters. Table C-3 summarizes the threat assessment frameworks used for potential surveillance incidents and for suspicious package incidents. (RTI did not develop a threat assessment framework for bomb threats).

Table C-3. Risk Assessment Frameworks

<table>
<tr><th colspan="3">I. Potential Surveillance Incidents</th></tr>
<tr><td colspan="3">Incidents are scored on four dimensions, described below. An incident can earn a maximum of 10 points.
• Incidents scoring 0-3 are considered <b>low risk</b>
• Incidents scoring 4-6 are considered <b>moderate risk</b>
• Incidents scoring 7-10 are considered <b>high risk</b> (clear threat)</td></tr>
<tr><th>Dimension</th><th>Score</th><th>Description</th></tr>
<tr><td rowspan="3">1. Atypicality of reported activities</td><td>Unusual:1 point</td><td>Could be explained by ordinary work, tourism, or criminal behavior. Examples include photographing office buildings, lesser-known landmarks, and airplanes.</td></tr>
<tr><td>Highly atypical: 2 points</td><td>Not readily explainable, especially if behavior is risky. Examples include photographing highways, railroads, and other public infrastructure.</td></tr>
<tr><td>Threatening: 4 points</td><td>Matches known pre-attack signatures. Examples include using large numbers of cell phones (or discarding them), attempted trespassing, and asking probing questions.</td></tr>
<tr><td rowspan="2">2. Attractiveness of target</td><td>Attractive: 1 point</td><td>Well-known landmark (and hence well monitored) or opportunity for significant casualties. Examples include high-density office and residential buildings, well-known landmarks, and bus systems.</td></tr>
<tr><td>Highly attractive and atypical: 2 points</td><td>Not normally photographed and could result in massive casualties or disruption. Examples include highway bridges and overpasses, chemical facilities, and subway systems.</td></tr>
<tr><td rowspan="2">3. Membership in a cluster</td><td>Moderate confidence: 1 point</td><td>Moderate confidence that the calls could be due to the same group of individuals because they are reasonably close in space, time, and descriptions.</td></tr>
<tr><td>High confidence and atypicality: 2 points</td><td>Atypicality score of at least 2, and high confidence that the calls are due to the same individuals because they are very close in space, time, and description.</td></tr>
<tr><td>4. Presence of police report</td><td>Police report: 2 points</td><td>Call record includes a police report number.</td></tr>
<tr><th colspan="3">II. Suspicious Package Incidents</th></tr>
<tr><td colspan="3">Incidents have one of two ratings:
• <b>Markedly suspicious</b> (higher risk): call's description implies the package actually was left or sent deliberately. Examples include: suspect seen leaving the package, package contained white powder or a threatening message, or package appears to have been made to look like a bomb.
• <b>Suspicious</b> (lower risk): no information provided about whether the package was left deliberately.</td></tr>
</table>

Once the individual incidents and clusters have been scored, the next step is to select those clusters and corresponding “locations of interest” worth further study. The rules to select locations of interest for this project were:

- five or more total potential surveillance or probing incidents
- two or more moderate risk incidents (moderate-risk potential surveillance or markedly suspicious packages)
- two or more incidents and a type of location that has seen escalating activity
- Having any incidents flagged as being especially suspicious, such as an actual incendiary or explosive device.

Note that judgment is needed to select locations of interest, in addition to using rules. For example, schools frequently received bomb threats in which the caller was believed to be a child; the schools were not selected as locations of interest.

The third step involves conducting “backsweeping” for the locations of interest. This involves extracting all call records (at least all suspicious activity and suspicious package records) for the location of interest, and manually reviewing them to find any additional relevant incidents.

The fourth step involves preparing lists of arguments for and against the proposition that the location is actually being targeted. In general, this involves describing and assessing the relevant incidents, and weighing how atypical and potentially threatening they are as opposed alternative, “normal” explanations for the same event (tourism, “ordinary” crime).

The final step is to critically assess the arguments and prioritize the locations of interest by perceived threat level. Broadly speaking, the highest priority locations of interest will be those in which the reported activities are clearly threatening; for this case study, fortunately we did not find any such locations. The second highest priority locations are those which have seen multiple instances of genuinely atypical behavior (assessed as being “moderate” or “high” risk) that have continued or escalated over time.

The prioritized locations of interest, along with the arguments and specific incidents responsible for their listing, are the main outputs of the methodology.

Appendix D: A Framework for Conducting Data Fusion

The Congressional Research Service's recent report on state, local, and regional information fusion centers notes that over 40 have been established since the 9/11 terrorist attacks. However, the same report also notes:

> While many of the centers have attacks as a high priority, little "true fusion," or analysis of disparate data sources, identification of intelligence gaps, and pro-active collection of intelligence against those gaps which could contribute to prevention is occurring.[1]

Little has been written about how to conduct data fusion, including in official guidelines. The DOJ and DHS Fusion Center Guidelines say little beyond defining data fusion as "turning information and intelligence into actionable knowledge" and that it refers to "the overarching process of managing the flow of information and intelligence across levels and sectors of government."[2]

This appendix places the Trinity Sight™ methodology described in this report within the context of a larger framework for conducting data fusion of homeland security and law enforcement data. The framework is based on the RAND Corporation's Atypical Signature Analysis and Processing architecture for intelligence analysis (ASAP, Hollywood et al., 2004). ASAP focuses on collaboratively analyzing observations of both suspicious behavior and known terrorist activity to find potential threats. The framework includes four key processes.

1. *Incident analysis*: analyzing clusters of suspicious activities that warrant further investigation. The methodology in this report is a specific information analysis thread within this larger process.

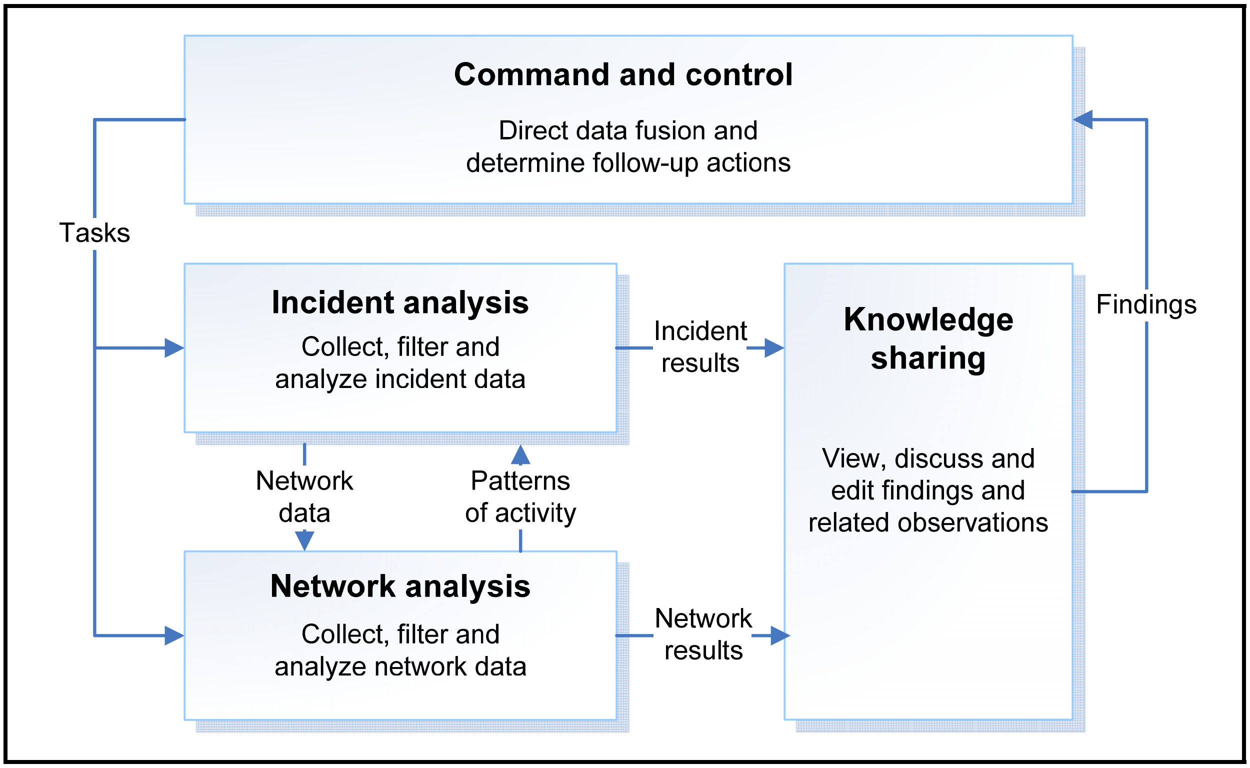
2. *Network analysis*: analyzing the people, assets, places, and relationships involved in carrying out suspicious activities.

3. *Knowledge sharing*: knowledge management and collaboration to further the analysis of suspicious incidents, people, and assets.

4. *Command and control*: monitoring and coordinating the above, and using the results of fusion to inform operational decisions.

These processes are fully integrated, as shown in Figure D-1. The incident analysis and network analysis processes collect, filter, and analyze incoming data. The knowledge sharing process permits analysts and law enforcement personnel to collectively view, discuss, and add to the analysis results. The command and control process both provides direction to the other data fusion processes and determines what operational actions to take as a result. The details of each process are discussed below.

Figure D-1. A Framework for Conducting Data Fusion


Command and control
Direct data fusion and determine follow-up actions
Tasks
Incident analysis
Collect, filter and analyze incident data
Incident results
Knowledge sharing
Findings
Network data
Patterns of activity
View, discuss and edit findings and related observations
Network analysis
Collect, filter and analyze network data
Network results

D.1 Incident Analysis

The incident analysis process searches for clusters of suspicious incidents that may be precursors for terror attacks, especially those related to casing or probing potential terror targets. As noted in the literature review, the recent major plot to attack U.S. bases in Germany was discovered as a result of catching participants attempting to carry out surveillance against the bases.[3] Similarly, the FBI has issued warnings about potential terror plots against the Washington State Ferry System based on analyzing reports of persons taking photos of ferry infrastructure and operations and asking probing questions about ferry operations.[4]

We expect that a fusion center will have multiple sources of suspicious incident data to work with. These might include calls for service data (the focus of this report), security and police agency reports on suspicious incidents, and private sector reports of on-premise suspicious activity submitted through public / private partnerships. We also expect that a fusion center will receive a stream of bulletins about ongoing investigations and profiles of suspicious activity to be especially aware of; these will help guide incident analysis processes.

As discussed in Chapter 2, RTI has developed the Trinity Sight™ methodology to perform incident analysis, focusing on analyzing the time, location and nature of suspicious incidents.[5] The methodology in this paper is a specific application of Trinity Sight™ to 911 calls for service. Trinity

Sight™ also applies broadly to other sources of suspicious incident data. As a summary, the general steps in Trinity Sight™ include the following.

1. *Questions and challenges*: This step includes identifying operational questions that describe what types incidents are of interest, and identifying challenges in answering the questions.

2. *Data collection and fusion*: This step includes collecting data that contains information on suspicious incidents of interest, and fusing these datasets into a single repository.

3. *Operationally relevant preprocessing*: This step includes inventorying data and data quality, and identifying key fields and variables for analysis, focusing on time, location, incident type, and incident description data. If necessary, this step also includes extracting structured data (especially time and location data) from the incident descriptions. Finally, this step includes the cleanup, transformation, and consolidation activities needed to prepare the data for use.

4. *Identification, characterization, and modeling*: This step begins with filtering the data to find incidents of interest, primarily using incident type fields and keyword searches. The next tasks are to cluster the incidents by time, location, and nature; to analyze trends in the incidents (flagging recent increases in activity); and to analyze the resulting risks posed by the incident clusters. Finally, this step includes identifying and assessing locations of interest (i.e., those locations identified as being at elevated risk of attack), and searching databases to determine if there is additional activity of concern at the locations of interest.

5. *Security-specific evaluation*: This step includes verifying and validating both the analysis to date and the specific hypotheses about the locations of interest. Validating the locations of interest involves asking the following questions: Do the findings make sense to law enforcement experts? Do law enforcement or security agencies have additional information that can quickly corroborate or reject the hypotheses? Are there quick follow-up investigations that can be performed to help confirm or disconfirm the risk?

6. *Operationally actionable output*: This step includes reporting findings to law enforcement and security agencies.

D.2 Network Analysis

The network analysis process seeks to build up a network (or link chart) of people, assets, and events engaged in activities suspected of being related to terrorism, with the goal of understanding the extent and intentions of the network. For example, there have been numerous network diagrams created showing links between the 9/11 hijackers and the events leading to the attacks.[6] More recently, the *National Journal* ran an article describing the 2004 investigation of an individual who called DHS warning that al-Qaeda would attack UCLA. The article describes creating a network linking the call, the person who made the call, aliases of the person (used in a prior theft investigation), potential links to greatly increased al-Qaeda terrorist chatter, and eventually capturing the person at a U.S. border and discovering the claim was false.[7] The process is similar to what a detective or private investigator would do to unravel the associates, activities, and whereabouts of a criminal suspect or organization.[8] Major steps in the process include the following:

1. *Collect and preprocess network data, to the extent it is available*: Commonly, a fusion center might receive a series of text records on persons and events of interest. A key example is

identifying information on a person participating in a highly suspicious event discovered through incident analysis, such as a name, description, or license plate number. Other examples include logs of calls, e-mails, or financial transactions considered to be suspicious.

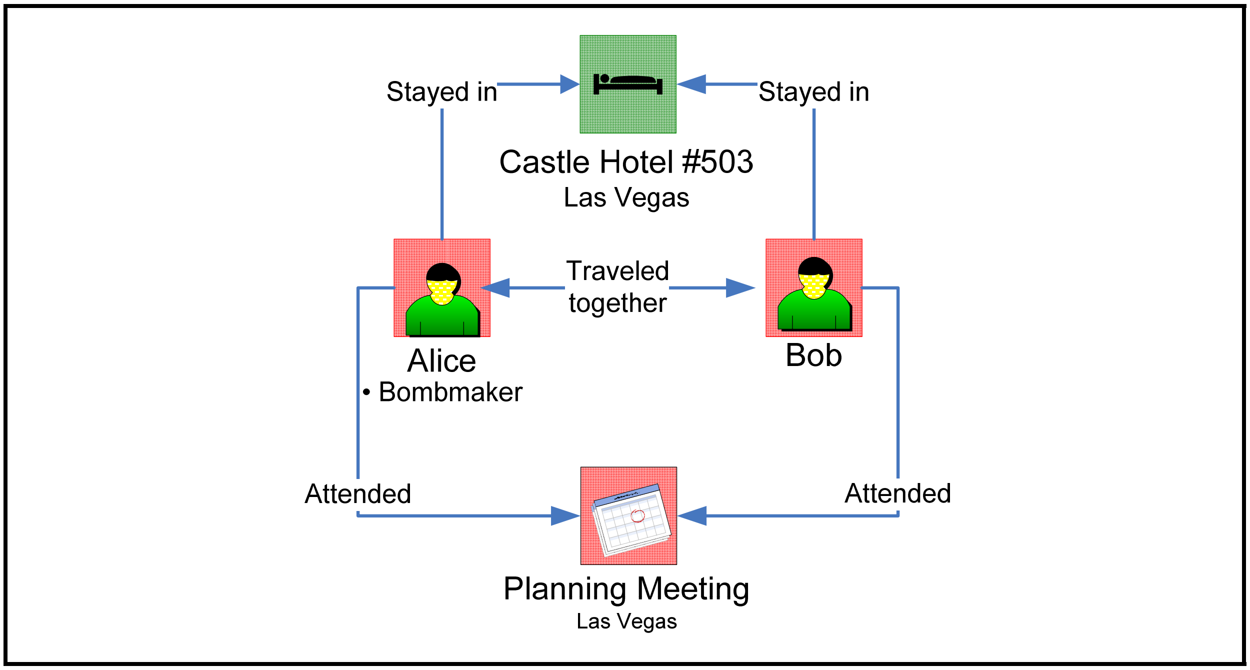
2. *Identify nodes and links*: These text records will contain the names of "entities of interest": people, personal characteristics, assets, locations, and events, as well as information about the relationships between them. A detailed example from an ongoing investigation might be: "Bomb expert Alice traveled with Bob to a planning meeting in Las Vegas, where they stayed in Room 503 at the Castle." These can be captured in list form.

3. *Assemble and visualize the resulting networks*: Figure D-2 shows the network diagram for the example above, which graphically displays entities and relationships.

4. *Identify subnetworks of interest*: These concern relationships or events that warrant further investigation. They can sometimes be found by eyeballing the network, and sometimes require algorithms looking for specific patterns (e.g., for complex networks of thousands of telephone calls). They may also concern relationships or events that provide opportunities for investigation such as apparent leaders, "communications hubs," or meetings that can be investigated.

5. *Drill down on subnetworks of interest*: This step seeks to "grow" the subnetworks of interest, adding more entities, relationships, and detail. In this step, investigators would use both public databases and standard investigative techniques to identify associates, track movements, track whereabouts, learn more about suspects' activities, and so on. The resulting data is, in turn, converted into nodes and relationships, fed back to the network diagram, and re-examined to determine the next drill-downs.

Figure D-2. Example Network Diagram



Note that the network analysis and incident analysis processes are tightly integrated with each other. The incident analysis process sends identifying information about people engaged in markedly suspicious activity (if available) to determine if the people are known risks (or can quickly be found to be risks). The network analysis process sends details about suspect networks' patterns of activities to determine if there have been any potentially related incident reports.

D.3 Knowledge Sharing

The knowledge sharing process has several objectives: ensuring that analysis findings and supporting data are distributed to the law enforcement personnel needing them, allowing personnel to comment on add to the findings, and allowing personnel to ask about potentially related phenomena. The objective is to share and maintain a "common picture" of current terror threats across law enforcement and homeland security communities. As a result, this process contains several tasks going on simultaneously.

1. *Display findings*: This task reports on findings from the incident and network analysis processes, with links to supporting data and visualizations.

2. *Search data and findings*: This task supports searching prior analysis results as well as data that might confirm or disconfirm the findings. It also supports advertising new analysis results and major suspicious observations. Data sources include material previously collected through the incident and network analysis processes, as well as externally available information (controlled and open source).

3. *Edit observations and findings*: This task allows personnel to post questions about suspicious or atypical phenomena they have observed (especially phenomena potentially related to the findings). It also allows personnel with appropriate access rights to update the findings based on new information or analysis.

4. *Collaborate*: This task allows personnel to discuss the observations and findings with analysts and with each other, providing their assessments and suggesting related observations.

D.4 Command and Control

The command and control (C2) process monitors and directs the other processes, and also ensures that action is taken as a result of analysis findings.[9] Major steps in the C2 process include the following.

1. *Identify questions and challenges*: These constitute the key information needs that the fusion processes will attempt to address.

2. *Task incident and network analysis processes*: The tasks should be tailored to address the questions and challenges.

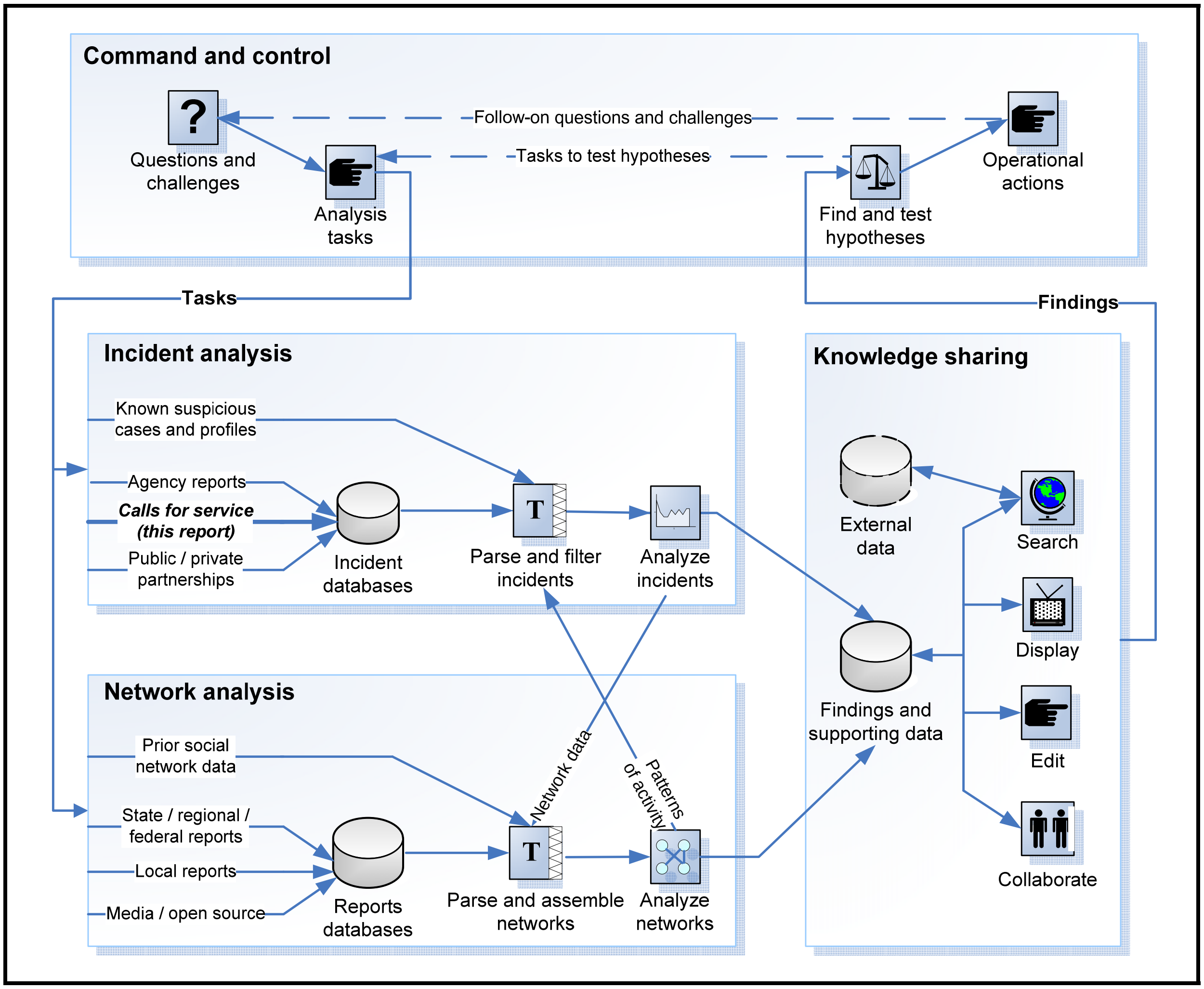
3. *Identify and test hypotheses*: The findings of the analysis processes and collaborations lead to creating certain central hypotheses – that specific clusters of incidents are related to terrorist activity, or that certain networks of individuals are involved with certain plots, for example. It is important to recognize these hypotheses explicitly, validate them with subject matter experts, and task follow-up analyses and investigative activities to test them.

4. *Review findings and generate operational actions*: Once the findings have been validated and verified (at least to a level warranting additional investigations), the findings are reviewed by senior staff, leading to operational actions. Note that some of these actions may include new questions and challenges for the fusion center, leading to new analyses.

D.5 Summary

Figure D-3 summarizes the complete framework for information fusion. The figure summarizes both the major steps within each of the four core processes and the major information flows between the four core processes. The figure also summarizes the major sources of incident data and network data, and shows where both input and analysis data are stored and accessed through the processes.

Figure D-3. Detailed View of a Framework for Conducting Data Fusion



[1] Todd Masse, Siobhan O'Neil, and John Rollins, *Fusion Centers: Issues and Options for Congress*, CRS Report for Congress RL34070, July 6, 2007, p. i.
[2] DOJ and DHS Global Justice Information Sharing Initiative, *Fusion Center Guidelines: Developing and Sharing Information and Intelligence in a New World*, July 25, 2005, p. 12.
[3] See, for example, Melissa Eddy, "Germany Searching for Ten Terror Suspects," *AP News*, September 6, 2007.
[4] Mike Carter, "Why Feds Believe Terrorists Are Probing Ferry System", *Seattle Times*, Oct 10, 2004, and Mike Carter and Jennifer Sullivan, "FBI Asks: Who Are the Men in This Photo From the Ferry?" *Seattle Times*, August 22, 2007.
[5] Trinity Sight™ was introduced in: Colleen McCue, *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis*, Burlington, MA: Butterworth-Heinemann, 2007. RTI funded the writing of this book as part of its homeland security research portfolio.
[6] Perhaps the best known 9/11 hijackers network diagram is: Valdis Krebs, "Social Network of the 9-11 Terrorist Network," URL http://www.orgnet.com/hijackers.html, 2006.
[7] Shane Harris, "Shadow Hunters," *National Journal*, April 27, 2007.
[8] See Jeff Jonas and Jim Harper, "Effective Counterterrorism and the Limited Role of Predictive Data Mining," *Policy Analysis*, No. 584, December 11, 2006. Jonas and Harper describe how a detective or private investigator might have used the knowledge that two suspected al-Qaeda terrorists were in the country, along with public databases and references, to find the two individuals and their links to other 9/11 plotters.
[9] For more information on architecting, monitoring, and controlling analysis processes, see John Hollywood et al., *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior*, Santa Monica, CA: RAND Corporation, MG-126, 2004.