Washington, DC, Area Sniper Investigation—Communications After-Action Report

FINAL

September 2003

FOREWORD

As part of the Federal Government's efforts to address public safety wireless communications interoperability in a more efficient way, the Public Safety Wireless Network (PSWN) Program is being folded into SAFECOM and will no longer function as a separate program.

Established in 2002 as part of the President's Management Agenda, SAFECOM is the overarching umbrella program within the Federal Government that oversees all initiatives and projects pertaining to public safety communications and interoperability– the ability of public safety agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice and/or data with one another on demand, in real time, when authorized. Through SAFECOM, the Federal Government is addressing public safety wireless interoperability issues in a more coordinated, comprehensive, and effective way.

The SAFECOM Program is managed within the U.S. Department of Homeland Security's Science and Technology Directorate and will cooperate with other federal organizations addressing interoperability issues through a Federal Interagency Coordination Council.

SAFECOM, with its partners, is working to assure a safer America through effective public safety communications.

For more information, contact the SAFECOM Program at safecom@dhs.gov or 1-866-969-7233.

Table of Contents

EXECUTIVE SUMMARY

In October 2002, local, state, and federal authorities from the Washington, DC, area joined in an unprecedented cooperative effort to capture the accused perpetrators charged with a series of shootings that paralyzed the National Capital Region. John Allen Muhammad and John Lee Malvo, the two suspects charged in the series of crimes, were apprehended following a 3-week shooting spree that brought together uniformed and investigative law enforcement personnel and communications resources from across the region. The extensive response and investigative effort required tactical and administrative communications among hundreds of law enforcement officers from a variety of jurisdictions and levels of government.

This report examines the use of communications equipment, interoperability issues, and communications coordination efforts among participating agencies during the Washington, DC, area sniper response and investigation. It addresses both public safety land mobile radio communications and commercially provided communications. The report includes general operational information related to response and task force communications, as well as operational and technical lessons learned related to communications interoperability between task force representatives. The intended audience for this report includes local, state, and federal public safety officials.

To develop this report, official letters were distributed to several key agencies that participated in the investigation. The Public Safety Wireless Network (PSWN) Program formally requested participation from 10 local, 1 state, and 5 federal law enforcement agencies. The PSWN Program also requested that representatives from Nextel Communications, Inc., participate in an interview. Commercial service representatives from other companies were not interviewed because public safety interviewees identified Nextel as the primary commercial service that enhanced interoperability during the investigation. Interviews provided PSWN Program staff with a clear understanding of the private and public wireless communication systems used and the interoperability issues that arose, as well as information on the specific examples included in this report. Drawing from the interviews and associated research, PSWN Program staff analyzed the information, identified primary interoperable communications solutions employed during the sniper investigation, and formulated findings. Based on these analyses, a communications and interoperability discussion along with key lessons learned were developed. The lessons learned discussion may provide guidance for communications planners and law enforcement personnel for future efforts of this magnitude.

During the course of the sniper response and investigation, several interoperability solutions were deployed to enhance both tactical and administrative interoperable communications between hundreds of officers and agents using disparate communications systems. Some of these solutions were developed long before the sniper events began, while others were initiated or enhanced for this specific set of circumstances. The primary interoperability solutions deployed included—

- Cross-system patch between Montgomery County (Maryland) Police Department's legacy ultra high frequency system and new 800 megahertz system
- Audio cross-connect switches
- Common system types and common frequencies across agency systems
- Police Mutual Aid Radio System
- Radio exchanges
- Commercial wireless services.

After analyzing the data collected from interviews with local, state, and federal agencies involved in the Washington, DC, Area Sniper Investigation, several lessons surfaced. These lessons are categorized as either operational or technical in nature, and are highlighted below.

Operational Lessons Learned	4.1.1 Preexisting relationships among participating agencies provided a foundation for effective interoperable solutions rollout
	4.1.2 Use of plain language transmissions, rather than 10-codes, enhanced interoperability between officers and agents from various agencies and jurisdictions
	4.1.3 Communications technical managers would have benefited from regular task force communications briefings and a post-investigation de-brief
	4.1.4 Lack of interoperability hindered search team communications
	4.1.5 Tactical communications planning prior to incidents enhanced operational responses
Technical Lessons Learned	4.2.1 Mobile telephones, provided by Nextel, enhanced administrative communications interoperability across the region and among participating agencies
	4.2.2 The Montgomery County radio system patch was instrumental in improving communications across the region
	4.2.3 Government and commercial communications technical staff were critical to successful deployment of communications systems and interoperable solutions
	4.2.4 Communications equipment training was critical for law enforcement officers who were unfamiliar with that equipment
	4.2.5 Interoperability across a large area and among multiple agencies required multiple solutions
	4.2.6 Interoperability between federal and state/local agencies was somewhat limited due to encryption issues

1. INTRODUCTION

In October 2002, local, state, and federal authorities from the Washington, DC, area joined in an unprecedented cooperative effort to capture the accused perpetrators charged with a series of shootings that paralyzed the National Capital Region. John Allen Muhammad and John Lee Malvo, the two suspects charged in the series of crimes, were apprehended following a 3-week shooting spree that brought together uniformed and investigative law enforcement personnel and communications resources from across the region. The extensive response and investigative effort required tactical and administrative communications among hundreds of law enforcement officers from a variety of jurisdictions and levels of government. Table 1 lists the many organizations that supported the response and investigative efforts.

Table 1
Entities That Supported the Washington, DC, Area Sniper Response and Investigation

Function	Location	Agency	Acronym	Incident Occurred in Jurisdiction
Local Law Enforcement	Washington, DC	Metropolitan Police Department	MPDC	√
	Maryland	Anne Arundel County Police Department	AACOPD	
		Frederick County Sheriff's Office	FCSO	
		Gaithersburg Police Department		
		Greenbelt Police Department		
		Howard County Police Department	HCPD	
		Montgomery County Police Department	MCPD	√
		Prince George's County Police Department	PGCPD	√
		Takoma Park Police Department	TPPD	
		Washington County Sheriff's Office	WCSO	
	Virginia	Alexandria Police Department		
		Arlington County Police Department	ACPD	
		Ashland Police Department		√
		Chesterfield County Police Department	CCPD	
		Fairfax City Police Department	FCPD	
		Fairfax County Police Department	FPD	√
		Hanover County Sheriff's Office	HCSO	
		Henrico County Division of Police	HPD	
		Loudoun County Sheriff's Office	LCSO	
		Manassas Park Police Department	MPPD	
		Manassas City Police Department		√
		Richmond Police Department	RPD	
		Spotsylvania County Sheriff's Office		√
		Stafford County Sheriff's Office		
		Prince William County Police Department	PWCPD	√
State Law Enforcement	Maryland	Maryland State Police	MSP	
	Virginia	Virginia State Police	VSP	

Function	Location	Agency	Acronym	Incident Occurred in Jurisdiction
Federal Law Enforcement	United States	Bureau of Alcohol, Tobacco, Firearms, and Explosives	ATF	
		Drug Enforcement Administration	DEA	
		Federal Bureau of Investigation	FBI	
		U.S. Customs Service	USCS	
		U.S. Marshals Service	USMS	
		U.S. Park Police	USPP	
		U.S. Secret Service	USSS	
Defense	United States	Department of Defense	DoD	

In this report, the Public Safety Wireless Network (PSWN) Program documents background information regarding law enforcement communications during the sniper investigation, identifies interoperable solutions that were deployed, and documents operational and technical lessons learned related to interoperable communications.

1.1 Purpose

The Washington, DC, area sniper response and investigation required significant sharing of communications resources through coordination across agencies and the implementation of interoperability solutions. The purpose of this report is to document both operational and technical findings related to the communications environment during the investigation. Specifically, the report provides an overview discussion of communications including—radio systems and equipment, deployed interoperable solutions, and commercial wireless services. The report also includes communications lessons learned during the investigation.

1.2 Background

Public safety agencies in the Washington, DC, region are not new to interoperability issues and major events. As early as 1982, when Air Florida Flight 90 crashed into Washington, DC's 14th Street Bridge, officials realized that the greater metropolitan area was in need of improved interoperable land mobile radio (LMR) communications systems. This tragedy uncovered the region's lack of compatible LMR systems as well as the limited solutions in place to support interoperability. In response to the various after-action reports describing the metropolitan area's communications systems during past events, the Metropolitan Washington DC, Council of Governments (COG) facilitated coordination among regional public safety agencies and the adoption of mutual-aid and interoperability agreements.

In light of recent terrorist attacks, natural disasters, and now, regional criminal activities, public safety agencies in the Washington, DC, metropolitan region have realized that interoperable communications are essential to the effective resolution of public safety issues. Further, multijurisdictional response often requires communication among local, state, and federal agencies. Because such events frequently require tactical communications among numerous groups of public safety personnel operating on disparate LMR systems, interoperable communications issues regularly pose problems that can impede joint public safety operations.

Interoperability is and will continue to be an issue that, if not addressed adequately, will be detrimental to the safety of public safety responders and the public.

1.3 Scope

This report examines the use of communications equipment, interoperability issues, and communications coordination efforts among participating agencies during the Washington, DC, area sniper response and investigation. It addresses both public safety LMR communications and commercially provided communications. The report includes general operational information related to response and task force communications, as well as operational and technical lessons learned related to communications interoperability between task force representatives. The intended audience for this report includes local, state, and federal public safety officials.

1.4 Organization

This report is composed of four sections, including this introduction. The remaining sections are organized as follows:

- **Section 2**—presents the methodology used to gather data and present the information contained in this report.
- **Section 3**—features background information regarding the sniper incidents, as well as an overview of various interoperability solutions used by participating agencies.
- **Section 4**—presents key lessons learned derived from an analysis of the data collected from both technical and operational perspectives.

The report also includes five appendixes following Section 4. These appendixes contain information that either provides additional context for the report or document additional lessons learned not specifically related to interoperability. The appendix descriptions are as follows:

- **Appendix A**—Features the interview guide used to assist in data collection.
- **Appendix B**—Provides system descriptions of the agencies affected by the sniper investigation.
- **Appendix C**—Provides a list of the agencies participating in the Police Mutual Aid Radio System (P-MARS).
- **Appendix D**—Provides lessons identified through project research but not specifically related to interoperability.
- **Appendix E**—Contains acronyms used in the report.

2. METHODOLOGY

To create this report, the PSWN Program developed a data collection plan composed of interviewing public safety officials, analysis, and identification of key findings. To begin the interview process, official letters were distributed to several key agencies that participated in the investigation. The PSWN Program formally requested participation from 10 local, 1 state, and 5 federal law enforcement agencies. The PSWN Program also requested that representatives from Nextel Communications, Inc., participate in an interview because the deployment of Nextel telephones contributed a significant component of task force interagency communications. Commercial service representatives from other companies were not interviewed because public safety interviewees identified Nextel as the primary commercial service that enhanced interoperability during the investigation. Table 2 lists the entities requested to participate in the interview process. The last column in the table notes whether the agency participated in the process. Note: Some of the non-participating agencies are mentioned throughout the document; this information is based on interviews with participating agencies.

Table 2
Data Collection Invitee List

Function	Agencies/Organizations	Participated
Local Law Enforcement	Alexandria Police Department (VA)	√
	Ashland Police Department (VA)	√
	Fairfax County Police Department (VA)	√
	Hanover County Sheriff's Office (VA)	√
	Montgomery County Police Department (MD)	
	Montgomery County Police Department Emergency 9-1-1 Communications (MD)	√
	Prince George's County Police Department (MD)	
	Prince William County Police Department (VA)	√
	Spotsylvania County Sheriff's Office (VA)	
	Washington, DC, Metropolitan Police Department	
State Law Enforcement	Maryland State Police	√
Federal Agencies	Bureau of Alcohol, Tobacco, Firearms, and Explosives	√
	Federal Bureau of Investigation (Baltimore and Richmond)	
	U.S. Customs Service	√
	U.S. Marshals Service	√
	U.S. Secret Service	
Commercial Wireless Services	Nextel Communications, Inc.	√

Interviews provided PSWN Program staff with a clear understanding of the private and public wireless communication systems used and the interoperability issues that arose, as well as information on the specific examples included in this report. To assist in conducting interviews, an interview guide was developed and used to ensure consistent types of information were

collected from each participant. The PSWN Program team used the guide as a tool to direct interview discussions rather than to collect quantitative information for statistical analysis. Interviewers used the guide to prompt questions and did not necessarily ask each question included in the guide. The interview guide is shown in Appendix A. Drawing from the interviews and associated research, PSWN Program staff analyzed the information, identified primary interoperable communications solutions employed during the sniper investigation, and formulated findings. Based on these analyses, a communications and interoperability discussion, along with key lessons learned, were developed. The lessons learned discussion may provide guidance for communications planners and law enforcement personnel for future efforts of this magnitude.

Figure 1 illustrates the process used to research the Washington, DC, area sniper response and investigation, interview representatives, analyze the information collected, and develop a report on key communications and interoperability issues and solutions. The lessons learned provide a high-level overview of the communications operational issues and the technical solutions used during the investigation.

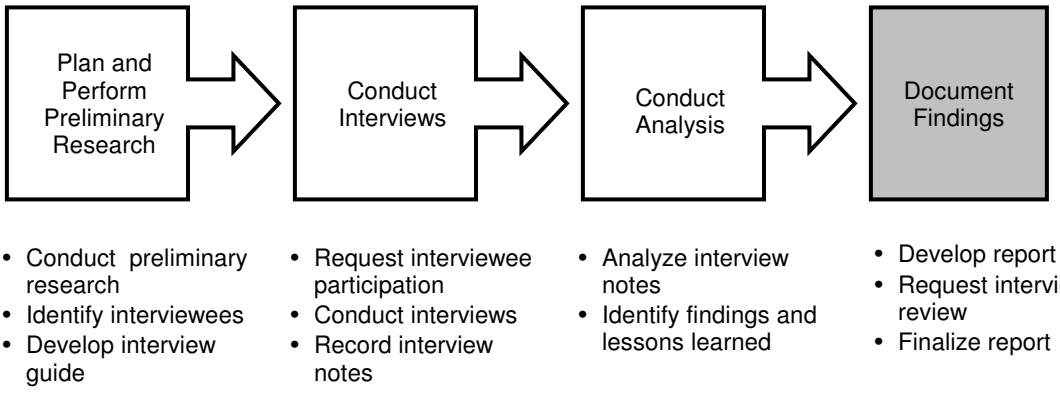

Figure 1
Sniper Investigation Communications After-Action Report Process Methodology

3. TASK FORCE COMMUNICATIONS AND INTEROPERABILITY SOLUTIONS

Over 3 weeks in October 2002, the sniper incident law enforcement task force investigation covered a large portion of the Washington, DC, area—from Frederick County, Maryland, to Richmond, Virginia. The area covered by the sniper investigation as well as the incident location is depicted in Figure 2. The expansive incident footprint and frequency of activities demonstrated that these shootings were a regionwide issue that needed immediate and coordinated response.

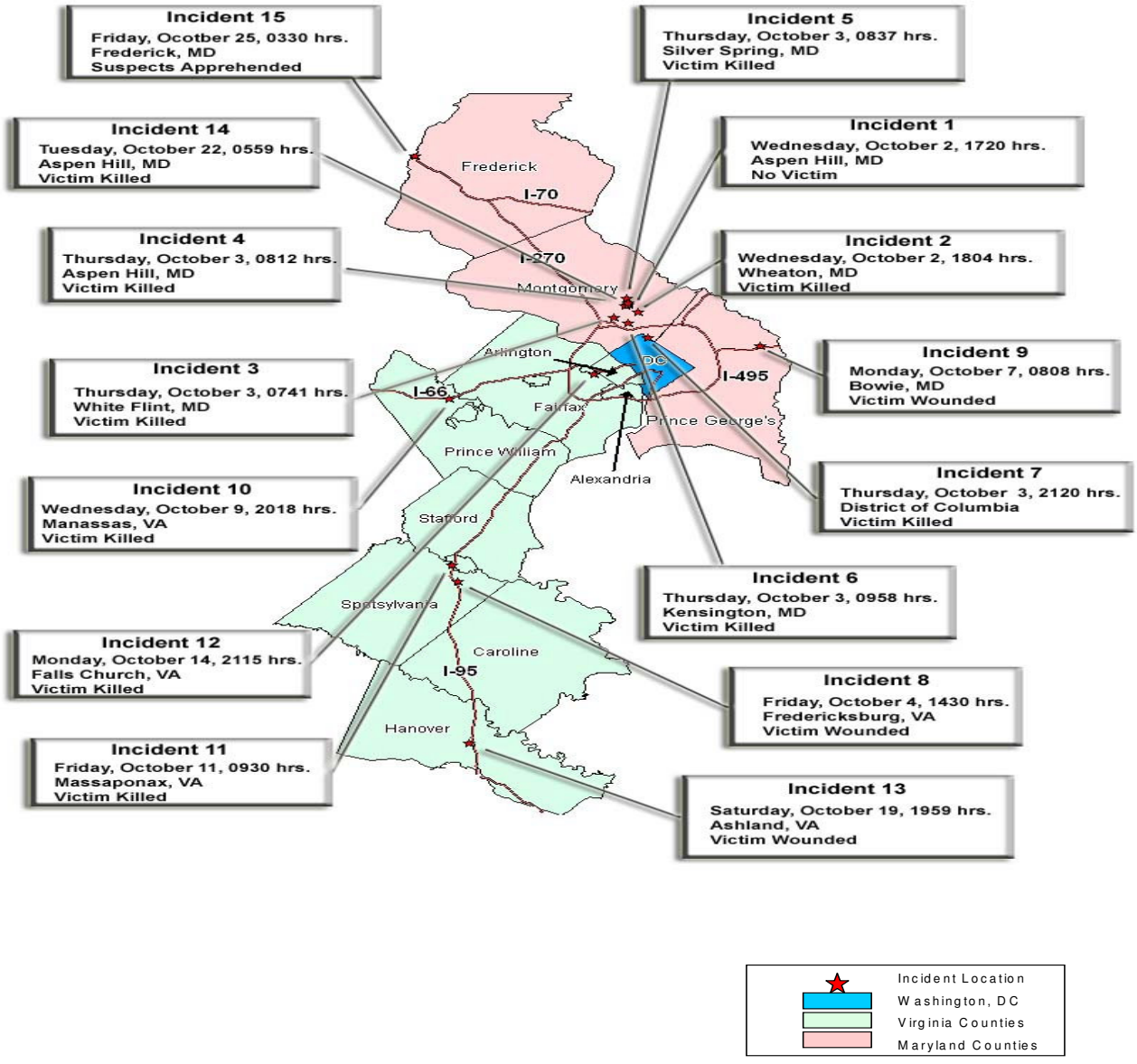

Figure 2
Washington, DC, Sniper Incident Locations

Officers and agents from local, state, and federal law enforcement agencies responded to and investigated individual incidents simultaneously, creating a unique operational environment not typically experienced in the law enforcement community. At some incidents, it was reported that upward of 300 local law enforcement officials from as far away as North Carolina responded. In addition, between incidents, hundreds of officers and agents worked in uniform and undercover, sometimes with little knowledge of the others' operations. On-scene commanders and task force commanders soon learned that establishing communications and interoperability between hundreds of task force responders would be a daunting task. As a result, communications managers and senior law enforcement personnel were faced with coordinating local, state, and federal agency response to incident scenes and managing communications at the task force investigation level.

3.1 Task Force Communications Overview

On the second day of the events (i.e., October 3, 2002), MCPD officials deemed that the series of shootings were being committed in a serial fashion and decided to form a multijurisdictional task force. The MSP offered MCPD its assistance followed by the ATF, which made agents available to take part in the growing investigation. Soon after, the FBI, USMS, USSS, and DoD all pledged assistance and staff to aid in the investigation. MCPD decided to create a formal investigative unit to coordinate response from the various agencies, which became the Montgomery County sniper task force, housed in the Joint Operations Center (JOC) in Rockville, Maryland.

After the formation of the task force, additional law enforcement personnel came to Montgomery County from all over the region to provide assistance with the investigation. As the progression of incidents began to spread across the region, several task force offices were set up to coordinate a more thorough and defined area response, specifically an investigative response to work leads. Additional task force locations included Fairfax County, Prince William County, and Richmond, Virginia; Prince George's County, Maryland; and Washington, DC. Before the task force investigation ended with the arrest of two suspects in Frederick, Maryland, more than 1,000 local, state, and federal law enforcement officers became involved in the task force.

As more and more officers and agents converged on incident scenes and spread out across the region following up on leads, the ability to communicate wirelessly between agencies became more difficult. Interoperability soon became a pressing issue for many agencies and required that command staff and communications officials respond.

3.2 Interoperability Solutions

During the course of the investigation, several interoperability solutions were deployed to enhance both tactical and administrative interoperable communications between hundreds of officers and agents using disparate communications systems. Some of these solutions were developed long before the sniper events began, while others were initiated or enhanced for this specific set of circumstances. The primary interoperability solutions deployed during the investigation included—

- Cross-system patch between MCPD's legacy UHF system and MCPD's new 800 MHz system
- Audio cross-connect switches
- Common system types and common frequencies across agency systems
- Police Mutual Aid Radio System (P-MARS)
- Radio exchanges
- Commercial wireless services.

Cross-System Patch Between MCPD's Legacy UHF System and MCPD's New 800 MHz System

MCPD command staff identified a need for enhanced interoperable communications as early as the morning of October 3. Early on Friday, October 4, Montgomery County communications officers began addressing interoperability shortfalls. MCPD officers had been using the county's Motorola, UHF, five-channel, conventional, analog radio system for conducting tactical communications in support of incident response and investigations. This system covered each of the six patrol districts in the county. Each patrol district had a dedicated channel for operations, and each channel had its own dispatcher. Conversely, federal agents and MSP officers initially assigned to the task force were using their mobile and portable radios on their disparate very high frequency (VHF) home systems to communicate within their own agencies but were not interoperable with other task force members. To make matters worse, the MCPD UHF system was overwhelmed with the volume of traffic coming in as local police responded to citizen reports across the area. The need to develop a solution to enhance interoperability and system capacity soon became apparent.

Fortunately, Montgomery County was completing the installation and testing of a new countywide, digital, trunked 800 MHz Motorola voice radio system to replace its existing UHF system. The 800 MHz system had been fully tested and was functioning properly but was not to be placed into service until the county's new emergency communications center was opened. A decision was made to press the new 800 MHz system into service and build a patch to connect the county's UHF legacy system to the new 800 MHz system. County communications officers hoped that once the patch was completed and tested, the county would be able to hand out 800 MHz radios to non-MCPD task force members for instant interoperability while MCPD officers continued operating on the UHF system. Further, the county could relieve some of the burden placed on its legacy system by adding capacity to address the sudden spike in voice traffic associated with the sniper attacks.

By mid-day on Friday, October 4, a permanent patch was established between the 800 MHz and legacy UHF radio communications systems in Montgomery County. The patch design was simple, connecting only two 800 MHz non-trunked frequencies to two of the UHF

alternative (non-dispatched) channels. Montgomery County's portable radio inventory was eventually assigned to the various ally agencies, including ATF, DoD, FBI, MSP, USMS, and others. MCPD distributed 250, 800 MHz portable radios for use by investigative personnel from those agencies and provided brief training to allow the new users to employ the radios for communications support while participating in the investigation.

Audio Cross-Connect Switches

Audio cross-connect switches, specifically JPS ACU-1000s like that shown in Figure 3, were deployed in Prince William and Fairfax counties and the City of Alexandria during the investigation. An audio cross-connect switch configuration, shown in Figure 4, can provide radio communications between agencies with disparate radio systems when they must interoperate. To provide interoperable communications during the sniper investigation, the audio cross-connect switches linked radio systems together and provided on-site interoperable communications.

Figure 3
JPS ACU-1000 Rack Mount

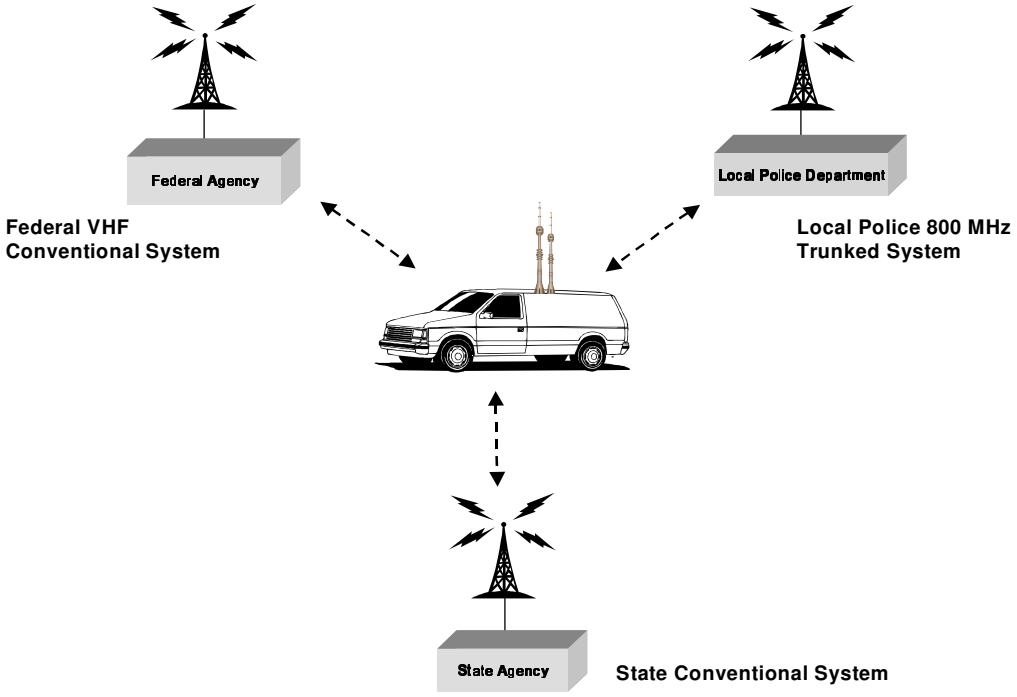

Figure 4
Generic Mobile Audio Cross-Connect Switch Configuration

PWCPD Deployment—Early in the series of sniper incidents the PWCPD requested that the USMS assist it with its surveillance efforts. In response to this request, USMS deployed approximately 40 marshals to assist in conducting these operations. For operational communications, USMS was using an Immigration and Naturalization Service (INS) VHF system, and PWCPD officers were using their UHF system, thereby prohibiting interoperability during these operations. Initially, each USMS investigator had to be paired with a PWCPD investigator to conduct surveillance and investigative operations to ensure communications across agencies. The short-term solution was radio sharing, but the lack of spare radios made this solution inadequate.

Identifying a key opportunity for interoperable communications support, USMS contacted the Alexandria Police Department. USMS requested that the Alexandria Police Department assist in providing an interoperability solution to link task force personnel in Prince William County using the Alexandria Police Department's mobile JPS Communications ACU-1000 mobile audio switch, which was provided to the Department as part of the National Institute of Justice (NIJ) Advanced Generation of Interoperability for Law Enforcement (AGILE) Program's test bed. Representatives from the Alexandria Police Department soon met with the Montgomery County Police task force, which authorized use of the ACU-1000 in Prince William County.

The Alexandria Police Department designated a communications officer to drive the mobile ACU-1000 unit out to the courthouse complex in Prince William County and to make it operational. This location provided good coverage throughout Prince William County. Alexandria personnel programmed the ACU-1000, using a Prince William County administrative channel and a USMS operational channel. The solution was effective in delivering on-the-spot interoperability between the USMS and PWCPD, furthering their ability to exchange communications during operations.

Fairfax County Deployment—The Fairfax County radio shop deployed its own ACU-1000 audio switch on top of the Massey Building in Fairfax City to support the Fairfax County task force. The primary goal of this deployment was to link the FCPD home 800 MHz system with the Statewide Inter-agency Radio System (SIRS). SIRS is a statewide low-band VHF system typically used by Virginia sheriff's department deputies when traveling to other jurisdictions. Because FCPD is already interoperable with other local agencies that use compatible 800 MHz systems (e.g., Alexandria, Arlington, Loudoun, Manassas, and Manassas Park), the switch provided interoperability between multiple local agencies and sheriff's offices across the state.

U.S. Customs Service—The U.S. Custom's Service deployed three helicopters to provide support in the Northern Virginia area during the investigation. Since the helicopters were not equipped with 800 MHz trunked radios, the VHF digital frequency used by U.S. Custom's helicopters was programmed into the Alexandria Police Department's Metropolitan Interoperability Radio System (MIRS) gateway ACU-1000 switch located at the Department's headquarters. This solution provided the capability to patch the helicopters directly to the 800 MHz trunked radio systems of the Alexandria, Arlington, and Fairfax County police departments. Several tests were conducted between the Customs Service's helicopters and patrol officers from the Northern Virginia agencies to ensure the crossband patch operated properly. A talk-around channel was also designated for general notification purposes.

Common Systems Types and Common Frequencies Across Agency Systems

Over the past 20 years, local agencies in the Washington, DC, area have worked diligently to implement compatible radio systems in an effort to ensure real-time interoperability across jurisdictions. Multiple law enforcement agencies, primarily in Virginia, currently operate compatible, digital, trunked, 800 MHz systems (see Appendix B for agencies with 800 MHz systems) as result of this coordinated effort. After these 800 MHz systems came on line, area leaders successfully put in motion a process to allow for units of each jurisdiction to access each other's system simply by programming other agency frequencies into their home radios. For the first time in the region, true interoperability was a reality for a great number of public safety agencies.

These compatible systems and radio programming efforts provided multiple agencies a readily available interoperability solution during the sniper investigation. Having repeatedly used the capability for mutual-aid responses, including during the Pentagon response in 2001, the responders had become familiar with frequency assignments. During the sniper incident

response and investigation, agencies switched to the designated frequency of other agencies and communicated directly with the affected jurisdiction immediately following an incident.

Once the new MCPD Motorola 800 MHz system was available, FCPD, also using a Motorola 800 MHz system, initiated procedures to quickly grant user privileges on the FCPD system for 600 task force members using the MCPD system. The hundreds of users on the MCPD system achieved real-time interoperability with FCPD simply by programming MCPD radios with Fairfax County's frequencies. The Fairfax County radio shop accomplished this by e-mailing appropriate system key numbers to the MCPD, whose officers programmed the information into their radios. Each user was then able to join a talk group, and the transmissions were automatically sent to any other users with the same talk groups.

Police Mutual Aid Radio System

During the Washington, DC, area sniper investigation, the Washington, DC, metropolitan area P-MARS was used sporadically for relaying initial shooting incident information across jurisdictions. Established during the mid-1980s under the sponsorship of the Washington area COG, P-MARS is used by area law enforcement agency communications centers for emergency notification messages and serves as a reliable interoperability solution during times of need. The system links local, state, and federal agencies in the region using a UHF radio system. Appendix C provides a list of P-MARS participating agencies.

Effective as a notification vehicle, the system is designed for dispatch center to dispatch center communications, although some law enforcement officers across the area can monitor P-MARS on their mobile or portable radios. Typically, information is broadcast over the system to notify the regional law enforcement agencies of multijurisdictional incidents. To eliminate the need for a memorandum of understanding (MOU) between all COG members, subcommittee membership serves as admission to P-MARS. The system is controlled by the Police Chiefs' Technical Committee and operationally maintained by the COG Police Chiefs' Police Communications Subcommittee, both of the Metropolitan Washington COG. System equipment is licensed, maintained, funded, and operated by the participating agencies.

Officials from FCPD indicated that whenever a sniper incident occurred, an emergency notification message was broadcast over P-MARS. However, some communications officials noted that P-MARS was not used routinely to broadcast incident information for several of the shootings. In fact, some law enforcement agencies learned of the sniper shootings through traditional media sources. To combat the sporadic and limited flow of initial incident information, communications personnel reviewed and revised their "communications plan" for major incidents. The changes included expanding the notification tree[1] and teletype recipient pool, as well as increasing the number of dispatcher positions. These changes ensured a wider dissemination of information to regional agencies.

[1] A notification tree is used to notify various entities of an occurrence in a specific order of priority.

Radio Exchanges

Radio sharing is a simple but reliable interoperability solution. Since portable radios became commonplace in law enforcement agencies, they have been loaned out when interoperability among officers from different jurisdictions was required. Agencies participating in the sniper investigation frequently exchanged radios, the most prominent example being the loan-out of hundreds of MCPD 800 MHz system portable radios to ATF, DoD, FBI, MSP, and USMS officials. Prior to the deployment of the ACU-1000 switch by the Alexandria Police Department in Prince William County, USMS had provided PWCPD with approximately 50–100 of its conventional VHF (138–174 MHz) radios to communicate with USMS during the sniper investigation.

Fairfax County also used some of its legacy VHF analog radios, programming them to operate on the 155.475 MHz local mutual-aid frequency. They supplied these radios to federal agents participating in the investigation in Fairfax County. Fairfax County Police provided the radios to federal agents on the sniper task force at the beginning of each shift. The radios were returned at the end of every shift and handed out again as new federal investigators came on duty.

Commercial Services

Nextel Direct Connect® mobile telephones and Nextel wireless service was identified by the majority of the interviewees as the primary commercial interoperability solution used during the sniper investigation for day-to-day, administrative law enforcement communications. Nextel Communications, Inc., uses Motorola's integrated Dispatch Enhanced Network (iDEN) which provided hundreds of officers and agencies with both traditional cellular and unique push-to-talk wireless communications service. Figure 5 shows the Motorola telephone supplied by Nextel to hundreds of officers and agents during the sniper investigation.

Figure 5
Nextel (Motorola R750) Telephone with Direct Connect Feature

Nextel mobile telephones and wireless services were used by numerous law enforcement officers across the region, particularly federal law enforcement agents, prior to the sniper incidents. Before the investigation started, ATF and FBI had used these mobile telephones throughout various field offices across the region. Federal law enforcement agents frequently used these telephones as their primary alternate communications device when exchanging non-sensitive communications. (Note: Sensitive communications exchange requires encrypted communications only available on private federal law enforcement LMR systems.) MCPD had also received a shipment of 225 Nextel mobile telephones before the sniper incidents started. In addition, MSP already had approximately 100 Nextel mobile telephones in its asset inventory.

As the sniper investigation expanded across the region, the requirement to communicate with a growing number of agencies also increased. It became obvious that officials needed to expand mobile telephone distribution and services for their officers and agents. Specifically, the need for a flexible, regionwide push-to-talk system, with talk group capabilities, grew hour by hour.

In the early stages of the investigation, Nextel received limited requests from local and federal agencies to procure additional mobile telephones for several agencies including ATF, FBI, and MSP. However, according to Nextel representatives, once the Montgomery County task force was formed, the FBI Crisis Incident Response Group contacted Nextel's Emergency Response Team (ERT) to provide a more formal interoperable communications solution for expanding task force investigation communications. Specifically, task force officials asked Nextel to provide hundreds of mobile telephones for its officers and agents, and more importantly, requested increased capacity and priority access to the Nextel infrastructure.

According to Nextel, the official order requested 300 mobile telephones for the task force members to use during the investigation. This included racks of batteries and battery charges to maintain the operation of the telephones. The order also included a cell-site-on-wheels (COW) to be deployed at the Montgomery County JOC to enhance coverage and ensure calls went through the system avoiding call blockages occurring because of intense wireless communications traffic along the Interstate 270 corridor. A COW diagram is shown in Figure 6. Finally, the order requested that six control base stations be installed at police dispatch locations across the region. Installation of Nextel's equipment began on October 15.

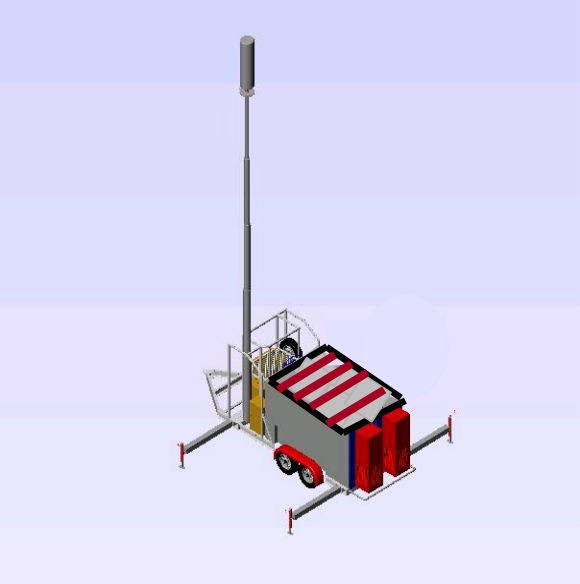

Figure 6
Depiction of Cell-site-on-Wheels Equipment Used During Sniper Investigation

Thirty Nextel ERT staff worked throughout the investigation to deploy the requested infrastructure and support task force operations. Members of the ERT were stationed primarily at the Montgomery County task force JOC as well as the MSP Headquarters near Baltimore, Maryland. Prior to the sniper investigation MCPD, ATF, and FBI all had Nextel telephones on agency specific fleets, enabling group call within their agencies as well as person-to-person capabilities across fleets. As the investigation grew, agencies recognized the need for additional talk groups and group communications across agency fleets. As a solution, all Nextel telephones supporting investigative efforts were reprogrammed onto a single fleet by the Nextel ERT and then configured into functionally based talk groups. During the investigation all Nextel telephones operated on a single fleet. At the close of the investigation, existing Nextel customers were reprogrammed back to their pre-existent fleets.

As mobile telephones were delivered, Nextel representatives provided instruction cards and trained law enforcement officers as needed. ERT staff participated in a series of meetings as the needs of the investigation task force changed over time. Reprogramming of talk groups was necessary as the task force teams changed. For example, users from MCPD, MSP, and FBI were moved seamlessly off of their home fleets and onto others.

Nextel provided proprietary priority access for the push-to-talk feature for the task force users. This feature, which was only available for public safety applications, gave the task force users network priority over other subscribers by moving their connection to the front of the queue.

Overall, by the end of the investigation, the agencies participating in the sniper investigation used approximately 1,400 mobile telephones. Based on information provided by Nextel, a number of agencies including MCPD, FCPD, MSP, FBI, and ATF were equipped with approximately 750 Nextel mobile phones prior to the investigation. The Nextel ERT deployed an additional 650 telephones to directly support the investigation. In fact, 150 of the loaned mobile telephones were issued to the Montgomery County School Board so that it would be notified immediately if another incident occurred. Approximately 350 mobile telephones were used on the multijurisdictional teams, which were rotated 12 hours on and 12 hours off. Nextel provided task force members from multiple agencies with the ability to talk in real time across the entire sniper investigation area. Specifically, the Nextel push-to-talk feature offered was available from western to eastern Maryland, as well as from central Maryland to southern Virginia. All major highways within the Maryland and Virginia area were also included in the coverage area.

4. LESSONS LEARNED

After analyzing the data collected from interviews with local, state, and federal agencies involved in the Washington, DC, area sniper investigation, several lessons surfaced. These lessons are categorized as either operational or technical in nature. Separating lessons learned into operational and technical categories makes it easier for readers to recognize that implementing effective communications and interoperable solutions during the sniper investigation involved not only technical solutions, equipment, and support but operational insight such as coordination and planning. These lessons are highlighted in Table 3 and described in this section. Appendix D contains communications center lessons that, although not specifically related to interoperability, were considered important findings.

Operational Lessons Learned	4.1.1 Preexisting relationships among participating agencies provided a foundation for effective interoperable solutions rollout
	4.1.2 Use of plain language transmissions, rather than 10-codes, enhanced interoperability between officers and agents from various agencies and jurisdictions
	4.1.3 Communications technical managers would have benefited from regular task force communications briefings and a post-investigation de-brief
	4.1.4 Lack of interoperability hindered search team communications
	4.1.5 Tactical communications planning prior to incidents enhanced operational responses
Technical Lessons Learned	4.2.1 Mobile telephones, provided by Nextel, enhanced administrative communications interoperability across the region and among participating agencies
	4.2.2 The Montgomery County radio system patch was instrumental in improving communications across the region
	4.2.3 Government and commercial communications technical staff were critical to successful deployment of communications systems and interoperable solutions
	4.2.4 Communications equipment training was critical for law enforcement officers who were unfamiliar with that equipment
	4.2.5 Interoperability across a large area and among multiple agencies required multiple solutions
	4.2.6 Interoperability between federal and state/local agencies was somewhat limited due to encryption issues

Table 3
Sniper Investigation Operational and Technical Communications Lessons Learned

4.1 Operational Lessons Learned

This section describes the non-technical findings associated with deploying interoperable solutions during the Sniper investigation. They include policy, coordination, and field operations related to communications and communications interoperability.

4.1.1 Preexisting Relationships Among Participating Agencies Provided a Foundation for Effective Interoperable Solutions Rollout

Several agencies involved in the sniper case had strong working relationships that were developed prior to the sniper shootings. These relationships were commonplace across the Washington, DC, area and had been growing due to the increasing requirements to respond to terrorism. New or enhanced relationships also developed between task force agencies during the sniper task force response and investigation. These working relationships proved to be beneficial to the sniper investigation and were especially critical in the planning and deployment of interoperable communications solutions.

For example, the existing operational relationship among the PWCPD, USMS, and the Alexandria Police Department provided the foundation for a key interoperable communications solutions deployment during the investigation. Early in the series of sniper incidents, the PWCPD requested that USMS assist it with its surveillance efforts. In response to this request, USMS deployed approximately 40 marshals to Prince William County to assist in conducting these operations. USMS quickly requested the assistance of the Alexandria Police Department for interoperability support. The existing relationship among these agencies provided the impetus to ensure quick and effective interoperability.

4.1.2 Use of Plain Language Transmissions, Rather Than 10-Codes, Enhanced Interoperability Between Officers and Agents From Various Jurisdictions

Given the multijurisdictional nature of the Washington metropolitan region, differences in communications-related terminology, codes, and even slang were widespread across the various municipal, county, regional, state, special district, and federal law enforcement agencies. Even when interoperability exists between responders, its value can be reduced quickly if the officials communicating do not understand each other because they use completely different codes or terms to explain what they are observing, where they are, or what they need.

"Plain language" protocols or procedures facilitate communication between personnel at the lowest common denominator by requiring that all officials talk to each other using common English language words, whenever possible, during mutual-aid or interoperability situations. This tactic was used successfully by officials in Montgomery County during their responses to sniper-related incidents and proved to be invaluable to the responding personnel regardless of agency, jurisdiction, or discipline. When the 800 MHz portable radios were handed out to local and federal agents in Montgomery County, it was decided that all radio users would refrain from using any types of codes, signals, or non-clear text communications when using the Montgomery County radio communication systems. The sniper incident helped to reinforce the concept that incorporating plain language as the operational communications standard detailed in any multiagency emergency response plans or exercises would solidify its importance and ensure that its use becomes a de facto standard during multi-agency or mutual-aid situations.

4.1.3 Communications Technical Managers and Task Force Participants Would Have Benefited From Regular Task Force Communications Briefings and a Post-Investigation De-Brief

A significant number of task force participants came from agencies and jurisdictions outside of the local, Washington, DC, metropolitan area. Many of them were unfamiliar with operational communications including local mutual-aid channel aliases, communications operating procedures, encryption procedures, and transmitter site coverage. Input received from interviews across agencies indicated that holding regular (i.e., daily) cross-agency communications briefings could have bridged many of these information gaps. Agency communications personnel indicated that such briefings often were held within a given agency, during the course of normal, daily operations, but not at the task force level. It was noted that the type of information exchange that typically might occur during a standard communications briefing would likely have greatly facilitated operations among task force participants in the field. Moreover, technical managers also would have benefited from a formal "post-investigation" de-brief that covered all of the communications and interoperability lessons learned during the investigation.

4.1.4 Lack of Interoperability Hindered Search Team Communications

On many occasions at incident scenes, officers from various jurisdictions were teamed with each other in the moments following an incident to perform searches for the perpetrator(s) or evidence within a defined geographic area. In some cases, a lack of interoperable communications between the searching officers hindered officers' ability to exchange information, request assistance, or provide status updates in a timely manner. Although some in-field operational solutions were employed, radio-based interoperability solutions would have increased the efficiency of the operations and drastically improved officer safety.

Searching for an armed suspect(s) immediately following a shooting event is an extremely high-risk operation for responding law enforcement officers. The fact that officers from multiple jurisdictions and levels of government responded to each sniper event introduced an additional layer of complexity based on differences in tactics, training, and operational procedures. When organized as "mixed" search teams, the ability to communicate both within each search team and across all search teams within a given geographic area was critical to officer safety. Interoperability in the Richmond region suffered most from a lack of interoperability during searches.

After the shooting in Ashland, Virginia, officers and K-9 units from various agencies participated in a grid search behind the Ponderosa Steakhouse. Officers from HCSO, HPD, RPD, VSP, FBI, and ATF all aided the grid search effort. Because the majority of these agencies did not have interoperable communications systems or equipment, the efficiency of the grid search was reduced because a member from each agency had to accompany each K-9 unit so that they could relay information back to the command post in the Ponderosa Steakhouse parking lot.

The command post helped to coordinate the investigation efforts, which included the grid search. RPD and HPD were interoperable because they both used a digital, trunked, 800 MHz

Motorola radio communications system. Although HCSO also operated an analog, trunked, 800 MHz system, its personnel could not communicate with the RPD and the HPD because the HCSO and RPD/HPD systems were proprietary in nature. Also, federal agencies and VSP were not interoperable with the other agencies participating in the grid search because of disparate technologies and spectrum.

Ashland Police Department personnel were able to interoperate with all Hanover County agencies that shared the regional 800 MHz system. HPD, CCPD, and RPD all communicated using the regional trunked Motorola 800 MHz system that they normally relied on for communications. These jurisdictions finalized negotiations to patch their Motorola system with Hanover County's M/A-COM system prior to the sniper investigation. Although Ashland Police Department was interoperable with Hanover County as well as the City of Richmond and Henrico County using the 800Mhz, National Public Safety Planning Advisory Committee (NPSPAC) channels, they were not utilized during the incident.

4.1.5 Tactical Communications Planning Prior to Incidents Enhanced Operational Responses

Once the shootings were attributed to a serial sniper, tactical communications planning became important to future operational responses. Planning for potential event response, on-scene command and control, and subsequent investigations were a strategic function that encompassed communications. Many agencies or groups of agencies developed tactical communications plans to enhance their overall response.

The primary example of effective communications planning was demonstrated with the Richmond Regional Sniper Response Plan. This plan included several agencies in the Richmond area including those in Hanover County, Henrico County, and the City of Richmond. Following the shooting incident in Spotsylvania County on October 11, Richmond area law enforcement and communications officials decided to develop a formal response document known as the Richmond Regional Sniper Response Plan. Tactical response planning was important in this area because agencies did not have interoperable radio systems to rely upon like those in Fairfax County or other agencies in the Washington, DC, area. Although both Hanover and Henrico counties have 800 MHz systems, they are from different vendors, therefore preventing interoperability across systems.

The Richmond Regional Sniper Response Plan served as a blueprint for operations that would immediately follow a sniper incident. Communications were a key component of this plan. Specific elements of the plan included—

- Designation of the radio channel of the "affected jurisdiction" to be used as the key communications channel for the initial response to the incident

- Regional channels for the command post, surveillance units, and tactical units following the initial response

- Comprehensive notification tree
- Statewide notification teletype
- Temporary console patches to establish interoperability with HCSO and other jurisdictions in the area
- Designation of "plain talk" rather than 10-codes as the primary communications language.

The Fairfax County Police Department, in its role as a secondary sniper task force location, began planning communications formally on Saturday, October 5. Sixteen agencies including Alexandria, Fairfax City, Loudoun County, VSP, FBI, USSS, USMS, and ATF were a part of the FCPD task force component. Communications was a key topic of the discussion at the initial task force conference call on October 5, and a formal regional task force plan was developed. This plan specifically included a communications component with information on assigning radios, channel use related to response communications, command communication at an incident scene, and equipment to be used for task force administrative communications. One important part of this plan included specific instructions not to share any secure information over cellular telephones or non-encrypted radios. The preference was to transmit sensitive information only over landline telephones.

4.2 Technical Lessons Learned

This section describes the lessons learned associated with the communications technology used to support the sniper response and investigation. These findings center on the communications capabilities and associated technical assistance available to users during the investigation.

4.2.1 Mobile Telephones, Provided by Nextel, Enhanced Administrative Communications Interoperability Across the Region and Among Participating Agencies

During the course of the Washington, DC, area sniper investigation, the equipment, wireless services, and technical support supplied by Nextel Communications, Inc., fostered interoperable communications between members of the sniper task force. Nextel provided an interoperable communications solution to approximately 1,400 officers and agents working on a multijurisdictional/multi-agency effort that spanned a large area. The solutions included telephones, COWs, control stations, and priority access arrangements for the system. The Nextel ERT was able to deploy several engineers to the region, set up infrastructures to support operations, plan and program talk groups, and provide ongoing technical support to the task force.

4.2.2 The Montgomery County Radio System Patch Was Instrumental in Improving Communications Across the Region

As it became evident that Montgomery County would be a hub for investigative operations, additional law enforcement officers and agents were assigned to the Montgomery

County area. A quick and maintainable solution to patch Montgomery County's legacy UHF and new 800 MHz system was required to ensure interoperability across primary task force participants as well as decreasing the loading on the legacy system. Montgomery County worked closely with Motorola to facilitate the patch connection between the two systems over only 1 day of work. This patch quickly enabled a significant level of interoperability to both local officers and federal agents, and because the new 800 MHz system provided coverage beyond Montgomery County, it greatly expanded the tactical communications operational area for MCPD officers and the task force.

4.2.3 Government and Commercial Communications Technical Staff Were Critical to Successful Deployment of Communications Systems and Interoperable Solutions

Government and commercial wireless services technical staff, knowledgeable in law enforcement communications requirements and interoperability, provided a critical support function throughout the course of the sniper investigation. Because a significant amount of LMR and Nextel subscriber equipment was being used by task force operatives, dedicated and competent support staff who knew the intricacies of their respective "home" systems proved to be invaluable in maintaining seamless, uninterrupted communications capabilities. Further, given the amount of reprogramming required for radios and Nextel telephones used by task force members not local to the area, without a dedicated technical staff, the logistics of "inserting" required frequencies alone would have proven to be a significant obstacle to establishing interoperable communications in a timely manner. The ability to troubleshoot equipment, ensure proper battery management, establish links/patches, etc., all in real time, significantly supported the task forces ability to accomplish its mission.

Several technical staff members, including representatives of ATF, FBI, and Nextel, worked around the clock at the Montgomery County task force headquarters. Other communications staff representing the Alexandria Police Department, FCPD, MCPD, MSP, ATF, USMS, Motorola, and Nextel worked diligently across the region to set up quick, usable communications solutions. For example, a full-time communications technical staff was critical to patching the existing UHF radio communications system in Montgomery County with the county's new 800 MHz radio communications system. A critical task performed by these staff was the establishment of two talk groups for the federal agents on the 800 MHz portable radios. These talk groups were designed so they could be monitored from the task force headquarters in Montgomery County. The 800 MHz radios were also set up so that they did not connect directly to the dispatcher in an effort not to overload dispatch operations.

Immediately following the third shooting, ATF radio support staff began working to enhance communications capabilities for ATF. Staff set up radio communications console capabilities at the Montgomery County task force headquarters. They also quickly planned and built out two additional repeater sites to fill identified ATF coverage gaps across the region for ATF's VHF system. In addition, ATF handled all of the tasks associated with radio management during this operation, specifically the encryption and programming problems associated with out-of-town agents coming from an analog to a digital radio environment. Issues such as encryption key management and radio maintenance were handled readily by ATF. Finally, ATF ensured

interoperability with helicopter operations (i.e., USCS and DoD) by providing ATF VHF radios to aircrew members.

Also, the Nextel ERT deployed approximately 30 staff members to assist task force components. They worked to distribute and program telephones, set up talk groups, deploy COWs across the region, and train users. The deployment of hundreds of Nextel telephones and the support provided by the Nextel ERT during this operation aided in the success of sniper task force interoperability for administrative conversations.

4.2.4 Communications Equipment Training Was Critical for Law Enforcement Officers Who Were Unfamiliar With That Equipment

As federal agents were tasked to join the sniper investigation, the need for deploying additional radios was identified. However, most federal agents were not familiar with local agency radio equipment. As a result, radio user training was provided to minimize the delay in effective operational use of the radios.

For example, as Montgomery County's new 800 MHz system was pressed into service, the inventory of portable radios was assigned to the various agencies including the FBI, ATF, USMS, DoD, and USSS. Agents and officers using this new system and associated radios were provided radio user training. Specific instructions were provided to the users regarding unit identifications as well as methods to contact the dispatchers, task force command post, and each other. Instruction was also given to the radio users to refrain from using any types of codes, signals, or non-clear text communications over the Montgomery County radio communication systems.

4.2.5 Interoperability Across a Large Area and Among Multiple Agencies Required Multiple Solutions

Installation of a system patch, deployment of audio cross-connect switches, and common radio-sharing arrangements were only a few of the interoperability solutions deployed during the sniper investigation. The fact that many different solutions were deployed should provide law enforcement executives and communications personnel a lesson that there are no "one-size-fits-all" interoperability solutions. Interoperability solution deployments frequently depend on the area of operation, agencies involved, existing systems, and information to be exchanged. Local, state, and federal agencies would be well advised to develop possible scenarios in their region and identify alternate interoperability solutions that could provide interoperability across systems during those scenarios.

4.2.6 Interoperability Between Federal and State/Local Agencies Was Somewhat Limited Due to Encryption Issues

Due to the sensitive nature of federal law enforcement communications, many federal agencies communicate only over encrypted radio channels and adhere to the Advanced Encryption Standard (AES) developed by the National Institute of Standards and Technology. Conversely, most non-federal agencies do not require encrypted communications, although some local public safety organizations use encryption for various tactical operations like narcotics

investigations. The lack of encryption capabilities among local sniper investigation participants caused some federal agencies to refrain from patching their frequencies through locally controlled audio switches and across local systems. As a result, the application of federal-to-local interoperability solutions was limited for task force participants.

APPENDIX A—INTERVIEW GUIDE

This guide was used by the PSWN Program team as a tool to direct interview discussions rather than to collect quantitative information for statistical analysis. Interviewers used the guide to prompt questions and did not ask each question in the guide.

I. Demographic Information

1. Please provide the following personal information

Name	Position/Division	Agency Name & Mailing Address
Phone & Fax Number	Email & Web Address	May we contact you in the future? (If yes, indicate any restrictions)
(P)		Yes _____ No _____
(F)		
(F)		

II. Background

1. When did your agency become involved in the sniper investigation or response?

2. What were your agency's responsibilities?

3. Describe the resources your agency provided for the investigation and incident response (e.g., officers, agents, equipment).

4. What was the primary information sharing method between your agency and other agencies or task force command? Describe.

Regularly scheduled briefings	
Ad-hoc in-field updates	
As necessary over radio/commercial networks	
Other	

5. Which outside agency(ies) did your agency directly coordinate with during the investigation?

II. Task Force and Incident Response Communications

1. What communications procedures/policies did your agency use, update, or create to ensure adequate communications were available for agency staff to respond to task force or incident response needs?

2. During your participation in ***task force activities***, what was your primary communications method?

Home agency's radio system (describe)	
Another agency's radio system (describe)	
Commercial network (cellular/ESMR)	
Other (identify)	

3. During your participation in ***incident response***, what was your primary communications network(s)?

Home agency's radio system (describe)	
Another agency's radio system (describe)	
Commercial network (cellular/ESMR)	
Other (identify)	

4. Were any commercial communications devices deployed to your agency?

Yes No

What impact did they have on your agencies ability to communicate?

5. Which agency(ies) did your agency require voice communications during the investigation or response?

6. Were there standing or established communications ***interoperability*** processes and methods used by your agency during the investigation or response?

Yes No

If so, what were the methods and how were they implemented?

7. Were there established communications processes for multi-agency response to additional incidents or reported suspicious activities?

Yes No

If so, what role did interoperability play during actual multi-agency responses?

8. During the investigation, was there a process through which you could get technical support for communications needs? (i.e. radio trouble shooting or repair, commercial service assistance, other)

9. What communications capabilities existed with the military assets that were pressed into service to support the response and investigation of these incidents?

10. Did your center have direct communications with air borne law enforcement (ABLE) units?

	Yes	No
Your jurisdiction		
Other neighboring city/county jurisdictions		
State agencies		
Federal agencies		

III. PSAP Center Operations and Communications

1. How was event information, supplemental information, and investigative information disseminated from the Center to the following?

Local officers	
Task force officers	
Neighboring jurisdictions (which ones)	
Media	

2. Subsequent to the first incidents being identified as a serial event with the likelihood of additional events, what changes were instituted in center operations?

	Yes	No
Dispatch policy changes (number of units to calls)		
Staffing changes (additional console staffed, additional personnel)		
System reconfigurations (jurisdiction split/combined for normal traffic)		
Dedicated channel/talk groups for specific operations		

3. Did/does your communications center support any fixed interoperability solutions within the communications systems infrastructure?

	Yes	No
ACU-1000 or similar switching mechanism		
Temporary or permanent console patching		
Control/base stations of distant systems		
Other I/O solution (identify)		

4. Are mobile data communications available in your jurisdiction?

Yes No

If so, were they used specifically during the sniper events?

Yes No

If so, how were they used during the sniper events?

	Yes	No
Routine/normal call for service dispatching		
Broadcast messaging/unit to unit messaging		
Investigate access to State/NCIC		
Interoperability with neighboring jurisdiction		
Other (identify)		

5. After the initial shooting events, 800-telephone tip lines were setup –

Did your agency/communications center participate in these lines?

Yes No

Was this information disseminated to the task force office?

Yes No

How were overflow conditions on 911, 7-digit, and 800 tip lines handled immediately subsequent to another shooting?

Describe the impacts on routine operations or communications processes?

6. How were normal telephone and dispatched call loads impacted?

Are there statistics available? Yes No

7. Was the task force provided specific, segregated channels, frequencies, or talk groups to operate on during initial response or follow-on investigations?

Yes No

Were specific dispatch resources assigned to these?

Yes No

8. After the initial shootings, were subsequent shooting calls handled differently? Explain.

9. Subsequent to the initial response and confirmation of a connected serial shooting –

   How was the communications from on-scene to the actual communications center handled?

   Were communications directed to specific channels, talk groups, or frequencies? Why?

   Were multiple channels used for a scene?

   Was encryption/scrambling used?

   Yes No

   Were there any impediments/overcrowding?

10. Did your center track and maintain the status of outside resources (other city, county, state, and federal) that were performing various assignments within your jurisdiction?

    Yes No

If yes, then how was this accomplished?

Who and what was tracked?

How were communications facilitated between the center and these outside resources?

APPENDIX B—WASHINGTON, DC, AREA AGENCIES AFFECTED BY SNIPER INCIDENTS AND RADIO SYSTEM DESCRIPTIONS

Function	Location	Agency	Radio Communications System	
			System Type	Frequency Band (Megahertz)
Local Law Enforcement	District of Columbia	Washington, DC, Metropolitan Police Department	Analog, Conventional	460 (UHF)
	Maryland	Montgomery County Police Department	Analog, Conventional	490 (UHF)
			Digital, Trunked	800
		Prince George's County Police Department	Analog, Conventional	490 (UHF)
	Virginia	Alexandria City Police Department	Digital, Trunked	800
		Arlington County Police Department	Digital, Trunked	800
		Ashland City Police Department	Analog, Trunked	800
		Chesterfield County Police Department	Digital, Trunked	800
		Fairfax County Police Department	Digital, Trunked	800
		Hanover County Sheriff's Office	Analog, Trunked	800
		Henrico County Police Department	Digital, Trunked	800
		Manassas Park City Police Department	Digital, Trunked	800
		Manassas City Police Department	Digital, Trunked	800
		Richmond City Police Department	Digital, Trunked	800
		Spotsylvania County Sheriff's Office	Analog, Trunked	800
		Prince William County Police Department	Analog, Conventional	453 (UHF)
State Law Enforcement	Maryland	Maryland State Police	Analog, Conventional	39 (Low Band VHF)
	Virginia	Virginia State Police	Analog, Conventional	138–174 (High Band VHF)
Federal Law Enforcement	United States	Bureau of Alcohol, Tobacco, Firearms, and Explosives	Digital, Conventional	138–174 (High Band VHF)
		Customs Service	Analog, Conventional	138–174 (High Band VHF)
		Drug Enforcement Administration	Analog, Conventional	406–420 (UHF)
		Federal Bureau of Investigation	Analog, Conventional	138–174 (High Band VHF)
		Marshals Service	Analog, Conventional	138–174 (High Band VHF)
		Park Police/Aviation Division	Not Available	VHF/UHF
		Secret Service	Analog, Conventional	138–174 (High Band VHF)

APPENDIX C—WASHINGTON, DC, METROPOLITAN AREA POLICE MUTUAL AID RADIO SYSTEM (P-MARS)

The agencies that participate in the Washington, DC, Area P-MARS include—

Alexandria City Police
Arlington County Police
Central Intelligence Agency Security Protective Service
Defense Protective Service
Fairfax City Police
Fairfax County Police
Falls Church Police
Federal Bureau of Investigation Washington Field Office
Federal Protective Service
Frederick Police
Herndon Police
Loudoun County Sheriff
Maryland State Police–College Park
Maryland State Police–Forestville
Maryland State Police–Rockville
Metropolitan Police
Metropolitan Washington Airports Authority Police
Military District of Washington–Fort Belvoir
Military District of Washington–Fort McNair
Montgomery County Police
Montgomery County Park Police
Naval Investigative Service
Prince George's County Police
Prince William County Police
Supreme Court of the United States Police
Takoma Park Police
University of Maryland at College Park Police
U.S. Air Force–Andrews AFB
U.S. Capitol Police
U.S. Marshals Service
U.S. Park Police
U.S. Secret Service–Uniformed Division
U.S. Secret Service–Washington Field Office
Vienna Police
Virginia State Police

APPENDIX D—ADDITIONAL LESSONS LEARNED

Two key lessons learned were identified that are outside the scope of the report. Both are related to public safety answering points (PSAP) and communications centers. They are described below.

D.1 An Automated Tip Sheet (for Citizen Telephone-in Tips) Would Have Been Invaluable to Support Follow-Up Queries and Lead Analysis

During the sniper investigation, thousands of tips from citizens came into the Montgomery County PSAP or communications center. These tips were documented on hard-copy forms by communications technicians rather than on electronic forms, making the analysis of the information on the forms time intensive. Montgomery County communications personnel indicated that the use of a records management system or other automated systems to gather, analyze, and report tip information without the need to re-enter and/or manually analyze the information, would have been valuable.

D.2 Establishing a Tip Line Requires a Readily Available "800 Number" and Bank of Telephone Landlines

As the shooting events progressed over the first 2 days, it was evident that the Montgomery County communications center staff would continue to be inundated with "tip" calls as well as the normal load of calls for police, fire, and emergency medical services. A decision was made to establish a "tip line" using a local (non-800) line at another location to take these tip calls. The intent was to remove as much of the call volume from the communications center as possible and establish a dedicated call center to handle the sniper information more effectively. The county's Department of Technology Services established the required telephone facilities in the newly built County Emergency Communications Center, which was still partially under construction. This tip center was located in the situation room of the new communications center and supported 12 telephone positions accessible through a local telephone number. The local number was broadcast to the public through the news media. The tip center did not have an automated system to facilitate the collection of the tip information from the calling public, and all information was manually recorded on paper "tip sheets."

Once the tip number was broadcast in the media for a short period of time, the tip center became overwhelmed, and the number of incoming tip calls again began to rise on the 911 and administrative lines. More than 15,000 calls were made to the sniper hotline by midnight on Tuesday, October 15, bringing the total number of calls received after the hotline was established to more than 69,500. Fortunately, Montgomery County had a facility that was available and had sufficient incoming telephone resources to support this 12-position call center. Additional trunk lines could have been acquired from the local telephone company to provide additional capacity as required, but the tip center was soon moved to another facility and an 800 number was established.

APPENDIX E—ACRONYMS

AACOPD	Anne Arundel County Police Department
ACPD	Arlington County Police Department
AES	Advanced Encryption Standard
AGILE	Advanced Generation of Interoperability for Law Enforcement
ATF	Bureau of Alcohol, Tobacco, Firearms, and Explosives
CCPD	Chesterfield County Police Department
COG	Council of Governments
COW	Cell-site-On-Wheels
DEA	Drug Enforcement Administration
DES	Digital Encryption Standard
DoD	Department of Defense
ERT	Emergency Response Team
FBI	Federal Bureau of Investigation
FCC	Federal Communications Commission
FCPD	Fairfax City Police Department
FCSO	Frederick County Sheriff's Office
FPD	Fairfax County Police Department
HCPD	Howard County Police Department
HCSO	Hanover County Sheriff's Office
HPD	Henrico County Division of Police
iDEN	integrated Dispatch Enhanced Network
INS	Immigration and Naturalization Service
JOC	Joint Operations Center
LCSO	Loudoun County Sheriff's Office
LMR	Land Mobile Radio
MCPD	Montgomery County Police Department
MHz	Megahertz
MIRS	Metropolitan Interoperability Radio System
MOU	Memorandum of Understanding
MPDC	Metropolitan Police Department
MPPD	Manassas Park Police Department
MSP	Maryland State Police
NIJ	National Institute of Justice
NPSPAC	National Public Safety Planning Advisory Committee
PGCPD	Prince George's County Police Department
P-MARS	Police Mutual Aid Radio System
PSAP	Public Service Answering Point
PSWN	Public Safety Wireless Network
PWCPD	Prince William County Police Department
RPD	Richmond Police Department
SBU	Sensitive But Unclassified
SIRS	Statewide Inter-agency Radio System
TPPD	Takoma Park Police Department
UHF	Ultra High Frequency
USCS	U.S. Customs Service

USMS	U.S. Marshals Service
USPP	U.S. Park Police
USSS	U.S. Secret Service
VHF	Very High Frequency
VSP	Virginia State Police
WCSO	Washington County Sheriff's Office