I. Introduction

This paper presents a technical overview to the use of video networks by law enforcement and emergency management agencies. The paper discusses the general approach and technical solution applied to implementing the Washington, DC remote video surveillance system. In the paper we also address the key issues associated with policy and procedures that guide the use of video monitoring by public agencies. This paper was written by Winbourne & Costas, Inc. of Washington, DC and XRAM of Herndon, VA.

II. Expanding Resources for an Expanding Mission

There is an emerging recognition among law enforcement and emergency management agencies that access to video monitoring assets can have a major impact on their effective management of emergency situations, which confront them on an all too frequent basis. Video surveillance can be used to monitor critical infrastructure on an ongoing basis, as well as in support of emergency response to the range of situations from man-made to natural disasters. In all cases, these services have the following requirements:

To compensate for increasingly complex demands, local police departments are increasingly turning to video technology to supplement their mission. The International Association of Chiefs of Police (IACP) says that over 80 percent of US police organizations use video surveillance.

- Ability to monitor multiple sites simultaneously
- Capacity to receive a full range of transmission resources from multiple sources
- Share and receive video data with federal and other local and regional agencies

Presently, most emergency management agencies do not possess their own video resources. Instead, many obtain feeds from other agencies such as transportation and law enforcement. Regardless of the source of the video feed, emergency management agencies will increasingly require new sources of video, as well as their own assets. In the event of a disaster, such as the release of a chemical of biological agent, emergency management agencies may need to quickly quarantine large areas. The ability to monitor and view the area by key decision makers could enhance the ability of the agency to provide the correct resources in a timely and effective manner.

The Washington, DC Experience

"We don't have enough officers to watch everything," states a senior Washington DC police official. Video monitoring "allows us to monitor more places and frees up officers to do their work in the neighborhoods."

Over the past two years, the Washington DC Metropolitan Police Department (MPD) has developed a multi-channel video monitoring system for the downtown area of the nation's capital. The video network utilizes multiple network configurations that allow MPD and its partners to share video data.

Starting in 2000, the Washington DC microwave system was designed to provide law enforcement officials images from a variety of sources including helicopter based video, as well as street and roof top surveillance. The wireless nature of the system provides flexibility to rapidly reconfigure surveillance assets, depending on the nature of the event. The system was designed and implemented as part of MPD's strategy to prepare for various upcoming large-scale events, including the Presidential Inauguration, and a series of World Bank –IMF meetings and the associated demonstrations. During the September 11th terrorist attack, the system was used extensively to monitor operations-critical buildings and thoroughfares in the nation's capital.

"The video technology is state-of-the-art, fully computerized switching equipment that is very similar to that you would find in a NASA or defense command center, stated Stephen J. Gaffigan, the MPD project director. The video display capabilities of the new Joint Operations Command Center (JOCC), jointly staffed between MPD, FBI and Secret Service, allows for a wider field of vision to operational commanders.

The video system was designed and implemented by Winbourne & Costas, Inc. and XRAM, Inc. to integrate with the JOCC and the cameras through a microwave network back to MPD and other participating law enforcement organizations. Eventually, the Washington system will bring together cameras operated by different jurisdictions across the metropolitan area to include transportation, schools and potentially private security sources. Law enforcement officials will be able to view these images at the command center and broadcast the video to computer units already installed in most of the city's 1,000 patrol cars.

III Technical Challenges and Solutions

Implementing the video surveillance system in Washington, DC presented a number of technical challenges. During the design phase, a wide range of locations, camera types, and transmission methods were considered and tested during several large events ranging from International Monetary Fund-World Bank demonstrations, the Presidential inauguration to sporting events. During this phase, MPD leased camera and antenna equipment and utilized the FBI microwave network when possible. MPD's operational

requirements lead to a design that combined remote security monitoring with a broadcasting system that could utilize traditional IP networks as well as wireless and Fast Ethernet transmission technologies. In addition, the network needed to provide the bandwidth that could allow for recording and redistribution of video signals without affecting the available use of wireless bandwidth.

Command Center Role--Central to the success of the video network is the role played by the command center receiving and managing the data. The MPD JOCC was designed with the intention of extensively using video as well as data and voice inputs to monitor events and manage resources. The video network planning and implementation process was integrated in the overall functionality of the JOCC with full redundancy and security.

Video Management Tools--A significant challenge is managing and filtering the volume of video now available to MPD. We have developed a set of tools to achieve the following video management requirements:

Management Tool Needs	Tool Availability and Description
Remote Control and Diagnosis to Identify the Condition of Remote Equipment	• Several custom software utilities were developed to enhance the ability to maneuver and control the condition of all of the components involved in the camera units
Recording with Playback/Reverse, Playback/Loop and Playback/Accelerated Playback	• Additional software utilities were created to simulate advanced broadcast recording equipment.
Video Feed Preview and Caching	• All video feeds can be previewed from any computer, this allows for a distributed (different individuals, departments or agencies) screening of the incoming video sources. • Video feeds are cached or recorded at the first point of entry into the Local Area Network (LAN) to allow for a less expensive bandwidth and redistribution to authorized parties. MPD assigns the screening of these video feeds to the intelligence component of the JOCC.

Video Network--The key components of the network are the following:

Integrated Web Server—The integrated web server allows you to remotely control the devices from any location. Each camera in this case is assigned an IP address on the network.

Web-based Remote Access—The type of wireless cameras used can stream video to any location using the Internet. The streaming video can be viewed on virtually any Internet enabled device including wireless mobile notebooks or wireless PDAs.

IEEE 802.11b Wireless and 802.3/3u Ethernet—The cameras used in Washington, DC are WiFi compatible with IEEE 802.11b wireless and IEEE 802.3/3u 10/100 Fast Ethernet network connectivity. The use of the wireless transmission allows MPD to move the camera to any location they require with set-up time of less than 2 hours. The signal transmission can support passing the signal to multiple IP networks.

This type of wireless camera can stream video to any location using the Internet. The streaming video can be viewed on virtually any Internet enabled device including wireless mobile notebooks or wireless PDAs.

Motion Sensors and E-mail Notification—This feature allows for notification whenever the input devices to take a snap shot. The cameras are configured with add-ons such as motion and infrared sensors, so that the user is instantly notified once a device is triggered.

Distributed Wireless Technologies like Ricochet or the emerging broadband cellular communications will allow for an even faster unplanned deployment. The availability of a "WAN" throughout urban areas will permit installation of the cameras virtually anywhere.

Licensed Vs. Unlicensed Radio Spectrum

Camera images sent wirelessly between two points using 802.11'X' technology is accomplished by sending the images between two line-of-sight antennas, more correctly called radios, operating on the same frequency. Licensed radio frequencies promise better communication between the radios since a frequency cannot be shared legally. However, radio equipment, of any type that uses licensed frequencies, is generally more expensive and less available. It is not unusual for this equipment to cost 3 to 4 times more than their unlicensed counterparts. Using the licensed microwave frequencies also increases other equipment costs and increases procurement time, usually adding 3 to 4 weeks. Since the radio equipment operates line-of-site, the risk of interference using unlicensed radio frequencies is minimized. This factor is a critical design consideration since that radios using licensed frequencies are also subject to interference, intentionally generated or unintended/collateral.

IV. Use of Video and Privacy Concerns

The expanded use of video surveillance for law enforcement has spurred privacy concerns from many quarters. The public policy issues related to the use video systems for law enforcement is an ongoing debate framed by concerns emanating from numerous sources.

In the United States, video surveillance is a wide spread activity. Most transportation centers such as airports, rail stations and bus terminals have used video for many years. Most public building security operations use video surveillance for monitoring activities in the facility. Areas frequented by tourists, such as Baltimore's Inner Harbor and Washington's Georgetown section are typically monitored by video. Some cities have also put cameras in busy intersections to gauge traffic or catch drivers who run red lights. In many ways, Great Britain has taken the lead on video monitoring usage. In response to terrorist activities in the 80's, the government has placed more than two million surveillance cameras throughout the country in recent years.

Impact of the September 11th Terrorist Attack-- The events and reaction to the September 11th terrorist attack have contributed to the policy debate. The value of the video monitoring was illustrated by the actions of the Washington, DC Metropolitan Police Department (MPD) and federal law enforcement agencies such as the FBI and US Secret Service (USSS) in response to this unprecedented assault on our nation. Once notified of the attack the MPD, FBI and USSS activated their new Joint Operations Command Center. Officers from other law enforcement agencies including Capitol Police, Park Police and Amtrak Police combined forces in the JOCC and in the streets to monitoring key buildings and events around Washington. The new wireless video network, populated with pre-positioned programmable remote cameras, provided a unique advantage to all emergency responders to effectively manage resources and security needs.

Media Coverage of Video Capabilities--Subsequent to these events, a debate has emerged over the use of video surveillance by law enforcement organizations. The Wall Street Journal, the Washington Post and Washington Times newspapers as well as the major television networks have commented on the use of video surveillance in the nation's capital. The articles note that there are few legal restrictions on video surveillance in city streets. Concerns for potential for abuse have prompted a debate over policy solutions.

Policy Issues and Requirements--Some of the key issues to address when preparing the policy and procedural documentation include:

Requirement	Issues and Concerns include:
Clarifying the Legal Basis	• Ascertaining local law or ordinance
Defining the Authorization for the Use of Cameras	• Determining threat level response requirements • Using audio surveillance in conjunction with the video surveillance cameras. • Unauthorized use or misuse of the cameras
Developing Clear Policy and Procedural Guidelines	• Determining local procedures • Conducting live video surveillance • Identifying recording authorization • Clarifying dispatching procedures • Defining retention and evidence needs • Preparing maintenance plans

IV. Our Services

The Winbourne and Costas-XRAM Team can provide a range of services in planning and implementing a video surveillance system. The following section describes the variety of roles in which we can assist an agency to meet this objective. Having the experience and knowledge associated with designing and implementing a successful system in Washington, DC can significantly contribute toward a successful implementation. The focal point of our assistance is described in the following subsections.

MPD's functionality requirements provided the framework for the MPD-FBI-USSS Synchronized Operations Command Center (SOCC) and video surveillance system.

Define Requirements--Successful projects define the operational and technical requirements prior to design and implementation decisions. Drawing from the Washington, DC experience, the Winbourne and Costas—XRAM Team can prepare the operational and technical requirements combining that unique experience with an agency's specific environment and design requirements. Our team can assist an agency to define the operational needs for agency-owned video data as well as for integration of video feeds from other agencies such as transportation. Also, we can assist an agency to define the surge and day-to-day operational requirements, location of cameras, networking options and video management at the agency's command center. One unique characteristic of our team is our product independence; our

analysis is not based on how best to use a particular commercial product, but on the required functionality, reliability and cost. As part of this task we will assess the available infrastructure for using ricochet, wired and other wireless networks.

Prepare Design and Conduct Integration--After establishing the requirements, our team can move directly to design and integration tasks. Designing and integrating a video network in Washington or any other jurisdiction present unique and yet similar set of challenges. Designing and integrating a camera network requires a significant level of inter-agency coordination. One of the key elements of our design and integration work on the Washington system was the coordination with many emergency services agencies such as fire departments, emergency management agencies, health, FBI, other federal, local law enforcement agencies. As more and more feeds come into the command center, video management requirements and operation become critical so not to overload decision-makers.

Building height and street patterns as well as a variety of naturally formed barriers present unique design challenges, especially for camera locations. Utilizing a combination of wired and wireless networks can provide video data transmission. In addition, using a range of types and locations of camera equipment will provide varying solution options for the design. We have designed systems using a wide variety of camera types including remotely controlled programmable cameras, ENG quality cameras, covert or hidden cameras as well as helicopter and satellite-based.

Assist with Video Network Operations--Our Team can provide specialized assistance with using and maintaining the video network. Typically, capturing the signal is being received and transmitted to other agencies are some of the assistance we provide.

Prepared Draft Video-Privacy Policy--The use of video surveillance has provided the catalyst for a renewed debate on the balance between effective police procedures and use of technology with concerns on the impact of video technology on civil liberties. As indicated earlier in this paper, the press has drawn significant interest to the use of this technology by law enforcement agencies. In addition, the use of video cameras in nation's capitol by law enforcement agencies was discussed in Congressional hearings with both the US Park Police and MPD leaders testifying. A critical item of interest by the Congress is the role of policy and whether the agencies were utilizing written policy guidance.

Congressional and media attention is focusing on use of video technology for policing operations. Documented policy guidance and oversight have emerged as critical issues.

Prior to the onset of the public discussion in the press and

in Congress, Winbourne and Costas prepared a draft video surveillance policy for MPD. This draft document provided the basis for a final video surveillance policy for the MPD. Specifically, the draft policy paper included proposed procedures for authorization, use, recording, archiving, maintenance, and disposal of video recordings. Based on the current public discussion on this subject, having policy guidance available to direct the overall effort is a critical element of success.

V. How to Contact Us

Winbourne & Costas, Inc.

James P. Costas
Partner and Chief Operating Officer
1000 Vermont Ave., NW Suite 900
Washington, DC 20005
Telephone (202) 216-0193,
Extension 202
Facsimile (202) 216-0275
jcostas@winbournecostas.com

Xram, Inc.

Junior Cristafulli
Vice President
4132 Westfax Drive
Chantilly, VA 20151
Telephone (703) 961-9630
Facsimile 703) 961-9631
jcristafulli@xram.com