SPECTRUM POLICY FOR THE 21ST CENTURY – THE PRESIDENT'S SPECTRUM POLICY INITIATIVE

A PUBLIC SAFETY SHARING DEMONSTRATION

U.S. DEPARTMENT OF COMMERCE

CARLOS M. GUTIERREZ, SECRETARY

JOHN M. R. KNEUER, ASSISTANT SECRETARY FOR
COMMUNICATIONS AND INFORMATION

May 2007

This page intentionally blank

LEADERSHIP AND CONTRIBUTORS

National Telecommunications & Information Administration

The Honorable John M. R. Kneuer
Assistant Secretary for Communications
and Information

Meredith A. Baker
Deputy Assistant Secretary for Communications
and Information

Office of Spectrum Management

Karl B. Nebbia
Associate Administrator

Emergency Planning and Public Safety Division

William A. Belote
Division Chief

Richard J. Orsulak
Team Lead

Charles T. Hoffman

This page intentionally blank

ACKNOWLEDGEMENTS

The National Telecommunications and Information Administration (NTIA) would like to thank the District of Columbia’s Office of the Chief Technology Officer (OCTO), under the direction and leadership of Robert LeGrande, for providing the necessary support and information during the demonstration of this pilot; and Televate, LLC for providing the necessary contract work for NTIA during the demonstration and development of this report.

This page intentionally blank

TABLE OF CONTENTS

APPENDICES

LIST OF FIGURES

This page intentionally blank

ACRONYMS AND ABBREVIATIONS

AAA	Accounting, Authentication, & Authorization
A/C	Air Conditioning
AIU	Alarm Interface Unit
AVL	Automatic Vehicle Location
BBU	Baseband Unit
BHU	Backhaul Unit
bps	Bits per second
CAD	Computer Aided Dispatch
CDMA	Code-Division Multiple Access
CDPD	Cellular Digital Packet Data
CMRS	Commercial Mobile Radio Service
cPCI	Compact Peripheral Component Interconnect
CSU/DSU	Channel Service Unit/Data Service Unity
DC DOT	District of Columbia Department of Transportation
DC EMA	District of Columbia Emergency Management Agency
DC FEMS	District of Columbia Fire Emergency Medical Services
DC MPD	District of Columbia Metropolitan Police Department
DC PHS	District of Columbia Public Health Service
DC WAN-VLAN	District of Columbia Wide Area Network- Virtual Local Area Network
DHS	Department of Homeland Security
EMS	Emergency Medical Services
EVDO	Evolution Data Optimized
FCC	Federal Communications Commission
FMDM	Flarion Mobile Diagnostic Monitor
GIS	Geographic Information System
GPS	Global Positioning System
IMF	International Monetary Fund
IP	Internet Protocol
IPSec	Internet Protocol Security
IT	Information Technology
JPEG	joint Photographic Experts Group
LAN	Local Area Network
LMR	Land Mobile Radio
MACC	Multi-Agency Communications Center
Mbps	Megabits per second
MCU	Master Control Unit
MDT	Mobile Data Terminals
MHz	Megahertz
MMCX	Micro Miniature Coaxial
MoA	Memorandum of Agreement
MoU	Memorandum of Understanding
MPEG4	Motion Picture Experts Group Version 4

NCR	National Capital Region
NPS	National Park Service
NPSTC	National Public Safety Telecommunications Council
NTIA	National Telecommunications and Information Administration
OCTO	Office of the Chief Technology Officer
PA	Power Amplifier
PAD	Portable Access Device
PCMCIA	Personal Computer Memory Card International Association
PCMIA	Personal Computer Manufacturer Interface Adapter
PCU	Power Control Unit
PDA	Personal Digital Assistant
PHY	Physical Layer Processing
QoS	Quality of Service
RF	Radio Frequency
RFP	Request for Proposal
RWBN	Regional Wireless Broadband Network
RXU	Receiver Unit
SNR	Signal to Noise Ratio
STA	Special Temporary Authorization
TXU	Transceiver Unit
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supplies
USB	Universal Serial Bus
USPP	United States Park Police
USSS	United States Secret Service
VSAT	Very Small Aperture Terminal
WARN	Wireless Accelerated Responder Network
WLG	Working Level Group
WMATA	Washington Metropolitan Area Transit Authority
WMO	Wireless Management Office
WPO	Wireless Programs Office

EXECUTIVE SUMMARY

In May 2003, President Bush established the Spectrum Policy Initiative to promote the development and implementation of a United States spectrum policy for the 21st century and to create a spectrum management system capable of handling the future needs of communications and the advances in communication technologies.

A main goal of the Initiative is to evaluate the communication needs of public safety agencies and the efficiency of spectrum use. This report fulfills recommendation 9(b) of the President's Spectrum Policy Initiative Report Two of July 2004 which states that the National Telecommunications and Information Administration (NTIA) should develop and implement one or more demonstration programs to test the operational and cost effectiveness of sharing spectrum and communications infrastructure between federal, state, and/or local governments and private users. After evaluating programs from across the country, NTIA chose the District of Columbia's (District) pilot program, "Wireless Accelerated Responder Network" (WARN), which was implemented by the District's Office of the Chief Technology Officer (OCTO). NTIA selected the WARN pilot program because it met NTIA's evaluation criteria; specifically, it demonstrated the use of a public safety network on which federal, state, local and private users share the available bandwidth.

The WARN system is a broadband, public safety wireless network providing citywide coverage to the District. It was created to fill a need of first responders to exchange large amounts of data wherever emergency services are required. WARN provides high bandwidth access to streaming video, large files and images, specialized emergency response databases as well as standard desktop applications such as email and instant messaging. The system operates in the 700 MHz band using an experimental license provided by the Federal Communications Commission (FCC). It includes 12 fixed transmission sites and roughly 200 subscribers.

The system became operational in January 2005, and has continued to operate throughout the publication of this report. During the demonstration period which was from January 2005 through December 2006,[1] WARN was used by more than a dozen federal, District, and non-federal agencies. WARN bandwidth was shared during multiple large-scale events, and enabled access to critical data for federal and non-federal users. It saw significant initial use during the Presidential Inauguration, International Monetary Fund (IMF) demonstrations, and Fourth of July celebrations. WARN improved collaboration between federal and District agencies. The system also demonstrated significant benefit to users according to user feedback. The demonstration also revealed several areas to improve future public safety solutions, including the need for increased broadband coverage.

[1] The demonstration period of this pilot is from January 2005 through December 2006. The District of Columbia began to operate the WARN system in January 2005 and intends to operate the WARN system beyond this demonstration period. Any reference to WARN in the past tense refers to the demonstration period itself.

WARN demonstrated a critical value in supporting federal and non-federal agencies as they work toward a spectrum-sharing solution to meet the increasingly complex, public-safety, wireless, broadband communication needs in the coming decades. Specifically based upon this pilot, NTIA observed and recommended the following:

Observations	***Recommendations***
Spectrum Planning	
• WARN demonstrated that in-depth spectrum planning and coordination are required to satisfy emerging broadband requirements. • WARN illustrated a growing need for broadband capabilities within the District.	• Federal agencies should clearly identify all broadband requirements in their agency strategic spectrum plans submitted to NTIA. • State and local public safety entities should develop spectrum plans that address their emerging broadband requirements.
Spectrum Use	
• WARN demonstrated that the availability of broadband leads to the realization of broadband potential and the creative identification of new applications. • According to the District's experiences, it appears the amount of spectrum used by WARN (2.5 MHz) under the experimental license within the 700 MHz band may be insufficient for public safety broadband use.	• The FCC should conclude their revision of the current 700 MHz band plan to provide the capability for public safety entities to deploy broadband services.
Spectrum Sharing	
• The WARN pilot showed that partnerships that share spectrum resources between all levels of government greatly increase interoperable communications. • The District discovered during the WARN pilot that spectrum and communications infrastructure sharing tends to provide operational and cost-effective solutions.	• Broadband partnerships should be considered by the public safety community to include all levels of government.
Feasibility of Commercial Services	
• The District analyzed the use of commercial services and determined that commercial networks did not meet the requirements of WARN. However, they are available and may be appropriate for non-mission-critical uses if reliability, throughput, coverage, security, and network management issues are addressed.	• Public safety agencies should use commercial broadband services, where appropriate, if they can satisfy their broadband requirements.

SECTION 1

INTRODUCTION

BACKGROUND

President Bush established the Spectrum Policy Initiative in May 2003,[2] to promote the development and implementation of a United States spectrum policy for the 21st century that will:

(a) foster economic growth;
(b) ensure our national and homeland security;
(c) maintain U.S. global leadership in communications technology, development and services; and
(d) satisfy other vital U.S. needs in areas such as public safety, scientific research, Federal transportation infrastructure, and law enforcement.[3]

To ensure that U.S. spectrum management policies are capable of harnessing the potential of rapidly changing technologies, the President charged the Secretary of Commerce to develop recommendations to: "(a) facilitate a modernized and improved spectrum management system; (b) facilitate policy changes to create incentives for more efficient and beneficial use of spectrum and to provide a higher degree of predictability and certainty in the spectrum management process as it applies to incumbent users; (c) develop policy tools to streamline the deployment of new and expanded services and technologies, while preserving national security, homeland security, and public safety, and encouraging scientific research; and (d) develop a means to address the critical spectrum needs of national security, public safety, Federal transportation infrastructure, and science."[4]

Based on the President's guidance, [5] the advice of the Federal Task Force,[6] and outreach efforts to the public safety and private sector communities,[7] the Secretary of Commerce, in June

[2] Memorandum on Spectrum Policy for the 21st Century, 39 Pub. Papers 23 (June 9, 2003), available at http://www.whitehouse.gov/news/releases/2003/06/20030605-4.html (President's Memorandum I).

[3] *Id.*

[4] *Id*.

[5] The President directed the Secretary of Commerce to initiate two courses of action: (a) to establish a Federal Government Spectrum Task Force (the "Task Force") consisting of the heads of impacted executive branch agencies, departments, and offices to address improvements in polices affecting spectrum use by federal agencies, and, (b) to schedule a series of public meetings to address improvements in policies affecting spectrum use by state and local governments and the private sector, as well as improvements in polices for the spectrum management process as a whole. *Id*.

[6] National Telecommunication and Information Administration, U.S. Dep't of Commerce, *Spectrum Policy for the 21st Century- The President's Spectrum Policy Initiative: Report 1, Recommendations of Federal Government Spectrum Task Force* (June 2004) at http://www.ntia.doc.gov/reports/specpolini/presspecpolini_report1_06242004.htm (Report 1).

[7] National Telecommunications and Information Administration, U.S. Dep't of Commerce, *Spectrum Policy for the 21st Century- The President's Spectrum Policy Initiative: Report 2, Recommendations from State and Local*

2004, submitted two reports to the President, titled *Spectrum Policy for the 21st Century – The President's Spectrum Policy Initiative (Report 1 and 2).* The two reports contained 24 recommendations for assessing spectrum use in the public safety and government sector. The President requested in an Executive Memorandum dated November 30, 2004, that the Department of Commerce submit an Implementation Plan to put the 24 recommendations into practice.[8]

NTIA published the Implementation Plan in March 2006.[9] A critical facet of the Implementation Plan is Project D, which addresses the recommendations related to public safety. The Department of Homeland Security (DHS) is responsible for addressing all recommendations related to public safety except for recommendation 9(b) of Report 2, which is NTIA's responsibility.[10] Recommendation 9(b) states that NTIA should "develop and implement one or more demonstration programs to test the operational and cost effectiveness of sharing spectrum and communications infrastructure between federal, state, and/or local governments and private users."[11]

Demonstrations or pilots that share resources and assets between federal, state, and local public safety agencies are not a new concept, although few include private users. In many instances, a Memorandum of Understanding (MoU) or Memorandum of Agreement (MoA) between federal and non-federal agencies outlines sharing and mutual aid arrangements that may never be registered or known at a national level. Most federal agencies have numerous such local arrangements. In recent years, many of these agreements have become more regional in nature. For example, the Department of Defense (DoD), through Alaskan Command, formed a partnership with various state and local public safety agencies to form the Alaska Land Mobile Radio System (ALMRS), a statewide public safety telecommunications system in which all users of the system share resources (spectrum, funding, and facilities).[12] Demonstration projects and proofs of concept, when properly designed and implemented, can show to the public safety community, elected officials, Congress, and the Administration, the effectiveness of cooperative solutions in responding to situations where interoperability may be problematic.

Additionally, these demonstrations can prove the application of innovative technologies to public safety and speed their introduction into the public safety community. Demonstrations can help resolve spectrum policy and regulatory issues among agencies at both the federal and non-federal level. These demonstrations enable more flexible rules to allow easier sharing of spectrum and systems among public safety agencies and between government entities and private networks, including the critical infrastructure industry and commercial service industry. The

Governments and Private Sector Responders, (June 2004) at http://www.ntia.doc.gov/reports/specpolini/presspecpolini_report2_06242004.htm (Report 2).

[8] *Memorandum on Improving Spectrum Management for the 21st Century,*_ Pub. Papers _ (Dec. 6, 2004) available at http://www.whitehouse.gov/news/releases/2004/11/20041130-8.html (President's Memorandum II).

[9] National Telecommunications and Information Administration, U.S. Dep't of Commerce, *Spectrum Management for the 21st Century: Plan to Implement Recommendations of the President's Spectrum Policy Initiative* (March 2006), available at http://www.ntia.doc.gov/osmhome/reports/ImplementationPlan2006.htm (Implementation Plan).

[10] Report 2, *supra* note 7, at 26.

[11] *Id*.

[12] *See* Alaska Land Mobile Radio Project, at http://www.ak-prepared.com/almr/.

lessons learned from these programs are invaluable tools in helping federal, state, and local agencies perform their jobs in a more coordinated manner.

OBJECTIVES

The objectives of the Recommendation 9(b) task are for NTIA to: (1) examine the feasibility of sharing spectrum among commercial, federal and local public safety and critical infrastructure applications, including the possibility of leasing services, and (2) develop and implement one or more demonstration programs to test the operational and cost effectiveness of sharing spectrum and communications infrastructure between federal, state, and/or local governments and private users.[13] Since new funding was not available, NTIA met these objectives through the selection of an existing demonstration pilot.

APPROACH

In order to successfully achieve the objectives of Recommendation 9(b), NTIA took the following approach:

- Conduct research on current public safety demonstrations and pilots; compile a list with background information on possible demonstration candidates and select an existing pilot based upon the recommendations and objectives as described above and consistent with established selection criteria;
- Provide Working Level Group (WLG) D members with information on the selected demonstration candidate and seek WLG D concurrence;
- Invite expert demonstration staff to brief WLG D members on the selected demonstration candidate;
- Work with demonstration staff, the DHS and the Federal Communications Commission (FCC), if necessary, during the duration of the pilot;
- Research sources of existing and available information on the feasibility of commercial services for use by public safety services; and
- Research information on the selected demonstration candidate, and compile data from interviews, the Internet, and other sources into a report.

[13] Report 2, *supra* note 7, at 26.

This page intentionally blank

SECTION 2

SELECTION CRITERIA

NTIA compiled a list of current and conceptual demonstration programs that NTIA staff knew to exist or that proponents presented to NTIA for consideration as a possible demonstration. Each of the identified projects possessed merits that could demonstrate sharing and interoperability among public safety entities. In addition to the basic and fundamental criteria in Report 2, Recommendation 9b, NTIA established other benchmarks that coincided with the intent or language of the Implementation Plan. These additional benchmarks became part of the requirements to be met in order for the project to be considered and selected. Therefore, the complete criteria required that the chosen project:

1. Demonstrate operational capability and cost-effectiveness of sharing spectrum and communications infrastructure between federal, state, and/or local governments and private users;
2. Already be in existence or fully funded (this would also avoid duplication of effort, reduce costs, and benefit from the potential synergies);
3. Provide results by December 2006;[14] and
4. Operate within current spectrum allocations, except that it may require special temporary authorizations and rule waivers during the demonstration phase.

NTIA identified conceptual candidates but did not consider them for a demonstration or ranking since there were too many unknown variables to meet the December 2006 deadline. Further, NTIA dismissed from consideration those candidates that used technology-only solutions (e.g., gateway or audio switch solutions to connect disparate frequency bands or systems) since they did not meet the basic recommendation of sharing spectrum. NTIA also dismissed other proposals that did not satisfy the recommendation of sharing spectrum with other private users.

Based upon the above selection criteria, NTIA selected and WLG D approved, the District of Columbia's Office of the Chief Technology Officer's (OCTO) Wireless Area Responder Network (WARN) 700 Megahertz broadband pilot program.[15] WARN met the established selection criteria:

[14] Implementation Plan, *supra* note 9, at 23.

[15] NTIA Press Release, *NTIA Selects DC Public Safety Network to Monitor Effectiveness in Sharing Radio Spectrum with Federal, State, and Local Government Users*, April 25, 2006, available at http://www.ntia.doc.gov/ntiahome/press/2006/publicsafety_042506.htm.

- The program was in existence and would likely meet the December 2006 deadline.
- The project was funded.
- The project demonstrated sharing between federal, state, local, and private users, since the Washington Metropolitan Area Transit Authority (WMATA), as defined under Part 90 Rules,[16] is a business licensee.
- The project was cost effective.
    - The WARN system used low-cost wireless Personal Computer Memory Card International Association (PCMCIA) cards allowing any laptop or computer to become part of the network.
    - The WARN system used the same sites as the current DC Land Mobile Radio (LMR) system (no additional infrastructure costs).
    - The WARN system costs less than twenty percent of the DC LMR system.
- NTIA would incur no extra expenses due to the geographic location of WARN, which would also allow NTIA personnel to attend all planning meetings and actively participate in the project.
- All coordination for spectrum was approved, and the WARN program was granted an experimental license by the FCC (the expiration of which would extend beyond the December 2006 deadline).
- The WARN system showcased new technology.
- Although at the time it was a broadband, streaming video project, narrowband-like Voice-over-Internet Protocol (VoIP) was being considered for the project in the future.
- The Implementation Plan stated that NTIA should work closely with DHS on the demonstration program, and the DHS Wireless Management Office (WMO) signed a MoU with the WARN program to become a user on the network. The WMO stated that they were willing to share any information that they gained from their testing and use of the system.

Ultimately, NTIA determined that the DC's WARN broadband pilot fulfilled the basic recommendation of "sharing spectrum and communications infrastructure between federal, state, and/or local governments and private users."

This report focuses on the scope, observations, recommendations, and conclusions drawn within the shared environment of the DC's WARN broadband pilot program.

[16] Federal Communications Commission, Private Land Mobile Radio Services, 47 C.F.R. Pt. 90 (FCC's Part 90 Rules).

SECTION 3

THE WARN PILOT

BACKGROUND

The District of Columbia (District) is in a unique situation regarding its public safety interoperability needs. It has both state and local responsibilities, and it is adjacent to five local municipalities and two states. This region, encompassing the District and all of the surrounding cities and counties in Virginia and Maryland, is most often referred to as the National Capital Region (NCR). Additionally, due to the small size of many of these jurisdictions and the significant scope of events in the District, mutual aid is provided far beyond the NCR. Also, the large presence of the federal government in the NCR requires that the District must be able to interoperate with numerous federal agencies.

The District is responsible for a significant number of incidents and events that occur in the nation’s capital, which also includes fire suppression and emergency medical services for federal structures and property. This responsibility demands coordination and extensive communication with many jurisdictions. For instance, daily traffic related incidents on the Wilson Bridge as well as frequent large demonstrations require ample inter-agency communication and coordination among federal, state, and local emergency personnel. At major events, such as the Presidential Inauguration or the incident on September 11, 2001 at the Pentagon, the breadth of mutual aid was significant — the need for interoperability and solutions that link multiple jurisdictions and extend beyond regional boundaries is paramount.

The District's OCTO develops and enforces policies and standards for information technology used within the District government. The OCTO identifies where and how technology can systematically support the business processes of the District's 68 agencies. These agencies can draw on the OCTO's expertise to get the most out of their technological investments. The OCTO assesses new and emerging technologies to determine their potential application to District programs and services. The OCTO also promotes the compatibility of computer and communications systems throughout the District government. Information Technology (IT) is the most powerful tool for achieving the District's business goals.

Since its establishment in April 2001, the OCTO has been implementing an eight-year, citywide, IT Strategic Plan (IT Plan). The IT Plan is designed to deliver a robust technology infrastructure for the District government, provide systematic technology support for District government functions, create a state-of-the-art public safety/homeland security infrastructure for the nation’s capital, and provide a complete and coherent Website offering a variety of Web services for the public.

In order to address the District’s needs for wireless communications, the Wireless Programs Office (WPO) was established at the end of 2001. The WPO is responsible for using wireless technology to improve District operations. Because wireless solutions are used extensively by the public safety community, the WPO focuses primarily on pubic safety wireless needs. In the aftermath of 9/11, the WPO initially focused on implementing a fully interoperable public safety radio system with ample in-building coverage for District emergency personnel.

While working on the public safety radio system, it became evident to OCTO and WPO personnel that existing data communications solutions were not meeting the needs of emergency responders within the District. For instance, public safety personnel needed to use real-time broadband data applications when working in the field (e.g., streaming video, detailed building blueprints, and high resolution images). These applications required a large transmission pipe, and the existing LMR systems and public safety spectrum were insufficient to support these needs over wide areas. This finding led to the development of WARN, the pilot network designed to provide wireless broadband at high speeds to emergency response personnel deployed in the field.

SPECTRUM CONSIDERATIONS

The District recognized the necessity of a public safety broadband wireless data network, but it also recognized that the technologies using existing public safety spectrum did not fulfill its broadband data needs. The private-owned network options offered at the time included narrowband channels in the 150 MHz, 450 MHz, and 800 MHz public safety bands, wideband data channels in the 700 MHz band, or broadband data channels in the 4.9 GHz band.[17]

The District's analysis of these options showed that:

- Although 150 MHz, 450 MHz, and 800 MHz band propagation allows a small number of sites to provide ubiquitous coverage to a wide area,[18] the narrowband (25 kilohertz) data channels in these bands did not allow for broadband data application use. The throughput provided was less than half that of a typical dial-up connection. Peak achievable throughput was about 20 kilobits per second (kbps), limiting operations to little more than text messaging. Also, the lack of contiguous blocks of spectrum prevents use of the necessary bandwidth to accommodate broadband applications. Furthermore, these bands are heavily used by thousands of licensees, and they would have to be cleared to allow for broadband channels.

- The current 24 MHz of public safety spectrum within the 700 MHz band possesses radio propagation characteristics that are similar to the 800 MHz band. However, the 150 kHz channel size limit in this public safety band does not allow for broadband applications. For example, Scalable Adaptive Modulation (SAM), the technology proposed as the wideband technology standard, was not expected to be cost-effective or to meet the demands of transferring data. Peak throughput is 460 kbps, allowing for only a few streaming video feeds; whereas some applications transmit multi-video feeds and require 1.2 megabits per second (Mbps). Therefore, the high bandwidth demand could not be supported by this technology. Furthermore, the District expected to secure only a few 150 kHz channels in the 700 MHz regional planning process. The result would be 50 times less throughput than what the applications required. Additionally, because the SAM technology is not easily scalable, the only way to increase capacity would have required costly upgrades.

[17] The District also looked at the possibility of using commercial services. Ultimately, the District decided that commercial services did not meet all of their requirements. More information on the feasibility of using commercial services for broadband applications and the District's decision not to use them is explained in Section Four.

[18] A small number of sites results in lower capital and operational costs for the network operator.

- Even though sufficient bandwidth exists in it, the 4.9 GHz (4940-4990 MHz) band allocated to public safety was not economically viable for deploying and operating a District-wide network. Ubiquitous coverage of the District (68 square miles) would have required more than 1,000 radio sites compared to roughly 10 sites in the 700/800 MHz band because of its short-range propagation characteristics. The District estimated that the deployment and operating costs for this quantity of sites would be prohibitive. The application of this band is more suitable to "hot-spot," short-range incidents.

After analyzing the available options, the District decided to deploy a pilot network in the 700 MHz band under an experimental license, and to seek permanent broadband spectrum for public safety.[19] An experimental license was necessary because the current FCC Part 90 Rules do not provide channel widths to accommodate high-speed/high-data rate broadband applications and the District intended, in part, to use spectrum not allocated to public safety.[20] Under the authority of an FCC experimental license, the District deployed a 700 MHz pilot network using a commercial technology called Fast Low-latency Access with Seamless Handoff Orthogonal Frequency Division Multiplexing (Flash-OFDM).[21]

The light yellow areas in Figure 1 show the spectrum granted to OCTO through the experimental license. Figure 1 identifies the 24 MHz of spectrum from TV channels 63, 64 (764-776 MHz) and 68, 69 (794-806 MHz) that has been reallocated for public safety uses.

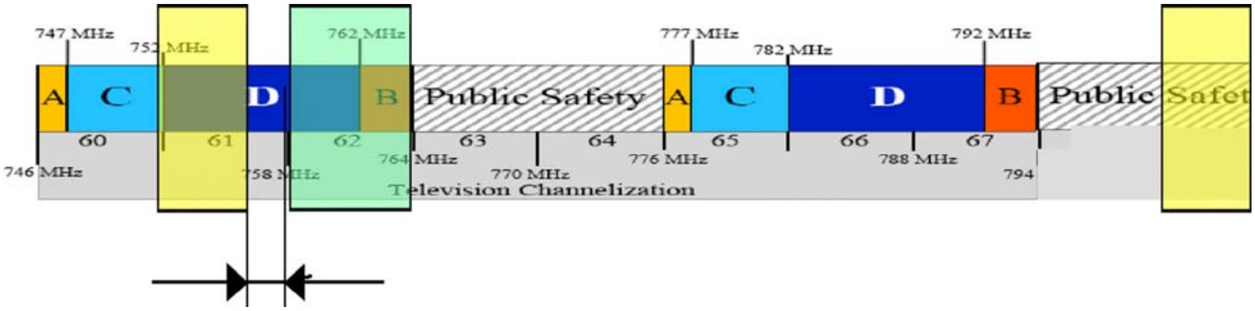

Figure 1: WARN Spectrum

WARN uses one 1.25 MHz channel in each of the two 4 MHz bands[22] allocated in the TV Channel 61 (downlink or base station to mobile terminal), and the TV Channel 69 (uplink or mobile terminal to base station) segments. The OCTO selected these bands since they afforded the only clear space in the 700 MHz band within the District at the time of the pilot launch.

[19] To this end, the District worked with Congress and other stakeholders and decision-makers to heighten awareness of broadband needs, not only in the District, but across the nation. As part of this effort, the District founded the Spectrum Coalition for Public Safety (Spectrum Coalition) to address the broadband spectrum needs for the country in the 700 MHz band. The Spectrum Coalition is a non-commercial affiliation of over 30 state, county and local government public safety communications organizations. *See* http://www.spectrumcoalition.org.

[20] *See* FCC's Part 90 Rules, *supra* note 16, at Section 90.531.

[21] Federal Communications Commission, Experimental Radio Construction Permit and License, Call Sign WD2XHO, File Number 0182-EX-RR-2006 (WARN Experimental License).

[22] The District initially planned for two technologies with channel bandwidths of 1.25 MHz each and an intermediate guard band to utilize this 4 MHz of spectrum. Ultimately, only one technology was deployed.

After the experimental license was granted in February 2004, the District learned that the Flarion equipment to be used in the experimental network would be available more rapidly if the uplink and downlink frequencies were swapped (e.g., if the base stations operated in the lower range of frequencies from 752.65 MHz to 756 MHz range,[23] and the mobile units operated in the upper range of frequencies from 800.65 MHz to 804 MHz). Swapping the uplink and downlink frequencies had no impact on the operations of WARN; however, in order to receive approval for this license revision, the District had to demonstrate to the FCC that the operations of Maryland Public TV broadcasting in the adjacent channel were not disturbed by WARN.[24]

The FCC stipulated that the District had to coordinate with the Maryland Public TV station (Channel 62) prior to network deployment to ensure that no harmful interference would be caused to its television operations.[25] As the license filing describes, the only TV Broadcasting station on a co-channel or an adjacent channel was a Maryland Public TV located in Frederick, Maryland, which operates on channel 62. This channel, represented in light green in Figure 1, was adjacent to OCTO's experimental downlink channel. However, the actual transmitted central frequencies used by WARN were 755 MHz and 803 MHz. The Maryland Public TV channel, therefore, was separated by 3 MHz from the transmitting Flash-OFDM station, which allowed for protection from interference. Moreover, an additional filter was added to further protect the TV station. Extensive testing was conducted to show that WARN did not interfere with Maryland Public TV. Maryland Public TV did not report any interference during the WARN operations. The Commission granted the experimental license revision. However, in order to minimize the potential for interference, the conditions of the experimental license allowed mobile use only within the geographic confines of the District to protect television broadcasters operating in the band.

WARN OVERVIEW

Purpose

The purpose of the WARN pilot was to determine how a broadband wireless network could address the needs of public safety and to further refine system and application requirements for future public safety data systems. The District designed the WARN program to use the upper 700 MHz band, thereby allowing it to evaluate the impact of interference received from or created by TV stations broadcasting in this band.

Applications

Responding to emergency events such as multiple-alarm building fires, chemical or biological attacks, or other large-scale attacks requires immediate and rapid wireless data communications among multiple first responders, including fire, police, and emergency medical services (EMS) personnel. Broadband applications now are considered essential tools for

[23] This band is part of the blocks of spectrum to be auctioned no later than June 28, 2008 and revenues deposited in the Public Safety Trust Fund. *See Digital Television Transition and Public Safety Act of 2005, Title III of the Deficit Reduction Act of 2005, Pub. L. No. 109-171, 120 Stat. 4, 21 (Feb 8, 2006) (The DTV Act).*

[24] The FCC Rules regarding such an experimental license protects TV Broadcasting stations that are co-channel (transmitting on the same channel) or adjacent channel to WARN. *See* FCC's Part 90 Rules, *supra* note 16, at Section 90.545.

[25] WARN Experimental License, *supra* note 21.

protecting lives and property. The ability to use these critical public safety data applications, among others, requires ubiquitous wide-area coverage with broadband throughput. The network allowed District first responders to use full-motion, high-resolution video monitoring and other bandwidth-intensive monitoring tools to immediately share time-critical incident and emergency event information with such applications as:

- Real-time, full-motion video;
- Digital imaging (e.g., building diagrams, mug shots);
- Remote access to databases (e.g., criminal, hazardous materials) and report management systems;
- Mapping, Geographic Information Systems (GIS);
- Remote sensors (e.g., biological, radiological);
- Automatic Vehicle Location (AVL), automatic collision notification systems; and
- Emergency Medical Services (EMS) applications.

Specifically, a number of diverse applications requiring varying degrees of data rates evolved over the duration of the pilot. The titles and descriptions of many of the applications are reflected in the following table. Not all of the applications listed have actually been used as of yet, but show the potential for future use on the WARN network.

Title	***Description/Benefit***
PROTECT (Chemical/biological terrorism detection and information sharing)	Existing applications of video and plume projection information to first responders in the field provides enhanced response time and real-time detailed information. Providing this information to the field to qualified personnel avoids missing key information that an untrained eye might miss.
Demonstration video surveillance	Dissemination of video from existing overhead traffic cameras provides field officers important information regarding the demonstration. It also allows law enforcement to locally identify needed resources before any officer is put in harm's way. LiveWave, Greenhouse, and KaptureNet are examples of this type of application that were used with WARN.
Bomb squad support	Local law enforcement bomb squad personnel can be supported remotely by federal bomb experts to analyze and incapacitate sophisticated bombs.
EMS support	EMS personnel providing critical care can receive diagnostic analysis and treatment support from hospital or other medical experts and drastically speed up the delivery of timely medical care.
Building images, etc.	Overhead building images from multiple angles provide firefighters with critical entry, exit, building vent points, and building vulnerability points. Computer-aided designs of buildings also provide firefighters with detailed floor plans and building materials. GIS systems provide fire hydrant locations and aid firefighters in identifying potential water sources while en-route, saving valuable time.

Helicopter video support	Video captured above a major building fire provides incident commanders with an important perspective on how to extinguish the flames and minimize risks to firefighters battling the fire.
Interoperable video	Police officers or other government personnel who arrive at an incident early can convey critical information back to EMS personnel to deliver resources to the incident at the appropriate priority.
Image or video distribution	The distribution of a picture of a missing child, convenience store robbery video, or criminal-sketch to all equipped vehicles in the field. High-resolution images can be quickly disseminated to an entire department with broadband networks. These images provide clearer representations of their subjects and allow first responders to more accurately identify important information. Video content might show a suspect with a telling limp.
Fingerprint distribution	A suspect's fingerprint can be transmitted from the field for detailed analysis in the lab or a fingerprint can be disseminated to the field for remote analysis.
Field reporting	Public safety personnel can prepare and submit reports in the field that include voice, images, and video. This can avoid unnecessary trips back to headquarters or the home office.
Field training	Training or instructional videos can be viewed in the field to minimize the impact on command, management, and training resources.
Management consultation	Officers or EMS personnel can consult with superiors and convey images or video of crime scenes or patients.
Remote Roll Call	Management can conduct roll calls remotely keeping public safety personnel in the field and minimizing out-of-service time.
CapWIN	An interoperable public safety application for the NCR. Provides NCR jurisdictions with the ability to communicate and access multiple law enforcement databases.
JUSTIS	The Criminal Justice Coordinating Council's information sharing application. Allows sharing of law-enforcement data among city and federal agencies.
WALES	The Washington Area Law Enforcement System is a real-time, computer-based, police information system serving the tri-state area of the District.

Timeline

The following timeline represents key milestones in the deployment of WARN:

Date	*Event*
August 03	Request for Proposal (RFP) for Pilot Network Released
December 03	Contract Awarded to Motorola
January 04	OCTO Files for Experimental License with the FCC
February 04	FCC Grants License
July 04	OCTO Files for a Revision to Experimental License; Original Network Sites Deployed
August 04	FCC Grants Revised License
August 04 - December 04	System Optimization and Testing of Network
December 31, 04	System Acceptance
January 05	Additional Site Added to Network (near White House); First Official Use of Network - Presidential Inauguration
April 05	Additional Site Added to Network (RFK Stadium)
January 05 - December 06	More than 200 Subscriber Devices Operating on the Network

Users

WARN network users included a vast group of federal and non-federal government agencies and public safety personnel from in and around the District. Their cooperation on the WARN network demonstrated the abilities of agencies to effectively work together. The following is a list of agencies that were users of WARN:

- City of Alexandria Police Department
- DC Metropolitan Police Department
- DC Child and Family Services Agency
- DC Office of the Chief Technology Officer
- DC Fire and Emergency Medical Services Department
- DC Department of the Environment
- DC Department of Transportation
- DC Department of Corrections
- DC Department of Health
- DC Emergency Management Agency
- DC Office of the Chief Medical Examiner
- DC Office of Unified Communications
- Fairfax County Fire Department
- Montgomery County Fire Department
- Washington Metropolitan Area Transit Authority
- US Department of Homeland Security
- US Federal Protective Service
- US Park Police
- US Secret Service

All user agencies were required to execute a MoU with the District's OCTO (see a sample MoU in Appendix B). This MoU required agencies to abide by the District's computer use policy, to utilize the network extensively, and to report back to OCTO with information that could lead to future requirements and enhancements.

Funding

The construction of WARN and its initial operations were funded through the District's capital funds. A total of $2.8 million enabled the District to build the initial ten-site network covering its 68 square miles, and provided one year of network operations, as well as 200 subscriber devices. For Fiscal Year 2006, the WPO received additional funding through the DHS State Homeland Security Grants, which covered network and customer operations for the WARN network.

WARN was cost effective in comparison to the upgrades made to the District's LMR system. The District spent $6 million on its original four-site 800 MHz LMR system, and an additional $17 million to upgrade it to a ten-site 800 MHz and 450 MHz network. However, the LMR network provides comprehensive in-building coverage to the 95th percentile versus outdoor coverage for the broadband network at the 95th percentile.

Technology/Vendor Selection

The OCTO sought technologies that would meet the needs and demands of the District's public safety personnel and be cost effective. The key qualities in technology that were sought for WARN included:

- High uplink speeds capable of supporting multiple video streams from mobile units to the network;
- Support of Quality of Service (QoS) which efficiently managed network capacity through flexible traffic prioritization administration;
- Same frequency reuse at all sites to facilitate scalability and minimize needed spectrum (i.e., spectrum efficient); and
- Use of existing LMR infrastructure for cost effectiveness.

The District selected Motorola to deliver WARN which had partnered with Flarion Technologies, the maker of Flash-OFDM equipment. The District selected the Motorola/Flarion solution over Lucent's 1xEVDO (Evolution Data Optimized) Rev 0 due to the higher uplink speeds enabling streaming video from the field as well as the support of QoS controls which enabled improved management of scarce wireless bandwidth. At the time of vendor selection, Verizon Wirelss had recently deployed a 1xEVDO Rev 0 system in the Washington, DC metro area.

Flarion's technology, Flash-OFDM, is a wireless data solution that provides high data rates at very low latency.[26] This feature gave WARN users a wireless connection that was always on, provided upload and download speeds (peak speeds of 900 kbps and 3 Mbps

[26] Low latency systems deliver data (packets) in shorter periods of time from source to destination.

respectively) comparable to residential broadband connections, incurred minimal delays in reception of streaming media, and performed all of these functions in any location covered by the network. Since Flash-OFDM was capable of supporting high data rates, it gave WARN users the ability to send and receive real-time video applications.[27]

Figure 2 illustrates the Flash-OFDM network architecture. At launch, WARN consisted of ten radio routers, an Internet Protocol (IP) network interface, and a network operations center. The architecture is based on the Mobile IP standard and provides seamless connectivity and a single IP address throughout the coverage area.[28]

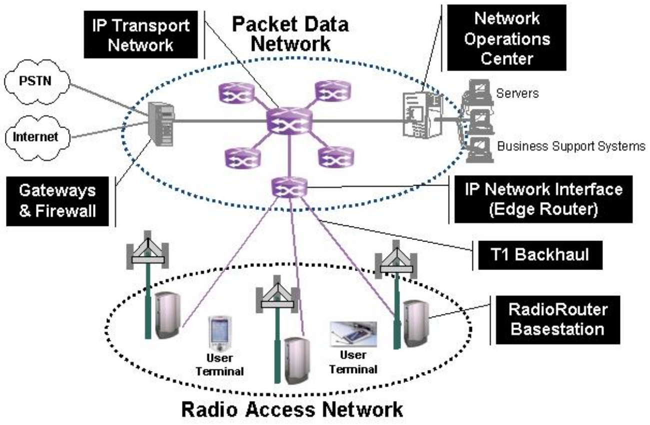

Figure 2: Flash-OFDM Network Architecture

The technology uses a 1.25 MHz channel bandwidth and supports re-using the same frequency at each site and sector via random frequency hopping. Interference occurred only if the power from two sites or sectors was relatively equal and then only part of the time because error correction made up for most of the difference. Though throughput was constrained in this scenario, connections were maintained with this advanced, interference-resistant technology.

Though not part of the solicitation, Motorola offered its Greenhouse video, audio, and dispatch software for WARN operations. This unexpected additional offering proved highly beneficial to the District. The Greenhouse software enabled WARN users to share real-time video and audio information at high video resolutions, with full motion, while using little network capacity. Greenhouse can also make use of inexpensive webcams or high-end professional cameras to share video information.

[27] The OFDM component of the radio link uses technology that can also be found in 802.11a and WiMax solutions. Flarion’s augmentations focused on creating a mobile access and full mobility OFDM solution.
[28] This single, static IP address enables servers to find mobile devices as they travel throughout the District.

Network Construction

Three additional antennas, six transmission lines, and three transceivers[29] were added to the ten LMR sites to provide citywide service. The resulting configuration provided for three sectors per site that delivered up to three times the capacity of a single sector. Additionally, all the sites were interconnected through the District's fiber optic network, DC-NET, to redundant central nodes. These hub sites included Accounting Authentication and Authorization (AAA) servers as well as elements that provided mobility management. The hub sites also gave network users access to the District Wide Area Network (DC-WAN) and the Internet.

Antennas and cables connecting the radio equipment were installed at each site and then activated. The basic function of each site (radio communication with mobile subscribers and routing of data packets) and the connectivity to the other components of the network were then tested. After testing the functionality of all individual sites, the performance of the entire network was verified during the optimization phase.

WARN's optimization phase was an iterative process that consisted of evaluating the performance of the network by driving around the city and testing network operations, modifying the configuration of the network, and then re-evaluating the network performance until optimal performance was achieved. During this phase, the antenna direction was altered to steer signals to where they were needed most and away from areas where interference caused poor performance. On December 31, 2004, the District formally accepted the network from the vendors. Preliminary users were added to the network in January 2005 for additional beta testing. The first major use of WARN occurred on January 20, 2005, for the Presidential Inauguration of President George W. Bush.

TECHNICAL ASPECTS

Overview

WARN is an "all-IP" network using the ubiquitous IP for all network elements, allowing low-cost network elements with simple interconnections to the Internet. WARN's base stations are IP routers that support the Flash-OFDM radio interface (radio-routers). Each terminal equipment unit, radio site, and sector was assigned an IP address. As an "all-IP" network, it was very easy to integrate WARN into most existing commercial and private data networks because it operated with IP. In particular, the functions of the network could be realized using equipment already deployed on wired networks.[30]

The network includes 12 transceiver sites interconnected to two redundant data centers via an independent, District-operated fiber ring. This interconnection at the data centers provides WARN users access through the DC WAN to other District agencies and the Internet, making it possible for agencies and users to share data and video.

[29] A transceiver transmits signals to mobile units and receives signals from mobile units as well as translates them for transmission over fixed lines back to the core network.

[30] For instance, the base stations were able to connect directly to the DC WAN at the core and DC-NET at each radio site. Additionally, the equipment and functions of the WARN were the same or similar to those already managed by the District.

In order for WARN to achieve proficient wide-area communications, application servers were placed inside the WARN network, in the District's data centers, and in the agencies' WAN. All application servers had significant interconnection and power redundancy to ensure the QoS offered by WARN. The network was further equipped with security policies, firewalls, and dedicated links that limited the access of specific applications to relevant end-users.

As Figure 3 shows, the configuration of the backhaul connections, the central node switches, and the AAA, are all fully redundant.

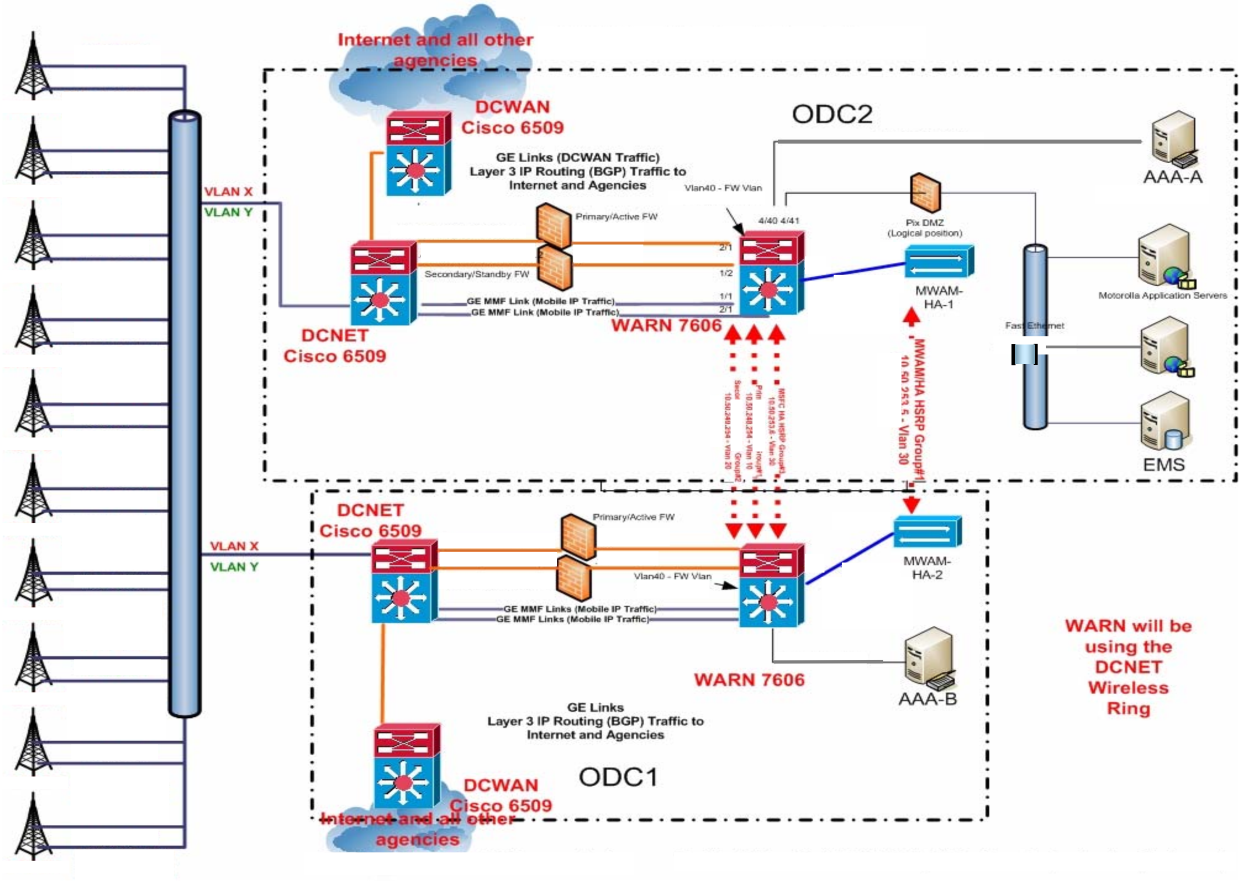
Internet and all other agencies
DCWAN Cisco 6509
GE Links (DCWAN Traffic)
Layer 3 IP Routing (BGP) Traffic to Internet and Agencies
Vlan40 - FW Vlan
ODC2
AAA-A
VLAN X
VLAN Y
Primary/Active FW
4/40 4/41
Pix DMZ (Logical position)
Secondary/Standby FW
2/1
1/2
1/1
2/1
GE MMF Link (Mobile IP Traffic)
GE MMF Link (Mobile IP Traffic)
MWAM-HA-1
Motorolla Application Servers
Fast Ethernet
DCNET Cisco 6509
WARN 7606
MSFC HA HSRP Group#1 10.50.253.6 - Vlan 30
Prim Group#1 10.50.240.254 - Vlan 10
Secol Group#2 10.50.240.254 - Vlan 20
MWAM/HA HSRP Group#1 10.50.253.5 - Vlan 30
EMS
DCNET Cisco 6509
Primary/Active FW
VLAN X
VLAN Y
Vlan40 - FW Vlan
MWAM-HA-2
GE MMF Links (Mobile IP Traffic)
GE MMF Links (Mobile IP Traffic)
WARN will be using the DCNET Wireless Ring
WARN 7606
AAA-B
GE Links
Layer 3 IP Routing (BGP) Traffic to Internet and Agencies
DCWAN Cisco 6509
ODC1
Internet and all other agencies

Figure 3: WARN Architecture Overview

The central node switch manages the users' network mobility. Both the switches and the AAAs are located in two different data centers allowing transition of operations from one data center to the other in the event of a failure. The critical network functions (switching that directs calls to the right recipients, AAA, and Mobility Management that ensures reaching users anywhere within the coverage area) are duplicated in each data center. Because of the ring nature of the fiber network, the backhaul offers no single point of failure.

Ten of the twelve WARN sites were already being used by the District's public safety, LMR, voice, push-to-talk network. They all offer redundant power supplies (including Uninterruptible Power Supplies (UPS) and diesel generators) and redundant air conditioning

(A/C) units. The radio routers also have redundant power units and redundant network interface units.

Two additional sites were deployed to address coverage and capacity (see the "Network Performance" Section). Because of the quick deployment requirements and a limited budget, it was not possible to offer the same level of reliability for these sites. Although power was secured with a UPS and battery backup at both sites, it was not possible to procure and install generators and A/C units.

Also, one of the additional sites did not have access to the fiber ring. For this site, backhaul was provided through a non-redundant microwave link that connected this site to the closest WARN site. These improvements are planned in 2007, when the District plans to implement a fully operational (non-pilot) broadband service as part of the National Capital Region Regional Wireless Broadband Network.

Ultimately, the architecture of WARN was designed to provide the best reliability, functionality, capacity, and spectral efficiency to its users. To achieve this goal, each of the network's radio sites included a three-sector radio router that allowed for maximum throughput of data (see Figure 4).

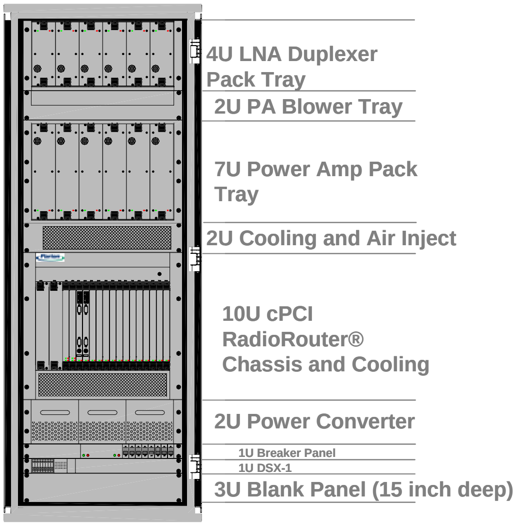
4U LNA Duplexer Pack Tray
2U PA Blower Tray
7U Power Amp Pack Tray
2U Cooling and Air Inject
10U cPCI RadioRouter® Chassis and Cooling
2U Power Converter
1U Breaker Panel
1U DSX-1
3U Blank Panel (15 inch deep)

Figure 4: Radio Router

Additionally, each sector was connected to a cross-polarized panel antenna, which provided for optimal coverage for data throughput. For the sites located at buildings, the panel antennas were mounted on the side of the penthouse for improved shielding between sectors.[31] The selected configuration included receive-diversity, which was used to improve signal reception and was achieved on WARN by having one transmitter, one amplifier and two receivers for each sector.[32] The combination of these characteristics of WARN's architecture

[31] The building itself provided some shielding that reduced interference from sector-to-sector.

[32] The same frequency was transmitted on each sector. The amplifier transmitted 20 Watts. The panel antennas have a 12 dBd gain.

ensured the consistency of coverage for network users. (Appendix C contains more technical details regarding network architecture.)

Devices

In order to transmit and receive data on the network, WARN users were assigned personal computer (PC) cards or Portable Access Devices (PADs). Some devices were assigned to agencies for distribution to users within their agencies as needed, and others were permanently assigned to individuals. The PADs were typically used in command bus applications and mobile video surveillance, but they also served as DC-WAN extensions for remote public safety offices. These remote extensions offered tremendous flexibility for public safety operations to be established almost anywhere in the District.

The PC cards and PADs served as communications modems for host computers – no different than a dial-up modem or Local Area Network (LAN) card inserted into a computer. Users could easily install PC cards in a slot in most notebook or laptop computers along with the installation of corresponding software drivers which provided the communications channel to the operating system and its applications. Although non-technical personnel could have performed these installations and used the WARN PC cards with minimal delay, OCTO installed all software drivers as an additional level of security and customer service. Likewise, a PAD could be installed very quickly by connecting the PAD to a host computer via a LAN Ethernet connection or Universal Serial Bus (USB) cable. Both the PC card and the PAD allowed the host computer to have access to the DC WAN and the Internet.

The District acquired 200 terminal equipment units for network users. The units consisted of 180 PCMCIA cards (Figure 5) that can be installed on most common notebook or laptop PCs, and 20 PADs (see Figure 6) with Ethernet ports that are compatible with all modern notebook, desktop, or network devices. The transmitted power of the terminal equipment is very low (250 milliwatts).

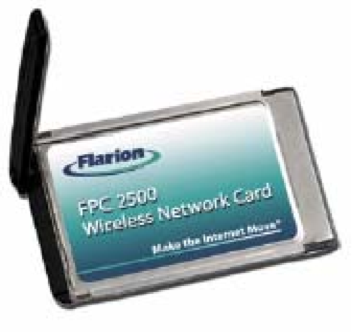

Figure 5: Flash-OFDM PCMCIA Card

The computer system requirements to support the PC card include:

- Card Slot: 1 Type II PCMCIA Card Slot
- Memory: 32 Mb

- Hard Disk Space: 5 Mb
- I/O Resources: 1 IRQ, 256 bytes I/O Space
- Processor Speed: 600 MHz
- Operating System: Windows 2000, XP, Me, Pocket PC

The cards come with a flexible antenna that bends and rotates to reduce breakage. The antenna is removable and connected by a standard Micro Miniature Coaxial (MMCX) connector. For some vehicular configurations, this antenna was removed and a coaxial cable and an external antenna was attached for superior coverage. With the appropriate drivers (provided by Motorola/Flarion), a new computer system can be configured in minutes to secure a connection to the DC WAN and the Internet.

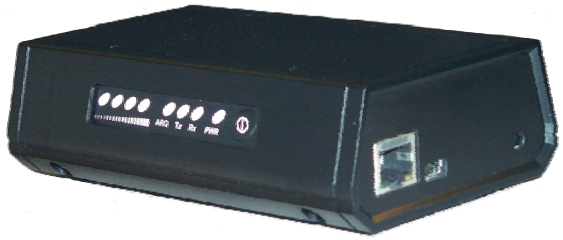

Figure 6: Portable Access Device (PAD)

The PAD (Figure 6) is a small box (3 3/8" x 5 3/8" x 1.5 ") that includes a card and an antenna, and it has a USB port and an Ethernet port for connecting to computing devices. The first iteration of the devices required the user to depress the power button to turn the unit on. Later releases automatically powered up and proved valuable in the event of a power failure. This feature was very useful in the command bus setting where the unit was immediately available when needed. Upon power up, each device was authenticated by the network. The PAD requires no host computer or software and was directly connected to a router, desktop, or notebook computer that supported a USB or Ethernet connection.

Security was provided for both the PAD and the PCMCIA card. If a device or card was lost or stolen, the device or card could be removed from the AAA database and would not be able to gain access to the network. Users employed additional security measures by controlling access to Mobile Data Terminals (MDT) and by using encryption of transmitted data.

SYSTEM PERFORMANCE

Overview

The WARN demonstration was positive and valuable to the Washington D.C. Metro-area public safety community. WARN was able to satisfy almost all expectations, and it met the basic needs of emergency personnel. Specifically, WARN supported the broadband applications, provided coverage over a wide area, and was easy to use. Furthermore, the cost of implementing and operating the network was significantly lower than the existing LMR system. During the demonstration, the technology and system proved to be scalable, allowing additional sites to be integrated without difficulty in order to improve coverage and capacity.

A main reason for the network's success, however, was the added value provided to public safety operations and the resulting positive reception from the user community, as reflected in Appendix E. In particular, WARN enhanced capabilities and interoperability of local and federal public safety agencies in major planned events such as the Presidential Inauguration, the State of the Union Addresses, the Fourth of July celebrations, the World Bank and IMF demonstrations, as well as unplanned emergency events, such as the Cardoza High School mercury spill incident, and others.

Additionally, using WARN stimulated creativity in its users who developed further uses of the network. For instance, two such examples include the U.S. Park Police (USPP) and the District's Fire Department developed a protocol to share USPP helicopter video over WARN to enhance emergency operations (that will be useful in events such as major fires). Also, the District and neighboring jurisdictions recognized the need for regional interoperable data solutions using broadband. As a consequence, the NCR initiated an exhaustive Regional Data Interoperability Program that includes the deployment of a Regional Wireless Broadband Network (RWBN).

Network Performance

WARN provided average speeds of 1 Mbps downlink (base-to-mobile) and 300 kbps on the uplink (mobile-to-base). It achieved these speeds outdoors with a mobile antenna inside a vehicle. These speeds provided the flexibility needed for delivering essential video streams, high-resolution images, and GIS information. The speeds were fast enough that the multiple streams and data information could be shared at the same incident location. The throughput of data improved as the signal level increased relative to the noise level. Throughput was at its weakest where the signal level was low and the noise level was high. Low throughput areas also included those where the signal was strong from other sites.[33] This performance was similar to in-building coverage of the District's radio network with only ten sites.[34] Detailed coverage maps and performance information can be found in Appendix D.

The implementation of QoS also efficiently managed the capacity of the network to share bandwidth among simultaneous users. Each user was assigned a profile and depending on the users' role (e.g., commander vs. officer) and the application used (real time or not), the system was able to prioritize traffic. The data transmission rates were also capped based on user needs.

The coverage of the system was less than expected by the District – especially at the edge of the system and at locations equidistant between sites. With the initial ten sites, the system provided outdoor connectivity (greater than 0 kbps throughput) to 95 percent of the city.[35] The District had expected that the system would provide broadband (a minimum of 300 kbps)

[33] The Flarion Flash OFDM technology uses the same frequency at each site; therefore, these other sites will cause noise among themselves.

[34] The District's LMR network was measured to provide more than 95 percent coverage and various levels of in-building coverage. On average, the system provides good audio quality inside most buildings through the first two walls.

[35] The contract called for 95 percent coverage of the city.

coverage over 95 percent of the city. In addition to capacity needs in strategic areas, this coverage deficiency led to adding two sites post network acceptance. Two factors contributed to this situation.

First, Flash-OFDM was not able to accept self-interference (cases in which the signal level of two adjacent sites is roughly equal) and maintain good data rates. In these areas, connectivity and throughput was highly variable. The cell edge is the geographic area located at the border between two sites' coverage areas. At this location, two signals of comparable strength were received from each site at the same location. Because the system used the same frequency at each site, these sites interfered with each other. When this condition occurred, the throughput of the system was very low and connectivity could have been lost. When compared to LMR, however, the use of the same frequency provided far greater spectral efficiency and scalability. Improvements in the ability to resist interference were needed to take advantage of the efficiency while ensuring reliable service for public safety users.

Second, the Flash-OFDM technology operates at lower power levels and antenna heights than the LMR network. Transmitted power levels of the Flash-OFDM technology were much lower than the LMR system, and radio propagation range is directly linked to how much power is transmitted (the more that is transmitted, the longer the range). Similarly, lower antenna heights lead to more obstacles that reduce signal levels, resulting in reduced transmission site range.

On the terminal side, the PC cards were transmitting a power of only 250 milliwatts, or less than one-tenth of the power of the typical handheld LMR unit operating at three Watts, and less than one-hundredth of the power of a mobile unit operating at 35 Watts. However, this tradeoff enables important capabilities such as the use of PC cards.[36] On the base station side, the WARN transmitters operate at one-fifth of the transmitter power of the LMR system. Even in situations where the content is downloaded from a server, the mobile unit must be able to communicate that messages were received properly. Therefore, this reduction in power from the mobile unit results in a smaller footprint per site.

Transmitting antenna height is also a factor in radio propagation range. Lower antennas are more impacted by natural obstacles (e.g., buildings and trees) and thus have reduced coverage footprints. For example, the Washington Monument is visible over a far greater range than the much shorter Lincoln Memorial. This same principle reduces the signal levels of shorter transmission sites. The WARN antennas were ten to 400 feet lower than the LMR antennas. This was done to reduce interference to other parts of the system and maximize spectrum efficiency. This tradeoff increased available use of the spectrum by focusing the coverage only where it was needed for each site. There were, however, some potential solutions to these coverage deficiencies without sacrificing the positive aspects of the lower power levels and antenna heights.

Two additional transceiver sites were added to address coverage/capacity issues in critical areas of the District after the initial ten-site deployment. The first site, in the vicinity of the White House, provided additional capacity for the White House and its grounds, as well as for part of World Bank neighborhood. The load on this site increased significantly, particularly

[36] The power consumption and heat output of a three Watt transmitter would not allow for PC card or other small form factors.

during major public safety related events. This site was added before the 2005 Presidential Inauguration in anticipation of significant traffic in the vicinity of the White House.

The second site was later added near Robert F. Kennedy Memorial Stadium (RFK) to alleviate coverage issues around the stadium and along the Anacostia River. This site enabled the support of first responders' critical communications during the Washington Nationals' baseball games. During the games, the D.C. Emergency Management Agency (DC EMA), the D.C. Metropolitan Police Department (DC MPD) and the D.C. Fire and Emergency Medical Services (DC FEMS) were deployed on site with their command buses, generating a high-traffic demand. Support of this demand was not possible before this additional site was operational.

The ease of integrating two new sites demonstrated the scalability of the system. The two new sites used the same frequency as the ten initial sites, and their footprints were contained in the coverage area of the initial system. As a consequence, their integration did not necessitate additional coordination with potential interferers, but it required some limited fine tuning of the parameters of WARN's configuration.

Due to the existing operations on the network at the time, the District could not perform throughput testing, as it could have disturbed public safety emergency communications. However, measurements of the Signal to Noise Ratio (SNR) allowed the District to estimate that the throughput, at the 95th percentile, was 200 kbps for the 12-site system.

Subscriber Device Performance

The failure rate of the subscriber devices has been very low since WARN operations began. Of the nearly 200 devices, fewer than five cards or PADs were replaced, and only three antennas required replacement as of August 2006. Thus, the failure rate was less than 2.5 percent in one and a half years (or a 1.6 percent overall annual failure rate).

More problematic, however, was that the PADs did not automatically power up when power was available during initial deployment. In the case of the command bus implementations, operators were already overloaded with duties; therefore, an automated solution was required. The District worked with Flarion Technologies to secure a modification to more than half of the PAD inventory to automatically power up the PAD when power was supplied to it. As a result, as soon as the command bus power supplies were on, the PAD provides the bus LAN with a connection to the DC WAN and Internet.

OCTO also identified a need to provide alternative subscriber device sizes and functions for WARN access. For example, many public safety personnel had notebook computers that were capable of embedded wide-area modems. These internal modems were more rugged and lacked the obtrusive WARN antenna. Additionally, the only PDA solutions that could accommodate a WARN PC card required a heavy and bulky expansion pack and a very limiting battery life. Finally, the District is a significant user of Automatic Vehicle Location (AVL). The systems that support AVL include an integrated Global Positioning System (GPS) receiver with a wireless modem; however, no such product was available for WARN compatible devices.

Application Performance

While supporting local and federal agencies in implementing and operating their communication applications, the program continuously fine-tuned the configuration of the available applications and evaluated alternative and creative solutions with vendors to better meet the needs of public safety first responders.

In particular, streaming video was a crucial application for first responders. Those video applications were particularly challenging in terms of data throughput and network load, and therefore drove the dimensioning of the network and the associated public safety spectrum requirements. The demand to enhance the availability and effectiveness of video applications for WARN users required significant efforts to review and evaluate video applications that were available on the market. Evaluating such applications allowed WARN users and OCTO to work closely with vendors to improve their products to match public safety's mobile communication needs.

Pilot research results showed that an increasing number of video products were maturing and becoming better positioned for the public safety wireless environment. Bandwidth requirements varied widely with the vendors' solutions, as did the quality of the video itself. A key criterion for evaluating the application was its flexibility to match the quality of the image (and therefore the required bandwidth) to the specific need of the first responder.

For instance, with the addition of the D.C. Department of Corrections (DC DOC) as a user on the network, KaptureNet was added as a video surveillance application to be used over the network. KaptureNet helps provide incident control during the transportation of inmates. In order to provide incident control, video is recorded and downloaded at a designated site, and it is also accessed wirelessly and instantly when necessary. The unique aspect of this product is that it combines a GPS locator with video to provide accurate geographical surveillance to the DC DOC. As a consequence of adding KaptureNet to WARN, the DC DOC was able to locate their vehicles at all times and could essentially "check-in and look" whenever they wanted to do so. To ensure the effective functioning of the application, the DC DOC and OCTO worked closely with the vendor to optimize their algorithms and ensure that adequate service was provided to the end-user.

The pilot program team also extensively evaluated Motorola's Greenhouse software, which contains streaming video components. It was used by several agencies including the USPP. The major upgrades made to the software are detailed as follows:

- The first upgrade was the addition of new codecs. Motion Joint Photographic Experts Group (JPEG) and H-264 were added to the existing Motion Picture Experts Group version 4 (MPEG4) codec.[37] This variety of codecs enables users to rank the merits of each and select the most appropriate one for their use.

[37] The video codec converts the video image to data packets that can be transmitted over a communications link or stored for later use. The codec codes the image on the transmitting end and decodes the image on the receiving end. In general, the higher the transmission rate, the higher the overall quality of the video image. However, the various video codecs are proficient at different tasks and there have been significant improvements to low data rate, yet high video quality codecs on the market. H.264 refers to the jointly developed video standard of the International Telecommunications Union Video Coding Experts Group and the Motion Picture Experts Group.

- Second, users were given the option to select not only the codec to be used, but also the transmitted bandwidth. This option brought some flexibility to the users to transmit at a lower quality level when the network is saturated or the radio conditions are not optimal.
- Third, a new version of the software was deployed that used one uplink stream independent of the quantity of users viewing the video. Previously, multiple viewers of a single video source would require as many uplink streams and thus significant amounts of scarce bandwidth. With the previous version, each user downloading the same streaming video transmission would take up additional bandwidth.

NETWORK USAGE

Overall, the pilot fulfilled the original purpose for which it was defined, which was to deploy and demonstrate a broadband public safety network used on the 700 MHz spectrum that emphasized sharing among public, private, and government agencies. There were multiple effective deployments of pubic safety applications over the network and no interference issues were documented from the use of the upper 700 MHz band.

Specifically, in regard to the interference issues, it is important to note that since the WARN network base stations began transmitting, Maryland Public TV station (Channel 62) did not report any interference issues. Likewise, WARN did not experience any interference issues from Channel 62.

The planning, deployment, and operations of WARN provided many useful insights about the effectiveness of the wireless broadband solution for public safety. They also highlighted several areas where improvements were needed. Many of these improvements were identified as a result of major events during the demonstration project.

Use of the network was relatively consistent over time. WARN was used on a daily basis with very high traffic volume during major events. Figure 7 illustrates comparatively equal uploads and downloads and notes the high traffic events. The total monthly traffic averaged almost 25 gigabytes of data from January 2005 through August 2006, amounting to an average of 130 megabytes per month per user (assuming 190 users).

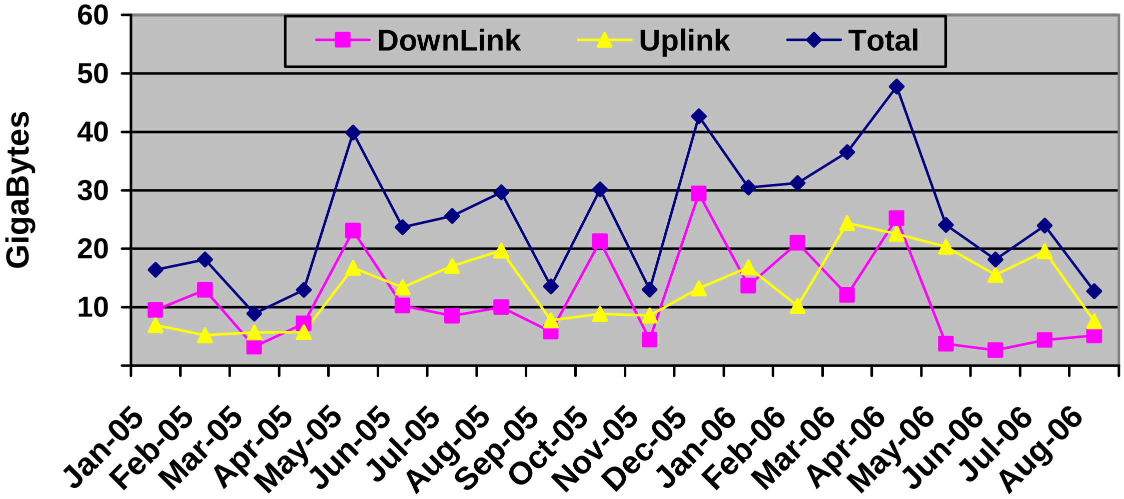

Figure 7: Monthly Data Transmission

The WARN network was used to support federal and District first responders and their agency command buses (USPP, Metropolitan Police Department, DC FEMS, and the DC EMA) during several large events in the District. For example, these events included the Fourth of July celebrations, the Million and More March, the World Bank and IMF demonstrations, anti-war protest marches, the Jamaican Festival, at the D.C. Armory for Hurricane Katrina evacuees, and the President's 2005/2006 State of the Union Addresses.

During these events, user agencies employed a variety of applications that enabled them to access remote Computer-Aided Dispatch (CAD) features to track vehicle fleets (I/Netview), transmit and receive across the city multi-streaming video links (LiveWave, Greenhouse, TrafficLand, KaptureNet), access and share critical data with other agencies and/or jurisdictions (CapWIN, JUSTIS, WALES), and remotely access vital information (Internet and GIS).

The USPP was a very active user of the system. For example, WARN was utilized by a patrol officer in Rock Creek Park during an arrest. The officer was able to access one of the three criminal information databases through CapWIN and determine that the individual was wanted. Additionally, USPP and OCTO jointly evaluated and determined best practices in the transmission and use of video from a helicopter. This capability was of keen interest to all first responder agencies, as they were interested in pooling resources and collaboratively sharing this type of information on a regular basis.

Another key user of the system was the DC FEMS, which actively used the WARN cards in a variety of functions, such as transmitting pictures from the Public Information Officer to media outlets, filing real-time reports in the arson department, and improving responses to chemical alarms in the hazardous materials department. Additionally, DC FEMS equipped their command bus with the capability to communicate on the WARN network. DC FEMS used the system on site at such incidents as the mercury spill at Cardoza High School on March 2, 2005. Following the success of these operations, DC FEMS requested additional cards to be deployed throughout the agency.

Customer Feedback

Since August 2005, the District asked WARN users to complete monthly customer surveys in order to assess the value of WARN and to capture needed improvements.[38] The surveys seek user opinions on coverage, reliability, support, benefits, and satisfaction with all aspects of the WARN network, including available technologies, network coverage, speed of communications, and usefulness. The response rate of these customer surveys is typically 30 percent of all users. The customer surveys allow the WARN team to measure how beneficial the network is to public safety operations as well as to obtain a thorough understanding of future technical requirements or items needing improvement.

Overall, customer satisfaction with all elements has been very high. Average monthly user ratings are shown in Figure 8: User Survey Results. The highest scores were support, benefit, and overall satisfaction, while the lowest-rated elements were mobile terminal antenna reliability and consistent coverage. This feedback was consistent with the findings of the coverage differentials between the District LMR system and WARN and with the lower throughput noted at cell-edge (see section on "Network Performance"). High scores on support were largely due to the attentive WARN customer support team. The small user community enabled this team to provide more personal customer support and quickly address any problems. In fact, the WARN customer support team spent considerable time working on issues that were unrelated to WARN network or subscriber device operations. The team typically helped customers bring new applications onto WARN and provided troubleshooting support for these applications. High benefit and overall satisfaction are testament to the usefulness of a broadband connection for public safety. For specific user feedback collected by the District regarding WARN use, see Appendix E.

[38] NTIA did not commission, pay for, or seek to have these customer surveys as part of the WARN pilot. In fact, the surveys were being conducted prior to NTIA's involvement with and selection of the WARN. The District collected and analyzed the surveys and provided this information to NTIA for inclusion into this report.

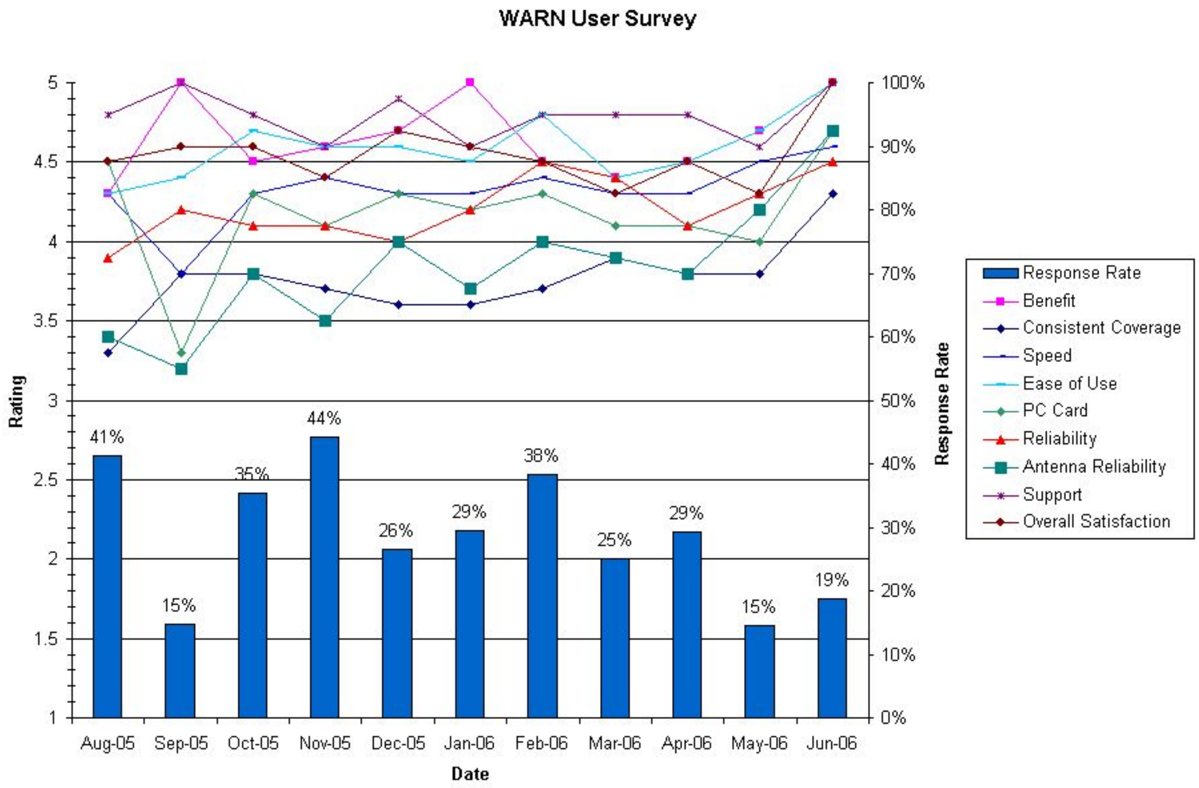

Figure 8: User Survey Results

The District received the most suggested improvements in the coverage category. As noted in Appendix E, the system provided broadband service in most of the city; however, public safety personnel needed and expected connections anywhere they had the potential to respond. Therefore, broadband connections were needed everywhere. Even with two additional sites and 700 MHz operation/propagation, many points in the District had limited connections.[39]

The lessons learned from the users of the network were among the most significant results of the pilot program. The network was not truly valuable unless beneficial data was shared by the WARN users. As seen in the customer survey reports, the users in the pilot program found the network of significant value to their everyday activities, as well as for large-scale incidents or events.

One of the most significant lessons learned from the user community was that public safety was unaware that these types of solutions were possible. Additionally, it was recognized that technology alone was insufficient for delivering useful solutions to public safety. Technology must accompany training and development of solutions that fit the public safety operational model. Once applications and systems met the operational needs of public safety and the user community was able to fully understand the benefits of the solution, the full benefit derived from a broadband network was realized. Furthermore, the WPO customer operations group was instrumental in ensuring that the users were able to make complete use of a broadband solution and were able to support ancillary systems.

[39] These limited connections take the form of low data transmission rates, temporary loss of connection, or both.

SIGNIFICANT WARN DEPLOYMENTS

Since January 2005, WARN was deployed at a number of events throughout the District. The use of WARN during major events demonstrates that WARN was both a critical and effective network for facilitating communications and data exchange among agencies to promote public safety. Furthermore, major events require special attention: they caused the most significant loads on the network and demonstrated the ultimate capabilities and benefits WARN provided. WARN became a resource that the public safety community relied on to facilitate command decisions from a remote location.

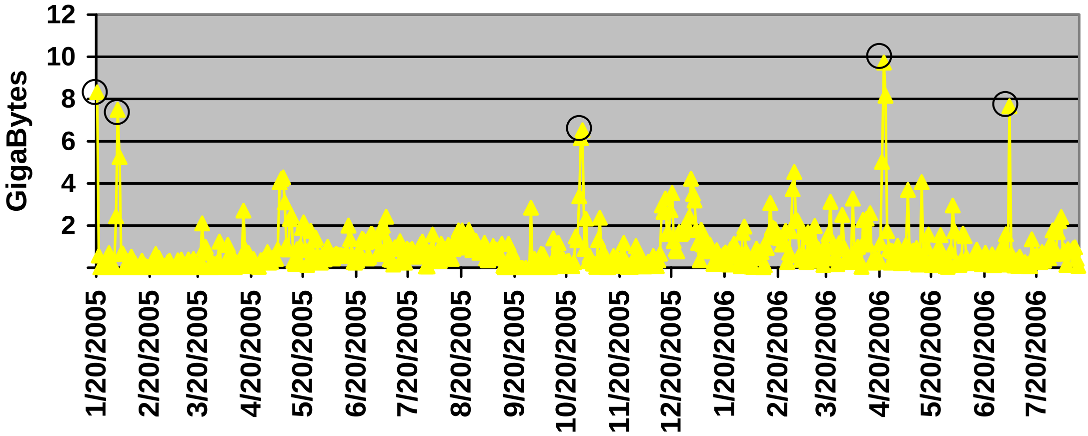

Figure 9: Daily Total Traffic Transferred

Figure 9 shows the five periods of highest WARN traffic. These periods saw public safety employ significant video applications to augment their operations causing spikes in network traffic. Both federal and District law enforcement use of video surveillance were the dominate drivers for these high-demand days. The five periods were:

- January 20, 2005: Inauguration Day
- February 2, 2005: State of the Union Address (including preparatory efforts on February 1, 2005)
- October 28-29, 2005: A.N.S.W.E.R.[40] demonstrations and IMF meetings
- April 21-23, 2006: IMF/World Bank meetings
- July 4, 2006: Independence Day-Fourth of July celebrations on the National Mall

Details of a few planned, major events in which WARN enabled the transmission of high-speed data from remote locations follow. These events highlight significant developments during the implementation of WARN and do not necessarily reflect the five busiest events as noted above. The first official deployment of WARN was the Presidential Inauguration in January 2005. The final event of this demonstration, July 4, 2006, illustrates the extensive

[40] A.N.S.W.E.R. refers to the coalition to Act Now to Stop War and End Racism.

progress that was achieved in deploying applications to meet public safety requirements during the demonstration.

Presidential Inauguration, January 2005

The geographic scope of the event included the parade route from around the White House up to the U.S. Capitol and back. The participants included the DC MPD, U.S. Secret Service (USSS), DC EMA, DC FEMS, USPP and WMATA. To coordinate the security of this event, agencies were contacted in advance, but most of the implementation occurred within one week or less.

During the Inauguration, most users planned to run standard Web-based applications (e.g., Web-based news) though one agency deployed an uplink video system that enabled command centers to have a view of streaming mobile video signals. Another agency worked with OCTO WPO to deploy Motorola's Greenhouse software in order to provide bi-directional audio and video with the intention to stream video from a command bus and an additional cruiser to an Operational Control Center. Other fixed video streams were transmitted from this Operational Control Center to other locations in the metropolitan area using commercial satellite communications. These video streams were used to allow command centers to monitor crowds, the progress of the Presidential motorcade, and other public safety operations.

The USSS accounted for more than 60 percent of the total traffic carried by WARN on that day (five gigabytes of a total of eight gigabytes). The use of real-time streaming video accounted for this traffic. The application used by USSS, LiveWave, uses motion JPEG to transfer video information. Essentially, this system transmits compressed snapshots in succession. Unfortunately, the motion JPEG system uses significant bandwidth to send just several frames per second.[41] The system tries to send as many frames as possible; therefore, it quickly overloaded the network.

OCTO staff worked with participating agencies to ensure the applications would function as needed. Multiple modifications of security systems were required to allow these applications to function. Significant advanced planning was necessary to ensure the integrity of the District and federal facilities, to maintain security, and to provide the needed wireless functions.

The generated traffic on WARN during this event was in the downtown area of the District, between the surroundings of the Capitol and the neighborhood of the White House. Three sectors of the WARN network covered this area.

[41] Full motion video requires 24 or more frames per second. Lower frame rate solutions cannot accurately portray fast moving objects.

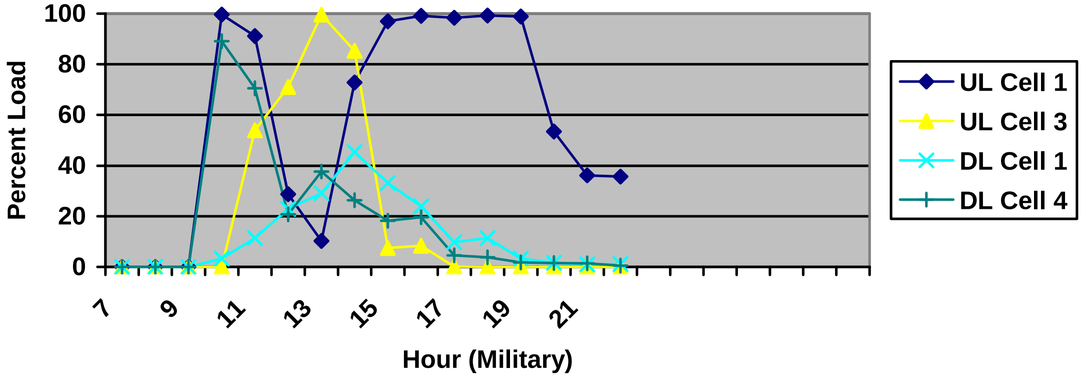

Figure 10: Hourly Traffic of January 20, 2005

Figure 10 shows the total loading of several highly-utilized sectors or cells during Inauguration Day. The measurement of this load was reported every fifteen minutes. This graph shows that for several hours, several sectors had a load of nearly 100 percent and therefore experienced overload conditions at some point during the 15 minute measurement period, especially on the uplink or upload path (mobile terminal to base station noted as uplink (UL), i.e., uplink in the figure). The two cells with the highest load, Cell 1 and Cell 3, served the White House and the U.S. Capitol, respectively. Note that traffic was highest at the Capitol during the Inauguration itself and that loading on the White House site continued through the night due to ongoing events. Only cells with a significant load are shown, and therefore, Cell 3, serving the Capitol, never had an appreciable load on the downlink (DL). Cell 4 covered part of Pennsylvania Avenue and part of the Mall between the White House and the Capitol.

The first significant use of WARN demonstrated its importance for public and national security, and it demonstrated that agencies can effectively operate on one network while performing different tasks. This initial large-scale use of WARN proved that advance planning is critical to achieving successful operations. Additionally, it was important to implement QoS so that no one agency acquired all of the available bandwidth. The use of applications that were bandwidth-efficient was a key to achieving successful operations. The implementation of an additional temporary site to support the needs of the USSS demonstrated the scalability and flexibility of the technologies. Finally, the system required much greater testing to ensure that upon failure, the system engaged the secondary components.

Independence Day, **July 2005**

WARN was used to support a number of agencies during the Independence Day celebrations on the Mall in 2005, which included activities on the Mall between the National Monument and the U.S. Capitol. Although this event was not considered one of the five busiest events, it highlighted a number of issues/applications of importance. There was significant coordination among OCTO and the users for this event. During this event, WARN mainly supported the USPP, the DC EMA, DC FEMS, and the DC MPD.

At this event, the applications deployed were:

- **I/Netviewer:** This is an application that allows remote access to the Computer-Aided Dispatch (CAD) system. It includes tracking and monitoring of vehicles using remote GPS, and was available in a command bus.
- **LiveWave:** This streaming video application uses motion JPEG to code images. Typically, it was used to send streaming video feeds from mobile cruisers to a server. It was then possible for any authorized user (typically a mobile command bus or a fixed command center, or even another cruiser) to pull the video on demand. Each video feed required up to 350 kbps or more.
- **Greenhouse:** This streaming video application uses MPEG4 as a codec. It also supports peer-to-peer video communications. Its capabilities are similar to LiveWave, except that its throughput requirements range from 100 kbps to 150 kbps per video feed with full frame rates (15-24 frames per second). The downside to this application is that it required consistent throughput (video quality degrades when the available speed drops below 100 to 150 kbps) and the video quality was not as crisp as the LiveWave solution.
- **TrafficLand:** This application includes a set of DC DOT cameras located at strategic locations (crossroads, sensitive buildings, etc.) and was connected to the DC WAN. It was possible for authorized users (command bus) to access cameras and download images. This application has various service rates. The basic service provides roughly one frame per second (not full motion) and requires about 45 kbps. The advanced service uses nearly full motion and requires hundreds of kilobits per second.
- **CapWIN, JUSTIS and WALES:** These are applications enabling regional public safety users to query several regional public safety databases and exchange messages.
- **Internet:** This application provides general Internet access with a particular emphasis on live weather updates and access to other information databases.

During Independence Day 2005, OCTO personnel were stationed at the USPP command bus to assist in the set up and maintenance of the system. With a combination of four agencies heavily using the network, it was vital to ensure the sharing of resources functioned efficiently. According to verbal feedback from the users, the District realized a savings in time, money, and personnel through the sharing of valuable resources such as video.

Moreover, during this event, the network enabled the deployment and the usage of these applications in a wide geographical area. Support of the applications would have been impossible with the traditional wireless technologies available to public safety, as illustrated in the following testimony from Lt. David Mulholland, USPP:

> “The United States Park Police increased its usage of the WARN network commencing with the National Fourth of July Celebration on the National Mall. The United States Park Police had currently used WARN to provide high-speed connectivity to its Mobile Command.
>
> On the Fourth of July, the United States Park Police also expanded usage of the WARN network to its stationary operation center, functioning as a Multi-Agency Communications Center for this activity, allowing connectivity to CapWIN, the

> United States Park Police helicopter video downlink (real-time), DC DOT traffic cameras, and the District JUSTIS network.
>
> Additionally, the United States Park Police deployed WARN as the primary connectivity medium for two mobile data computers in patrol vehicles. These patrol vehicles tested the reception of WARN throughout the western half of the District including the Rock Creek area. The tests were met with very positive results. These MDCs[42] were also used to receive real-time video imagery from the United States Park Police helicopter. They continue to be used as the primary means of connectivity for these two patrol vehicles."[43]

Independence Day, July 2006

WARN was utilized to support a number of agencies during the events of Independence Day 2006 which included activities on the Mall between the National Monument and the U.S. Capitol. Representatives came from a cross-section of agencies, including state, local, federal and non-federal organizations. The agencies included the National Park Service (NPS), USPP, the Red Cross, Smithsonian Institute, WMATA Transit, WMATA Police, DC DOT, DC FEMS, DC EMA, OCTO, the National Weather Service (NWS), and the DC Public Health Service (DC PHS).

For this event, a significant alteration to the network occurred on Monday, July 3, 2006, when the USPP gave permission for DC FEMS to view their helicopter video over WARN (using Greenhouse). The OCTO WARN team modified the Greenhouse installation on the DC FEMS command bus to allow them to sign in as part of the USPP domain.

During the July 4, 2006 celebration, the USPP hosted a Multi-Agency Communication Center (MACC) at their Anacostia facility, during which WARN was used to facilitate the transmission of streaming video from multiple remote locations back to the MACC. The purpose of a MACC is to provide a remote location for all agencies to provide assessments and from which to make command decisions.

The MACC was set up with five large plasma displays. One was dedicated to the air traffic control radar, one for the NWS, two for TV stations (CNN/FOX), and one for WARN and Greenhouse. The NWS feed and traffic information (via TrafficLand) were delivered over WARN. The equipment used for this event included a Laptop PC with a WARN PCMCIA card and a WARN PAD connected to a router that provided Internet access to half of the computers in the MACC.

The DC-FEMS command bus at 15th Street NW and Constitution Avenue NW transmitted video pictures from the mast camera to the MACC using Greenhouse. This particular view was used all day by the MACC users to observe crowd size, review the parade,

[42] Mobile Data Computers (MDCs) are rugged personal computers that largely serve the same function as standard desktop or notebook PCs and are typically mounted inside vehicles. They are hardened to withstand the vibration and heat of the mobile environment.

[43] E-Mail correspondence from Lt. David Mulholland (USPP) to Guy Jouannelle (Televate), August 21, 2005, quoted in the District of Columbia THIRD PROGRESS REPORT on the Construction and Operation of the Experimental Wireless Accelerated Responders' Network (August 2005), at 13.

and observe the effects of the severe thunderstorm that moved through at 5:30 pm. The staff on the DC FEMS Mobile Command Unit had the ability to pan, tilt, and zoom the mast camera at the request of staff from the MACC.

When a strong line of thunderstorms entered the NCR, WARN provided a tremendous benefit via its connection to the NWS. The joint team at the MACC used the NWS feed to determine that the storms were quite severe and decided to evacuate the National Mall and take cover. This proved to be beneficial, as the large tents blew over and could have caused injury. All of this was visible to the emergency personnel at the MACC via several DC DOT, USPP, and DC FEMS cameras situated on or near the Mall.

The careful planning and continued relationship-building demonstrated through the MACC resulted in a smooth execution of the systems and further demonstrated the benefits of the WARN network across agencies. Additionally, they provided insight to the benefits that can be derived among many agencies – even those without wireless broadband connections. For example, DC DOT was able to receive important weather information and traffic camera information at a joint command post. Ultimately, this last significant deployment showed how improvements to WARN increased user education, and how inter-agency communication created a network that was critical to public safety needs.

SECTION 4

FEASIBILITY OF COMMERCIAL SERVICES

BACKGROUND

The proliferation and deployment of Commercial Mobile Radio Services (CMRS) now extends beyond the traditional cellular voice communication to include wide-area, high-speed data communications. Initially, data service, such as text, was limited to low-speed Cellular Digital Packet Data (CDPD) services. However, within the past few years, the technologies and networks that support far greater speeds have become available and public safety agencies have adopted these services. Commercial wireless and broadband services could offer a potential alternative for private public safety networks to assist in emergency response and preparedness and to improve or augment existing infrastructure or capabilities. However, the public safety community identified wider-bandwidth applications that CDPD services at the time could not support. Additionally, CDPD has since been phased out in favor of wider-bandwidth applications and solutions. In response to consumer demand, the CMRS carriers have deployed broadband services in cities across the United States. These wireless broadband connections are available at major metropolitan areas for about $60.00 a month for unlimited use of the services.[44] Hence, a user with a properly equipped laptop or smart phone with a PC card can get a high-speed wireless connection for such things as downloading streaming video, accessing Web sites, or opening e-mail/text attachments.

COMMERCIAL SERVICES IN THE DISTRICT

Prior to the development of the WARN pilot, the District examined the use of commercial networks and services to deliver broadband applications. In February 2003, the District informed the FCC of its needs during a presentation to the National Coordinating Committee. In that presentation, the District stated that its known broadband applications required:

- Forward link (Base-to-Mobile) throughput of 1.56 Mbps;
- Reverse link (Mobile-to-Base) throughput of 325 kbps;
- Commercial off-the-shelf technologies;
- High mobility; and
- Full scalability.

During the course of 2003, and up until the Request for Proposal (RFP) was issued in August 2003, the District further refined its requirements to include:

[44] Commercial carriers AT&T, Verizon, and Sprint/Nextel all offer wireless broadband services in the District. *See* for example http://b2b.vzw.com/broadband/serviceoverview.html and http://powervision.sprint.com/mobilebroadband/.

- 1.5 Mbps forward link and 500 kbps reverse link throughput at the 95th percentile;
- Support prioritized use to dynamically address its own user needs; and
- Multicasting capability to create more efficient streaming video and audio expected in the public safety operating environment.

At the time, the fastest data service offered by the commercial providers was 1xRTT which had typical speeds of 80 kbps. In October 2003, Verizon Wireless launched 1xEVDO Revision 0, which, for the first time, provided commercial wireless broadband speeds. In discussions with the commercial carriers at the time, the District found that they could provide:

- Forward link throughput of 2.4 Mbps (with 80 percent of the channel speed available to the users);
- Reverse link throughput of 153 kbps;
- No support for prioritized use;
- No support for multicasting capability; and
- No support for continuous streaming of media, including video and audio, in either direction, because their service agreement did not allow for it.

As a result, based upon the District's articulated requirements as noted in their RFP, and the available commercial offerings as stated, the existing technology of the commercial carriers did not meet the expected needs of the District in late 2003. The District quickly recognized the promise of the technologies utilized by the CMRS. However, the District found that the carrier solutions did not provide the level of network management, control, throughput, coverage, security, and reliability desired. The District had just lived through LMR outages during Hurricane Isabelle when it relied on commercial interconnect services that failed. It now operates on a redundant fiber ring it calls DC-NET. Additionally, the throughput offered by the CMRS community did not satisfy the District's need for streaming video from the field.[45]

The District also recognized that in many scenarios rugged devices were not essential for data communications. The model for data exchange in the District was a vehicle-based solution that did not typically come into contact with harsh environments. The existing commercial subscriber solutions were largely meeting the needs of the public safety community for data communications. More importantly, at the same time, the LMR devices did not provide the throughput demanded by the District's emergency response personnel.

The District concluded during its studies that the commercial technologies were viable for public safety data, but the commercial services and networks were not. Essentially, the subscriber and network equipment could be public safety grade, but the network needed to be controlled in order to manage priorities and dedicate bandwidth where needed. It was also necessary to have a solution that was built for an event requiring high-speed, high-volume data exchange, such as the 9/11 Pentagon incident.

[45] Verizon Wireless had launched its EVDO Rev 0 network that offered peak uplink data rates of 153 kbps. The rate of the entire channel to an end-user is somewhat lower and is shared with other users on the site.

The District recognized that its broadband network would be an island of coverage for some time. It further recognized that routers could support switching between its private network and commercial networks. Such routers, however, required a large host incapable of supporting handheld configurations and such a host would cost in excess of $2,000 per vehicle – a direction the District was hoping to avoid. In light of these economic realities, the District was optimistic that Nextel (then independent of Sprint) would select Flarion Technologies' Flash-OFDM technology for its national broadband network. Later, Sprint would purchase Nextel and abandon the Flash-OFDM technology, thereby making roaming to a nationwide commercial network with the same devices very unlikely.

The District recognized that control of the network and the users would prove to be invaluable. Not only would this control lead to improved uptime of service, but it also allowed for improved distribution of capacity to the needed users as well as enhanced security. Through advanced QoS parameters, the District was able to prioritize traffic and cap the throughput available to users. Considering the disparity of usage, from hundreds of bits per seconds for simple text transmission to hundreds of thousands of bits per second for streaming video, managing priorities and overall QoS is very important for broadband data networks. For its broadband network, the Wireless Program Office was able to pre-plan events with significant video usage and use these control mechanisms to ensure the right information was transferred over WARN in a timely manner. Additionally, since WARN was within the DC WAN, it was protected by the same security measures that protect the servers and desktops within the District.

The District currently uses commercial data services for its other operational public safety needs. These other commercial services are required, due to the limited scope of the experimental license, therefore a limited number of subscriber devices were purchased. The District uses nearly 1,000 commercial AVL modems for public safety vehicles and an additional number of handheld data devices. The District sees this as an interim solution until it can build a permanent network operating on a fully operational FCC license with widely available subscriber devices. The District recognizes that the commercial carriers represent communications solutions outside the coverage area of public safety broadband systems, and that they can serve as a redundant backup to public safety systems. The District seeks partnerships with the CMRS community by utilizing the commercial carrier's existing operations, thereby allowing the District to satisfy its needs as economically as possible by reducing deployment and operational costs.

Finally, the WARN, as a pilot, enabled the District and its personnel to fully understand the District's needs as well as its ability to operate such a network, and to determine the overall benefits. A services-based approach from the commercial carriers was not pursued for WARN for the reasons as noted above. The District examined the use of commercial services to fulfill its broadband needs under this pilot, and the specific conclusions of the District in development of the WARN were based on their own analysis of the service offerings at that time. Nonetheless, the capability of commercial services to provide the network management, control, throughput, coverage, security, reliability and applications remains an open issue for the public safety community as a whole. As the District continues the implementation of the WARN, it should reevaluate the evolving offerings of commercial technology and services and take advantage of those that meet the District's requirements.

To fully evaluate the capabilities of the commercial offerings or the ability of proposed commercial systems to meet public safety broadband requirements necessitates a complete and transparent presentation of those requirements. In response, the commercial providers would need to delineate those requirements they can or cannot meet. Furthermore, in the evaluation of options of government-owned versus commercial services, funding, maintenance, and ongoing transition of technology will need to be considered.

SECTION 5

OBSERVATIONS AND RECOMMENDATIONS

By all accounts, the WARN 700 MHz broadband pilot met the objectives of testing the operational and cost-effectiveness of sharing spectrum between federal, state, local, and other private users. Considerable interest by the public safety community at large, Congress and the FCC has shown that there is a real demand for broadband services. Based on this pilot, the following observations were identified and recommendations developed to demonstrate the feasibility of public safety spectrum sharing initiatives and broadband solutions.

OBSERVATIONS

Benefits

Data applications are becoming more important to support response and recovery efforts. The WARN system provided ample benefits to both federal and non-federal users and demonstrated a successful, cost-effective, spectrum-sharing initiative. Importantly, it used only 2.5 MHz of spectrum, yet delivered tens of Mbps of data throughput, demonstrating efficient use of scarce spectrum resources. It delivered sufficient broadband speeds in most situations, but needed improved coverage to allow public safety to reliably use broadband speeds wherever required. The most beneficial aspect of this demonstration project, however, was in the collaboration between federal and District agencies. Such coordination was only possible because of the significant capacity offered by WARN. Without this capacity, the District would not have been able to accommodate the additional demand of the federal agencies. Ultimately, the project demonstrated not only successful spectrum sharing, but also successful spectrum use. WARN could be a model of the future of public safety communications as a result of its high bandwidth capabilities that supported voice, video, text, images, and a host of other critical public safety applications. Similar broadband technologies also harness the economies of scale of commercial markets, and provide far greater capabilities at ever decreasing costs. As such, projects like WARN demonstrate great promise for addressing the next generation of public safety interoperable communications systems.

The use of WARN provided significant benefits to federal agencies within their organizations, including interoperability that might not have been possible if the agencies had used different networks. The high degree of collaboration between the USPP and the District afforded tremendous additional opportunities for interoperability. For example, DC FEMS and USPP personnel became familiar with one another’s capabilities and needs via WARN user group meetings. As a result, they began to collaborate on sharing video content. Had this collaborative opportunity not existed, each may have had the technical capability to share video content, but would have been less likely to do so.

The WARN pilot demonstrated a diverse set of broadband applications including helicopter video, traffic management support, bomb squad support, and fingerprint distribution. Users on the WARN system found these applications to be useful, and as they became more accustomed to the network, the demand for new applications continued to grow. The applications provided seamless interoperability among all WARN users.

The Growing Demand for Public Safety Broadband

Just as consumers are looking for other mobile services and features, such as data and video imagery, there is a growing interest in public safety operated broadband networks across the country to augment their current capabilities. The District and the local governments in the Metropolitan Washington Area are working to implement such a solution for the NCR – extending the capabilities of WARN into the urban and suburban areas outside of the District. This region filed a waiver from current 700 MHz FCC Rules to allow for a regional, interoperable, and broadband wireless network.[46] This regional network, while not an expansion of WARN, will draw significantly on the lessons learned from the WARN pilot.

Spectrum Issues

The WARN pilot used spectrum in the 700 MHz band that is not currently authorized for broadband use in FCC Part 90 Rules.[47] Hence, the pilot needed an experimental license to transmit with broadband channels. This license is set to expire in mid 2007. Thus, a solution is still needed to enable permanent use of this band for broadband operations. Additionally, this band only allows federal government use as an end user in coordination with a state and/or local partner.[48]

Several spectrum issues become clear as a result of this WARN demonstration project. They include:

- Existing amounts of spectrum bandwidths may be insufficient for meeting the growing mobile, wide-area broadband demands of public safety; and
- The federal government does not have spectrum allocated specifically for dedicated mobile public safety-related broadband applications.

Amount of Spectrum. According to the District's experiences, it appears the amount of spectrum used by WARN (2.5 MHz) — under the experimental license and within the 700 MHz band — is insufficient for broadband public safety use.

With only 20 users on Inauguration Day, WARN was overloaded in the downtown area, bringing into question the adequacy of a single broadband channel for a city the size of the District. Though these users were expected to be super-users (meaning they should generate much more traffic than the average user), the capacity of the system to support all public safety

[46] Federal Communications Commission, Public Notice, *Public Safety and Homeland Security Bureau Seeks Comment on Request by National Capital Region for Waiver of Part 90 Rules to Allow Establishment of a 700 MHz Interoperable Broadband Data Network*, DA 06-1973 (September 29, 2006) at http://hraunfoss.fcc.gov/edocs_public/attachmatch/DA-06-1973A1.pdf (Waiver RFC). Subsequently, the FCC has approved the waiver request.

[47] FCC's Part 90 Rules, *supra* note 16, at Section 90.531.

[48] *Id*., at Section 2.103(b).

use in the District remains questionable. Over 3,800 District police officers, 1400 Fire and EMS personnel, and thousands of additional District and federal law enforcement personnel have data needs inside the District. Additionally, providing other emergency response services from fire suppression and emergency medical to emergency management could also place considerable demands on the network. Therefore, if the data needs of public safety expand far beyond the limited WARN deployment, and if these additional users have usage profiles similar to those using WARN, the required bandwidth could be substantially more than a single broadband channel can accommodate.

The use of video presented the most significant demand to WARN. OCTO made changes to user profiles after the 2005 Inauguration to prevent excessive bandwidth use by individual users. These changes could degrade the frame rate to the extent that motion representation becomes inadequate. However, despite these changes, subsequent major events resulted in as much or more use with fewer than 200 users.

Furthermore, emerging applications are likely to become available to public safety in the near future and place significant additional demands on data networks. Few would have predicted the wide-scale use of the Internet today as compared to ten years ago and few can predict the capabilities that may be available to public safety in the next five to ten years. Also, other broadband applications such as three-dimensional GIS and high resolution image sharing were used sparingly over WARN, but interest in these applications is increasing. Likewise, smarter technologies are being developed that deliver better applications in more spectrally efficient ways.

The DTV Act directs the FCC to take all steps necessary to require, by February 18, 2009, that full-power television stations stop analog broadcasting, and that Class A stations, whether broadcasting in analog or digital format, and full-power television stations broadcasting in digital format, conduct such broadcasting on channels 2 to 36 and 38 to 51.[49] This enables channels 52 to 62 and 65 to 67 to be auctioned, and channels 63, 64, 68, and 69 (i.e., the 24 MHz at the 700 MHz band) to be used for public-safety purposes.

Federal Broadband Spectrum. By agreement, some federal agencies were participating users of WARN, however, they cannot presently be licensed to operate in the 24 MHz public safety 700 MHz band that is expected to support broadband.[50]

The federal government does not have spectrum identified specifically for mobile public safety-related broadband applications, whereas non-federal public safety services do at 4.9 GHz and the potential exists for such capabilities in the public safety 700 MHz band. If federal agencies identify a need for broadband access, they have, for example, a number of options in the near future: utilizing commercial services; partnering with state or local governments in building and operating broadband private networks; or identifying spectrum for broadband use within the current federally-allocated bands based on specifically identified requirements.

[49] DTV Act, *supra* note 23, at Section 3002.

[50] 47 C.F.R. §2.103(a). However, federal government entities are authorized to use channels in the 700 MHz band subject to conditions and agreements in place with non-federal public safety agencies. See 47 C.F.R. §2.103(b).

For example, satellite services may be a solution only for command vehicles and other specialized units due to the cost and size of Very Small Aperture Terminals (VSAT) applications with large bandwidth. Satellite services are also frequently unavailable in urban or natural canyons or inside buildings. For reasons mentioned previously, federal agencies should appropriately consider the use of satellite and other commercial services based upon such issues as reliability, coverage, security, and network management.

If spectrum were to be identified for federal broadband use from the federally-allocated bands, it should be near or co-located with state, local, and tribal spectrum so as to easily tie the networks operationally together and build a greater, national, economy-of-scale network that would foster interoperability. Furthermore, the band should contain enough spectrum to accommodate broadband channel widths.

Coverage

Achieving adequate broadband coverage is perhaps the biggest challenge to implementing WARN, as indicated by the need to add two sites to the WARN system. The inherent lower power of broadband technologies delivered significant advantages, such as smaller base station equipment and handheld devices, but it also resulted in less in-building coverage when compared to LMR. Adding sites was an excellent solution to the coverage dilemma, but they were costly to implement and operate. The challenge is now to match broadband coverage to LMR coverage, allowing public safety to better leverage existing infrastructure, saving capital and operating dollars. The District expects that technologies are on the horizon that can help make up for broadband coverage deficiencies in the long-term, providing excellent coverage even in the dense granite structures of downtown Washington, D.C. Meanwhile, however, the District intends to enhance coverage by adding up to double the number of existing sites to the WARN network. Using NCR's RWBN, sufficient outdoor coverage is expected in the first half of 2007, with citywide indoor coverage expected by the end of that year.

Devices

Additional types of subscriber devices would help meet public safety needs. Rugged computing devices are sufficient, and the PC cards have proven to be sufficiently rugged, with the exception of the antenna. The PC cards and PADs have a small paddle antenna that can pop off, break, or become an obstruction to the user. Additionally, the cards are custom-made at a cost of $600 each and they do not allow roaming on commercial networks. Although antenna reliability issues were not prevalent in user feedback, using integrated or fixed antenna technology in the next generation of laptops is a viable solution to this issue.

Technologies that can support all user needs would be ideal. For example, OCTO could not satisfy requests to provide WARN connections for PDA devices without significant sacrifices of battery power and usefulness of the device due to bulk. Therefore, users requiring a handheld device with WARN access could not be supported. Furthermore, integrated modems with AVL were also not available and could not be supported. With commercial technologies, however, WARN users would have had the opportunity to acquire the necessary solutions and more. For example, voice and data integrated devices in a phone format allow users to read email, use Web sites, and access other information. These features may be attractive for some users who desire limited capabilities in a small, handheld form. Additionally, some commercial handheld devices are built to withstand shock and moisture. This selection of devices would have enabled OCTO to better meet the needs of its user community. Ultimately, the commercial technologies would offer more choices for public safety and address a wider variety of needs.

FUTURE TRENDS AND QUESTIONS

The initial data collected from the WARN pilot program suggested that a strategy was needed to deal with the long-term trends in technology for wider channels, more data, and higher data throughput. Based on verbal feedback from the user community to the District, it is believed that more data will be required over time (video, biometrics, imagery), requiring an increase in bits per second (bps) throughput to handle the demand. This increase will demand reliable broadband solutions for the entire public safety user community. Leveraging innovation and competition in commercial markets, while providing sufficient economy of scale for customization for public safety, appears critical for maintaining the needed capacity to address these demands. Planning is critical to ensure that a blueprint for regional or national wireless broadband solutions is available when the user community needs them.

RECOMMENDATIONS

The recommendations that stem from this demonstration project include guidance for technological improvements as well as additional short and long-term planning and sharing required among and between government agencies for broadband services.

Identify Broadband Requirements

Agencies that have the need for broadband applications should identify their requirements in their strategic spectrum plans submitted to NTIA. State and local public safety entities should similarly plan and identify their broadband requirements.[51] Without identifying the requirements, a viable spectrum plan cannot be developed. In order to provide a comprehensive view on what spectrum and technical solutions may satisfy agency requirements, agencies should consider the following in their spectrum needs planning:

- **Throughput and tolerance:** The throughput of the applications and application tolerance of deviation (e.g., streaming media versus transmission of file) that are or will become mission critical.
- **Latency:** The latency tolerance of the applications, i.e., does the application need to hear back within a short time frame or will excess latency cause some degraded quality of service?
- **Device requirements (e.g., small PDA, embedded in notebook, PC card):** Some critical differentiators include requirements for lightweight, handheld solutions. This

[51] One of the recommendations of the President's Spectrum Policy Initiative is to encourage state and local spectrum planning. This planning process will provide a mechanism for state and local entities to identify and plan for their future broadband needs. *See* Report 2, *supra* note 7, at 26.

will become a driving factor on the coverage footprint, size of the device, battery life, and the usefulness that the public has become accustomed to with today's commercial devices. If this is not a factor, many more options open up.

- **Coverage requirements and spectrum options:** If the public safety mission for broadband includes areas within foliage, inside buildings, and in urban or natural canyons, then satellite communications become difficult. On the other hand, building broadband networks in remote areas is expensive. At the other extreme, on-scene communications solutions at unlicensed or 4.9 GHz may provide the needed capacity if the coverage expectations can be met. These may be the main differentiating factors as to what frequency and architecture are needed to address the requirement.
- **Required scalability:** Agencies will need to estimate demand over time to ensure growing user communities and usage will be accommodated. Projections for the growth in data needs are critical in understanding the needed pace for technological advancements of any data solution. Other solutions, such as cell splitting, may be an alternative solution to address capacity, especially for same-frequency-reuse technologies. However, it is critical to understand the demand curve for individual applications and users, and in aggregate, to ensure the spectrum and infrastructure solutions can stay ahead of the curve.
- **Required reliability of the solution:** It is vital to consider the degree to which the data solutions are mission critical and their impact if lost. Important factors for reliability include the power, backhaul, and other redundant components. Additionally, the type of priority access may become an important consideration.
- **Commercial services:** Agencies may consider the trade-offs of using commercial services and networks instead of private networks in satisfying the identified broadband requirements.

Begin Planning To Share Spectrum Resources

Some may debate the need of public safety broadband capacity. Others may also question the need for public safety operated networks. In any case, these are important issues that will require years of planning to achieve regional or nationwide solutions. In the event that private broadband networks are needed in the coming years, planning must begin to address the need. Regardless of method, public safety must share spectrum at some level in order to accommodate its broadband needs – either with the public or with other public safety agencies or governments. WARN demonstrated the feasibility of spectrum sharing among governments, but considerable efforts are required to make such a solution permanent.

Additionally, it is impractical for individual jurisdictions to go it alone. Both high deployment and operational costs will result. The more entities that work together to deploy similar solutions, the more built-in interoperability will inherently exist. Additionally, regional efforts can share significant costs in the build-out and operations phase. Regional deployments and systems could also reduce the complexity of roaming arrangements.

Partnerships between federal agencies, regions, states, and their local jurisdictions are an important component of an effective public safety broadband solution. Partnerships among federal, state and local public safety entities, as demonstrated by WARN, have shown to improve coordination and interoperability between federal and non-federal agencies. Interoperability is needed at the borders between states and regions, and therefore, a more global approach to spectrum and technology use is required to address these areas. It is also impractical to set up agreements among every local or county jurisdiction in the nation. State, regional, and national partnerships are more appropriate.

Leverage Standardized Economies of Scale

The lessons learned from the District are to choose standard solutions that are also affordable due to mass commercialization. The WARN pilot provided for lower-cost network and subscriber devices when compared to LMR systems, but subscriber devices were considerably more expensive than commercial cellular devices. Further, the subscriber device options in the commercial markets provide tremendous choices that will benefit public safety as compared to the limited choices offered to WARN users.

These same commercial technologies decrease year-by-year in cost versus an increase in the LMR marketplace. Therefore, over time, the cost disparity between commercial broadband and other solutions will grow even larger. Public safety should leverage commercial wide-area solutions in order to continue to harness the economies of scale. If demand is as significant as presented by WARN, it may also be important to tap the research and development efforts and solutions that deliver exponential growth in capacity and features of the commercial markets.

Additionally, these solutions may inherently deliver built-in roaming solutions. As a result of mass-scale standard technology use, vendors will find it easier to deliver solutions that can support the frequencies of public safety and commercial markets. This will enable roaming on to commercial networks from private public safety networks using inexpensive subscriber devices.

The benefits of the use of standard solutions can also facilitate national interoperability. Such mass-scale solutions are already delivering national commercial networks and can be adopted to address seamless interoperability among private networks. If state and local public safety entities deploy different broadband solutions across the country, then it is likely that federal agencies would have to buy multiple devices (and routers to support seamless operations) to have coverage on each operating network. Whether the federal solution becomes a private one hosted by regional state and local public safety agencies, or a federally-owned network, the devices that are purchased should be compatible with existing nationwide commercial networks. Initially, any private solution will provide an island of coverage. Compatibility with commercial services could then also deliver more cost-effective national solutions to accommodate federal and regional needs through economies of scale.

Improve Buying Power and Public Safety Capabilities

A significant limitation for deploying this type of broadband solution is the reduction in coverage compared to a LMR system operating on the same frequency band. Agencies will desire network capacity and the ability to support more broadband applications. However, their ability to deploy more sites to address the limited coverage in comparison to 700 MHz or 800

MHz LMR deployments could be problematic. In order for broadband solutions to become viable, they may need to deliver coverage on par with LMR networks. This would allow public safety to fully leverage existing assets such as sites, generators, and backhaul.

Several technologies are on the horizon that could potentially improve coverage and investments in infrastructure, and subscriber devices are needed to bring these technologies to the marketplace. Smart antennas, for one, focus signals where needed and away from areas where they would cause interference. Other techniques such as transmit diversity, whereby the same signal is transmitted from two antennas and at two different points in time, may also deliver improvements in range. More mobile power may also deliver additional range, but at the expense of reduced portability.

A focused effort around broadband solutions will help to energize a public safety broadband marketplace and result in a lower cost, yet customized solution for agencies nationwide.

Consider Commercial Services Where Appropriate

As discussed previously, it was the District's decision not to use commercial services for a broadband network because user requirements (reliability, coverage, security, and network management) could not be met. However, in some areas, commercial services may be the only solution in the near term for affordable broadband services. Should commercial services be used, public safety agencies will need to deal with issues like coverage, priority service, redundancy, reliability, and other features (e.g., streaming video, access to GPS information, etc) to ensure that they can perform their missions. Public safety agencies are encouraged to appropriately use commercial services for broadband applications should their requirements dictate.

SUMMARY

WARN demonstrated a critical value in supporting federal and non-federal agencies as they work towards a spectrum sharing solution to meet the increasing complexity of public safety's wireless broadband communication needs in the coming decades. In these times of heightened awareness and security, public safety agencies are asked to provide more effective vigilance, response, and recovery efforts for its citizens. The WARN pilot demonstrated a new way to approach this demand.

Specifically based upon this pilot, the following observations and recommendations were identified:

Observations	*Recommendations*
Spectrum Planning	
• WARN demonstrated that in-depth spectrum planning and coordination are required to satisfy emerging broadband requirements. • WARN illustrated a growing need for broadband capabilities within the District.	• Federal agencies should clearly identify all broadband requirements in their agency strategic spectrum plans submitted to NTIA. • State and local public safety entities should develop spectrum plans that address their emerging broadband requirements.
Spectrum Use	
• WARN demonstrated that the availability of broadband leads to the realization of broadband potential and the creative identification of new applications. • According to the District's experiences, it appears the amount of spectrum used by WARN (2.5 MHz) under the experimental license may be insufficient for public safety broadband use.	• The FCC should conclude their revision of the current 700 MHz band plan to provide the capability for public safety entities to deploy broadband services.
Spectrum Sharing	
• The WARN pilot showed that partnerships that share spectrum resources between all levels of government greatly increase interoperable communications. • The District discovered during the WARN pilot that spectrum and communications infrastructure sharing tends to provide operational and cost-effective solutions.	• Broadband partnerships should be considered by the public safety community to include all levels of government.
Feasibility of Commercial Services	
• The District analyzed the use of commercial services and determined that commercial networks did not meet the requirements of WARN. However, they are available and may be appropriate for non-mission-critical uses if reliability, throughput, coverage, security, and network management issues are addressed.	• Public safety agencies should use commercial broadband services, where appropriate, if they can satisfy their broadband requirements.

This page intentionally blank

APPENDIX A

GLOSSARY

1xRTT	A version of CDMA2000 that utilizes a pair of 1.25 MHz radio channels. 1xRTT (Radio Transmission Technology) offers high-speed data services and voice capability and is more efficient due to its use of a pilot signal and more channels between fixed stations and mobile users.
4.9 GHz	The frequency band 4940-4990 MHz designated by the FCC for fixed and mobile wireless services and for use in support of public safety. The allocation of this band for public safety provided public safety users with additional spectrum to support new broadband applications.
700 MHz	The frequency band 764-776 and 794-806 MHz designated by the FCC for general use and interoperability narrowband channels, narrowband low power channels and wideband general use channels for public safety.
800 MHz	The frequency band designated by the FCC for public safety use in the 806-869 MHz range. This band is currently in a re-banding process to alleviate the commercial/public safety interference issues.
ALMRS	Alaska Land Mobile Radio System is the shared and interoperable statewide public safety telecommunications system used by state, local and federal first responders and public safety agencies in Alaska.
AVL	Automatic Vehicle Location is a technology that monitors vehicles in real-time and conveys navigational or operational data to the driver or monitoring center.
CDMA	Code-Division Multiple Access is a technology for digital transmissions of radio signals between a wireless device and a radio base station.
DC FEMS	District Fire Emergency Medical Services is the agency that provides emergency support services in the District.
DCWAN-VLAN	District Wide Area Network-Virtual Local Area Network is the telecommunications network providing coverage to the government agencies in the District.
DHS	U.S. Department of Homeland Security develops and coordinates a comprehensive national strategy to strengthen and protect against terrorist threats or attacks in the United States.
"Direct" Communications	Short-range, line-of-sight communications directly from one radio to another without benefit of a repeater to extend the range of the transmitted communication.
Downlink	The downlink (otherwise known as forward or download) path is the path from the base station to the wireless subscriber device (e.g., computer modem).

EVDO	Evolution Data Optimized, EVDO is a standard for broadband wireless technology. Initially developed by Qualcomm, EVDO operates on a CDMA signal with a higher data rate capability that 1xRTT. It has been adopted by many CDMA mobile phone service providers as an "always-on" on wireless connections, similar to DSL.
FCC	The Federal Communications Commission was established to regulate all non-federal government use of radio spectrum, interstate communications, and international communications that begin or end in the United States.
IPSec	Internet Protocol Security is a framework of standards for secure communications over the Internet.
IT	Information Technology is the branch of engineering that deals with the use of computers and telecommunications to gather, store, and transmit information.
LMR	Land Mobile Radio is a mobile service between fixed base stations and stations capable of surface movement within geographical limits.
MACC	A Multi-Agency Communication Center is a consolidated emergency response point in which agencies come together in a central location to coordinate responses to emergency situations.
MHz	Megahertz is a unit of frequency equal to one million cycles per second.
MoA	A Memorandum of Agreement sets forth basic principles and guidelines under which two parties will work together on a given issue or to meet common needs/goals.
MoU	A Memorandum of Understanding sets forth basic principles and guidelines under which two parties will work together on a given issue or to meet common needs/goals.
NCR	National Capital Region is the geographical area in which WARN is deployed, covered the District of Columbia and surrounding counties and cities in Maryland Virginia.
NTIA	National Telecommunications and Information Administration is responsible for telecommunications and information policy in the United States, as well as managing the federal use of radio spectrum.
OCTO	The Office of the Chief Technology Officer. The District's Agency responsible for the development, operations and maintenance of the technology infrastructure.
OSM	Office of Spectrum Management is responsible for managing the federal government's utilization of the radio frequency spectrum and establishing policy and plans for spectrum regulation.
PAD	A Portable Access Device is a mobile data access unit.
PCMCIA	Personal Computer Memory Card International Association is a non-profit trade association and standards body consisting of around 500 companies that has developed a standard for small, credit card-sized devices, called PC cards, that are used in notebook computers.
PCMIA	A Personal Computer Manufacturer Interface Adapter (PC card) is used to connect a mobile phone to a laptop enabling the user to

	expand communication abilities while on the move. When a user is connected via the PCMIA he or she can send and receive data and access the Internet.
PDA	Personal Digital Assistants are handheld devices, originally used for personal organizers, but are now are used for transmitting data, video and audio recording, accessing the Internet, among other high technology functions.
SAFECOM	SAFECOM Program is the communications program of the DHS providing research, testing, and evaluation to better address the needs of emergency responders.
Repeater	A repeater is a high powered radio generally co-located with a tower to amplify and extend the geographic coverage area of portable and mobile radios.
RWBN	Regional Wireless Broadband Network is a mobile communications system created to transmit broadband wireless voice and data communications in a specified geographic region.
"Talk-around" Communications	Short-range (a few miles or less), communications directly from one radio to another without the benefit of a repeater to extend the range of the transmitted communication. Generally limited to a few miles of effective coverage.
Transceiver	A transceiver is a device that contains a combined transmitter and receiver.
Uplink	The uplink is the path from the subscriber device to the base station or other system wireless access point and is also known as the reverse path or reverse link
USPP	The United States Park Police is the security police force jurisdiction in all National Park Service areas and other government lands. It is the oldest uniformed federal law enforcement agency in the United States.
USSS	United States Secret Service is responsible for protecting our nation's leaders, visiting world leaders, and special national security events.
VSATs	Very Small Aperture Terminal is a 2-way satellite ground station with a dish antenna that is smaller than 3 meters that serves home and business users and handles data, voice, and video signals.
WARN	The Wireless Accelerated Responder Network was the pilot network in the District providing wireless broadband speeds to law enforcement and fire personnel while deployed in the field.
Wireless Broadband	A technology aimed at providing wireless access to data networks, with high data rates. In the public safety sector, wireless broadband applications, such as high-speed digital technologies and wireless local area networks (LANs) have been utilized for incident management and dispatch and public safety vehicle operations.

WLG	Working Level Groups established by NTIA to assist in the implementation of the recommendation of the President's Spectrum Reform Initiative.
WMATA	Washington Metropolitan Area Transit Authority is a non-federal tri-jurisdictional agency authorized by Congress and funded by the District, Virginia, and Maryland that operates transit services in the Washington D.C. Metropolitan area.
WMO	Wireless Management Office is a division of the DHS that ensures the wireless needs of the Department are met.

APPENDIX B

SAMPLE MEMORANDUM OF UNDERSTANDING (MoU)

MEMORANDUM OF UNDERSTANDING
BETWEEN THE
OFFICE OF THE CHIEF TECHNOLOGY OFFICER,
[GOVERNMENT OF THE DISTRICT OF COLUMBIA]
AND AGENCY/DEPARTMENT

I. INTRODUCTION

This Memorandum of Understanding ("MOU") is made this ______ day of ___________ 2005, by and between the Government of the District of Columbia Office of the Chief Technology Officer ("OCTO") and the (Agency/Department), ("XXX") concerning providing XXX access to the Pilot Wireless Broadband Network operated by OCTO, otherwise called the Wireless Accelerated Responder Network (WARN).

WHEREAS, OCTO will provide access, usage and support of the WARN network, and

WHEREAS, OCTO has identified the objectives of the WARN network during this pilot program as to:

- Support the NCR Public Safety organizations in the protection of the city
- Demonstrate wireless broadband Public Safety applications
- Provide the national Public Safety community with lessons learned from the pilot program
- Leverage the network and OCTO's interoperability studies to support a Congressionally mandated Federal Communications Commission (FCC) and Department of Homeland Security (XXX) study for Public Safety broadband needs, and

WHEREAS, XXX desires to access and test the WARN network for XXX operations, and

WHEREAS, both parties desire to expedite connection of XXX to the WARN network,

NOW THEREFORE, the parties agree to enter into this MOU to provide XXX access to use and test the pilot WARN network.

II. OBLIGATIONS OF OCTO

OCTO will:

- Provide access to the pilot wireless broadband network.
- Provide a network device which may be a PC card and/or a Portable Access Device (PAD).

- Use its best efforts to provide system reliability and availability 24 hours a day, 7 days a week (24/7).
- Resolve network outages as quickly as possible as defined in Exhibit A.
- Provide wireless data transport service to XXX.
- Provide an administrative and technical point of contact for XXX. Provide Tier 1 support. Tier 1 support is defined as 24/7 telephone and email support. Tier 2 will be provided by OCTO and includes hardware and software support for the hardware and software as defined in Exhibit B.
- Conduct and manage periodic user feedback sessions, surveys, and/or drills.
- Provide training to WARN users, as requested.

III. OBLIGATIONS OF XXX

XXX will:

- Adhere to and enforce the "Customer Operations Usage Policy" attached hereto as Exhibit D.
- Sign OCTO Security's "Network Interconnection Agreement" attached as Exhibit E.
- Provide an administrative and technical point of contact for OCTO.
- Use the WARN network only within the borders of the District of Columbia.
- Restore the performance of its computing device within twenty-four (24) hours or by the next business day in the event that such device is malfunctioning.
- Obtain the approval of OCTO before installing or downloading any software as specified in Exhibit C. Such approval shall not be unreasonably withheld.
- Not modify any hardware or software that would increase transmit power of the network device (i.e. PC card and/or a Portable Access Device (PAD)) as this event could jeopardize OCTO's FCC Experimental Radio Station Construction Permit and License, file number 0013-EX-PL-2004.
- Not copy or distribute network device installation software.
- Immediately notify OCTO if hardware or software connected to WARN is lost or stolen.
- Immediately notify the help desk of any problem that interrupts service, such as network outages, hardware and/or software malfunctions.
- Refrain from creating any network connection bridge between the OCTO network device and another network connection.
- Adhere to the "Server Hardening Policy" attached as Exhibit F when installing servers in OCTO Security's hosting facilities.
- Participate in periodic user feedback sessions, surveys, and/or drills.

IV. USAGE

XXX warrants that each network device, i.e. PC card and/or PAD, issued to it by OCTO will be used as much as operationally required by XXX to provide feedback on network effectiveness to OCTO for the purposes of the pilot network evaluation.

V. DISCLAIMERS AND RESERVATIONS

- OCTO makes no guarantees that service will be available at any given time or everywhere within the boundaries of the District of Columbia.
- OCTO reserves the right to rate-cap available bandwidth to ensure that all users can participate during the pilot period.
- OCTO reserves the right to determine if the deployment of any application may be deemed a security risk and/or may degrade network performance as defined in Exhibit C. If so determined, OCTO may discontinue service to those users with access to the application.
- OCTO reserves the right to publish any data collected during the pilot period, including, but not limited to, individual usage statistics, network performance information, and/or reports on deliverables required by OCTO's National Institute of Justice ("NIJ") funded cooperative agreements ("grants"). The data presented to NIJ will not include personal identification of users, identification of user organizations, or details of user operations. The data will be presented in a manner that prevents reviewers of the data from identifying individual users.
- XXX is solely liable for the cost of replacement or repair of any network device provided by OCTO.
- OCTO disclaims all liability for any lost productivity, personal injury or loss of life, or loss/damage to property that XXX may incur in connection with its use of WARN.
- XXX is wholly liable for the reliability and availability of its software and hardware systems and the security of the data transported over the WARN network.

VI. FEES

1. Fees OCTO incurred significant cost to develop the WARN network and reserves the right to charge XXX fees for its use of the network, subject to the waiver provided in Section V.2. OCTO will charge no fees until the amount of the fees has been determined by agreement of the parties and set forth in an amendment to this MOU. If XXX does not agree to pay fees that are reasonable in the judgment of OCTO, OCTO may choose to terminate this agreement upon seven (7) days' written notice.

2. Initial waiver
OCTO will waive all fees during the initial term, until August 31, 2006, of this MOU. Should circumstances change prior to that time, the provisions of section V.1 will apply.

VII. EFFECTIVE DATE

This agreement is effective on the date of the last signature.

VIII. TERM

The Term of this Memorandum of Understanding shall be until August 31, 2006. This term shall be extended for one (1) year periods unless terminated by either party upon thirty (30) days' written notice.

IX. MODIFICATION

This agreement may be modified at any time by agreement of the parties.

X. TERMINATION

This agreement may be terminated by either party upon 30 days' written notice. Notice will be sent to the administrative point of contact.

XI. SIGNATORIES

XXX Agency/Department	Office of the Chief Technology Officer
By: ______________________________	By: ______________________________
Name:	Name: Suzanne Peck
Title: _____________________________	Title: Chief Technology Officer
Date: _____________________________	Date: ___________________________

Exhibit A – Service Level Agreement

SECTION	SERVICE	SERVICE LEVELS		
1.0	**Telephone Service**			
	Hours of Operation	24 hours a day; 7 days a week		
	Time to Answer	< 30 seconds		
2.0	**Response Time**			
	Response Time to E-Mail	The Help Desk will respond within four hours via email response unless additional details are required. Then, Help Desk will contact the customer via phone.		
	Response Time (onsite) to Hardware	The Help Desk will dispatch a resource to respond onsite by Next Business Day.		
3.0	**Help Desk Technical Support**			
	Telephone First Call Resolution Rate	75%	**Definition** – The percentage of calls that are resolved on the first contact; that is, while the user is still on the phone.	
	Telephone Extended Call Resolution Rate	90%	**Definition** – The percentage of calls that are resolved within the first 72 hours after the call is logged. The extended call resolution rate is an extension to the First Call Resolution.	
	Priority	**Priority**	**Definition**	
		High	Network connectivity down; system failure;	
		Standard	Routine problems; minimal impact on job functions; application usage; "how-to" assistance	
	Telephone Resolution Times	**Priority**	**Ticket Type**	**Resolution Time***
		All	GDC – OCTO Software – First Call	First Call
		All	GDC – OCTO Software – Extended Call	72 hours
		Priority	**Ticket Types**	**Resolution Time***
		Standard	Network Access	Next Business Day
		All	GDC – OCTO Hardware	Next Business Day
		* Resolution time is defined as the period of time between the initial ticket creation (open date/time) and documented problem resolution (closed date).		

Exhibit B – Hardware and Software

OCTO will provide, manage, and support the following hardware and software. Any hardware and/or software not listed below but is used on the WARN network is the sole responsibility of XXX for maintenance, support and/or replacement.

Hardware

ID	Type	Quantity
1.	Flarion PC card Network Device	10
2.	Network Device Antenna Connector	10

Software

ID	Type	License Quantity
1.	Flarion Installation Drivers	10

Exhibit C – Software Application Implementation

OCTO will work with XXX and document the requirements needed to ensure accessibility to the required applications that will be used over the WARN network. A new application will not be deployed if it degrades network performance. The requirement gathering will determine the necessary ports that need to be opened, the expected throughput needed, the configuration of the device, and what security measures are implemented.

It will be required by this MOU that XXX work with OCTO Security to implement new software applications. The WARN network is protected by several firewalls which block all ports except for the ports needed for existing applications or ports requested specifically by XXX and approved by OCTO Security. OCTO reserves the right to prevent the deployment of any application that may be deemed as a security risk and/or may degrade network performance.

Exhibit D – Server Hardening Policy

Servers are depended upon to deliver data in a secure, reliable fashion. There must be assurance that data integrity, confidentiality and availability will be maintained. One of the required steps to attain this assurance is to ensure that the servers are installed and maintained in a manner that prevents unauthorized access, unauthorized use, and disruptions in service. The purpose of the Server Hardening Policy is to describe the requirements for installing a new server in a secure fashion and maintaining the security integrity of the server and application software.

Policy

- A server must not be connected to the WARN network until it is in an accredited secure state and the network connection is approved by OCTO.
- The Server Hardening Procedure provides the detailed information required to harden a server and must be implemented for OCTO's accreditation. Some of the general steps included in the Server Hardening Procedure include:
  - Installing the operating system from an OCTO approved source
  - Applying vendor supplied patches
  - Removing unnecessary software, system services, and drivers
  - Setting security parameters, file protections and enabling audit logging
  - Disabling or changing the password of default accounts
- OCTO will monitor security issues, both internal to OCTO and externally, and will manage the release of security patches on behalf of XXX.
- OCTO will test security patches against OCTO core resources before release where practical.
- OCTO may make hardware resources available for testing security patches in the case of special applications.
- Security patches must be implemented within the specified timeframe of notification from OCTO.

This page intentionally blank

APPENDIX C

TECHNICAL INFORMATION

This Appendix provides high-level, technical details on the aspects of WARN's architecture for those that are interested.

CONFIGURATION

The Radio Access Router on the network was based on a Compact Peripheral Component Interconnect (cPCI) standard compliant chassis platform comprised of a number of hardware and software elements. The Access Router included the Baseband Unit (BBU), which performed the Flash-OFDM waveform processing, the RF system consisting of a Receiver Unit (RXU) and Transmit Unit (TXU) pair, the Master Control Unit (MCU), the Backhaul Unit (BHU), Power Conditioning Unit (PCU), and the Alarm Interface Unit (AIU). The Radio Access Router provided network access control, authentication, routing and mobility management functions, as well as backhaul connectivity interconnecting the Access Router with the rest of the Flash-OFDM system. Configuration options of a radio router are shown in Figure 11:

Subsystem Non Redundant Configuration	One Carrier Omni	One Carrier Simulcast	One Carrier 3 Sectors	Tx Diversity
BBU Rev 1	1	1	3	1 to 3
RFU Rev 1	1	1	3	1 to 3
MCU	1	1	1	1
Quad T1/E1	1	1	1	1
AIU	1	1	1	1
cPCI Chassis	1	1	1	1
20 Watt PA	1	1	3	3 to 6
LNA/Duplexer Filter	1	1	3	3
LNA/Rx Filter	1	1	3	3
Combiner/Splitter		1		

Figure 11: Section 6 RR Configurations

The Radio Router base station fits in a standard 19" rack for indoor applications and a two-bay cabinet for outdoor applications. The MCU and the BHU are rated for an extended temperature range (up to 65ºC), but are otherwise standard off-the-shelf cards. The BBU, TXU and RXU are proprietary custom circuit cards that generate and receive the Flash-OFDM waveform. The PCU was very similar to standard 24VDC cPCI power supply but outputs a non-standard 5.8VDC that was used by the BBU, TXU and RXUs. The AIU was also a circuit card that was custom developed by Flarion. It provided the alarm collection function for the base station. It also had a role in redundancy swap over of the MCU and BBUs. Some of the cards in the Access Router had options for redundancy and failover as Figure 12 shows.

Off-the-Shelf Cards	**Redundancy**
2 MCUs	2N
2 BHUs	2N
2 PCUs	2N
Custom Cards	
4 BBUs	N+1
3 TXUs	None
3 RXUs	None
2 AIUs	2N

Figure 12: Access Router Cards

BBU Description-Air Interface

The BBU was the baseband modem processor for a sector of the radio router base station (i.e., the air interface). It provided the link layer interface between the MCU (router) running IP protocols and the RF cards (RXU and TXU), which required analog baseband Flash-OFDM signals. Link, MAC, and physical (PHY) layer processing functions for the station are performed by the BBU. The telemetry and control functions for the RF cards were also performed by the BBU. The card's main components were two FPGAs, a DSP, a Power PC (PPC), PCI interface chip, and DAC and ADC.

The radio router supports N+1 BBU redundancy as an optional feature. In a radio router so equipped, the failure of a BBU would automatically be detected and the failover process initiated, where the redundant BBU would be electronically switched into that sector. Operation would then resume, although all active sessions would experience an interruption to service. The backup BBU could have been switched into any of the three sectors.

MCU Description – The Router

The router functions of the access router were implemented in the MCU board. The MCU was a Pentium III-based single board computer (SBC) in a 6U cPCI standard format. The unit was procured as a standard off-the-shelf computer with the main characteristics as follows:[52]

- CPU -Intel Pentium III, 800 MHz and higher
- L1 Cache I/D - 32K/32K
- L2 Cache - 512KB
- Memory Speed - 133 MHz
- Flash BIOS - Phoenix
- Local PCI Interface -1-66 MHz/64b; 1-33 MHz/32b
- Storage - Assembly options for Hard Disk or Flash Disk
- 10/100 Base-T Ethernet interfaces - 2 (in front panel)

[52] The list describes the characteristics and matching processing options of the unit.

- PMC1 and PMC2 I/O connectors - 2
- Serial Ports – 3

RF SUBSYSTEM DESCRIPTION

The RF part of the Flarion base station was defined as all the hardware between the digital section of the BBU and the antennas on the other end. Physically, all the hardware except for antennas and antenna cables resided in one 19” cabinet together with all other components of the radio router. The cabinet accommodated all the hardware needed for up to a 3-sector base station with receive and transmit diversity.

The major components of the RF subsystems were (see Figure 13):

1. A/D and D/A sections of BBU
2. TXU – Transmitter Unit
3. RXU – Receiver Unit
4. LNA/Duplexers
5. Power Amplifiers
6. Antennas

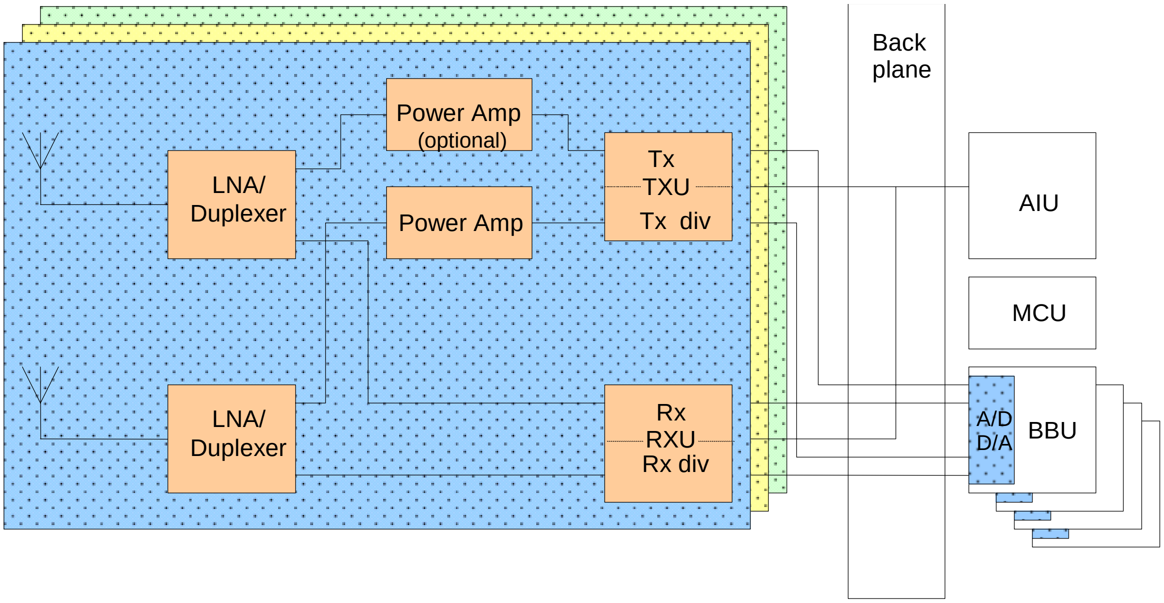

Figure 13: RF Subsystem High Level Block Diagram

A/D and D/A sections of BBU

A/D and D/A sections were located on a BBU cPCI card together with all the physical layer digital circuitry. They convert signals from/to digital and analog formats. There were two identical A/D and D/A sections (main and diversity) per BBU per antenna sector.

TXU and RXU

TXU and RXU are cPCI circuit cards that plugged into the cPCI backplane together with all other base station circuit cards. They provided up and down frequency conversion and filtering of the analog signals. TXU and RXU interface with BBUs on one end and with LNA/Duplexers and power amplifiers on the other end. There was one TXU and one RXU per sector, and up to three of each could have been accommodated in a cPCI chassis. Each TXU and RXU had two identical signal paths for diversity. The units contained self-diagnostic capabilities and switch matrices to allow switchover to a redundant BBU in case of a BBU failure

LNA/Duplexer

LNA/Duplexer was comprised of a depleting filter followed by a low noise amplifier. The duplexer was composed of two frequency filters joined together at a common port that connects to antenna cable. The transmitter filter provided frequency filtering of a signal from a Power Amplifier (PA) before it reached the antenna, and the receiver filter does the same between the antenna and the Low Noise Amplifier (LNA). The LNA was built into the same assembly as the duplexer, while the PA connected to the duplexer through cable. There was one LNA/Duplexer per antenna, so two were needed if diversity was used. However, since transmitter diversity was optional, the second assembly could only have a receiver filter instead of a full duplexer. Up to six LNA/Duplexers could have been accommodated in a cabinet for a 3-sector system with diversity.

Power Amplifier

The PA provided the final high power amplification for the transmitter. The standard PA was rated for 43 dBm (20 Watt) output, which provides approximately 41.3 dBm at the antenna connector after internal losses are accounted for. The radio router used PAs commonly used for existing cellular/PCS CDMA systems.

The PA interface to TXU at the input and to the transmitter port of LNA/Duplexer at the output. PA linearity, together with the transmit part of a duplexing filter and any optional filtering, further determined out-of-band emissions of the system. The PA also included forward/reflected power detectors and other alarm and diagnostic monitors.

RF Operating Characteristics

Operating characteristics include the following:

Signal Format:
MHz Frequency Division Duplex (FDD) (duplex separation is band dependent)
QPSK Transmit; QPSK, 16QAM Receive

Frequencies Supported:

1. 700 MHz: 30 MHz duplex separation
Receive: 777 MHz to 792 MHz
Transmit: 747 MHz to 762 MHz

2. SMR: 45 MHz duplex separation
Receive: 806 MHz to 821 MHz
Transmit: 851 MHz to 866 MHz

3. 800 MHz Cellular: 45 MHz duplex separation
Receive: 824 MHz to 849 MHz
Transmit: 869 MHz to 894 MHz

4. 1900 MHz PCS: 80 MHz duplex separation
Receive: 1850 MHz to 1910 MHz
Transmit: 1930 MHz to 1990 MHz

5. 2100 MHz UMTS: 190 MHz duplex separation
Receive: 1920 MHz to 1980 MHz
Transmit: 2110 MHz to 2170 MHz

6. 2300 MHz Korean: 70 MHz duplex separation
Receive: 2300 MHz to 2330 MHz
Transmit: 2370 MHz to 2400 MHz

Performance:

- Approximately 3 Mbps Peak Downlink (Receive) Burst Rate
- Approximately 900 kbps Aggregate Peak Uplink (Transmit) Burst Rate
- 4 dB composite RR Noise Figure, typical
- -117.7 dBm typical receiver sensitivity @ 50 kbps

Back-Haul Unit Description

The Back Haul Unit (BHU) featured 4 fully independent line protected T1/E1 Channel Service Unit/Data Service Unit (CSU/DSU) channels. Each channel supported full, fractional and 56K mode T1/E1 protocols. T1 speeds up to 1.544 Mbps and E1 speeds up to 2.048 Mbps are supported. The unit was procured as a standard off-the-shelf TI card with the following characteristics:

- Infineon DSCC4 PCI / 4 channel HDLC Controller
- Four independent Full Duplex T1 or E1 Channels with rear panel I/O
- Full CSU/DSU Line Protection
- Alive led to indicate micro functionality
- Channel blocking and 56K mode support
- Channel independent internal loopback test mode

- Channel independent Data and Clock Inversion modes
- Local, Line and Framer loopback modes

The four supported T1s on two BHUs provided a maximum of eight T1/E1 connections for the Radio Router base station. Any four of the eight T1/E1s could have been active at one time.

Power Control Unit Description

The Power Control Unit (PCU) was a DC/DC converter that provided power to the cards in the Access Router shelf. The PCU accepted an input of 21VDC to 28VDC, and output five voltages: +5.0V, +5.75V, +3.3V, +12V and –12V. Since a standard cPCI supply does not have a +5.75V output, a custom supply was required in the Access Router shelf. The analog circuitry within the BBU and the RFU required +5.75V.

Alarm Interface Unit Description

The Alarm Interface Unit (AIU) had a dual role in the radio router base station. It managed all hardware connections of the base station alarms and communicates alarm status to the MCU. It was also involved in the fail-over of the redundant BBU and the redundant MCU. The AIU handled, or was involved with, the following tasks:

- Fail-over facilitation
- Alarm monitor and user defined alarms
- Maintenance features
- Battery backup power for system management
- Base station clock synchronization and distribution
- System reset
- Customer defined functions
- Inventory and configuration

There are 2 AIU slots in the Access Router shelf. A single AIU card could have handled all of the alarming and fail-over requirements for the base station. The second AIU provided redundancy.

The software and hardware of the base station were able to function without a populated AIU slot. A base station without an AIU would not provide redundancy fail-over for the MCU or BBU and would not provide hardware connectivity for user specified external alarms. Platform management of internal alarms was handled by the MCU in a base station that had no AIU present.

APPENDIX D

WARN PERFORMANCE TESTING

TESTING METHODOLOGY

Drive tests were performed by the District with a laptop that included a Flash OFDM card. The antenna was located inside the vehicle. The antenna configuration corresponded to an additional propagation loss of 6 dB to 8 dB. The laptop ran the Flarion Mobile Diagnostic Monitor (FMDM) software. FMDM monitored performance parameters such as data rates and link states for each test session. Concurrently, FMDM collected geographic location data through a GPS receiver connected to the same laptop.

The laptop would receive IP traffic from the core network to evaluate the downlink performance and would transmit IP traffic to the core network to evaluate uplink performance using the Internet Performance (Iperf) application. The “ping” command ran repetitively to evaluate the network latency. Uplink and downlink tests were run on different laptops. Iperf was configured such that data streams were generated on a User Datagram Protocol (UDP), which is a means to broadcast messages over the network. UDP is the protocol used for streaming video.

FMDM collected data twice a second. Through post processing, the data collected by FMDM was aggregated into 400 meter grids. The value attached to each grid was of the median value for all the instances of the parameter collected in that grid.

TESTING RESULTS

Figure 14 represents the field strength received from the site that has the dominant pilot channel.

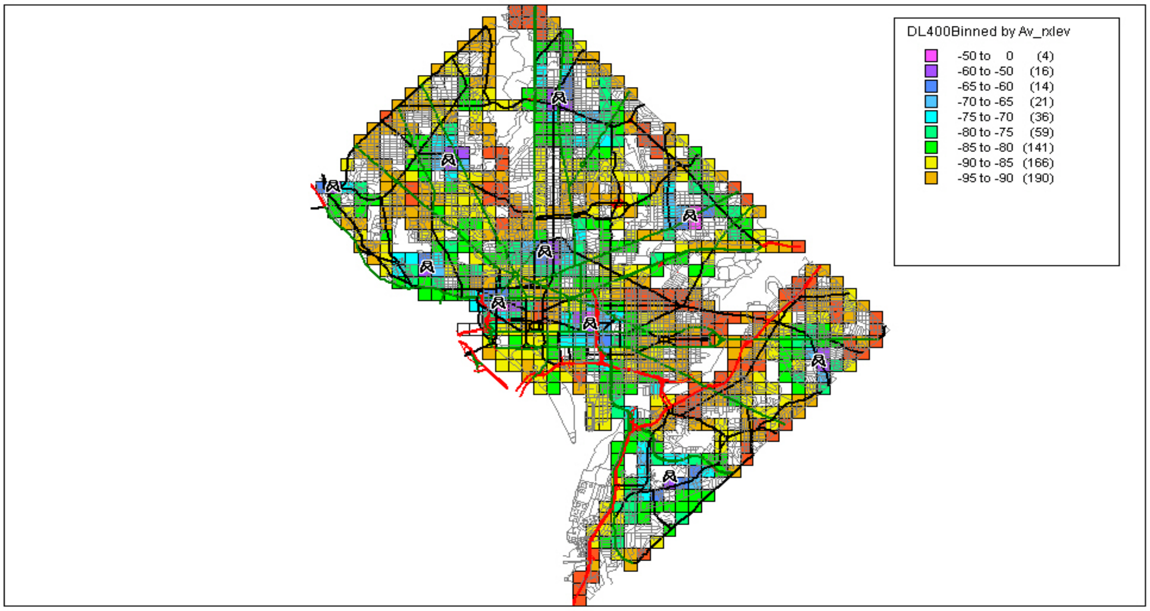

Figure 14: Measured Downlink Received Level

Several poor coverage areas appear on this map, although they did not exist for the voice network. The two main areas are the bed of the Anacostia River, and the Rock Creek Park (both of those areas are significant terrain depressions). Other smaller-coverage holes included the vicinity of the White House, a portion of Nebraska Avenue, and some other locations closer to the city boundaries.

More than the received field strength level, the received Signal-to-Noise Ratio (SNR) is the parameter that indicates the performance of the radio link, e.g., the achievable data rate. SNR was not satisfactory when the coverage was not sufficient, but also when the level of interference was too high. Figures 16 and 17 depict the downlink throughput measured throughout the city. The correlation between this map and the pilot field strength level map is high. Figure 18 shows the uplink throughput measured across the city. The technology allowed for peak rates of 2.7 Mbps for the downlink, and 900 kbps on the uplink. About 70% of the locations received more than 300 kbps in the downlink, and 60% of the locations were able to transmit 100 kbps on the uplink.

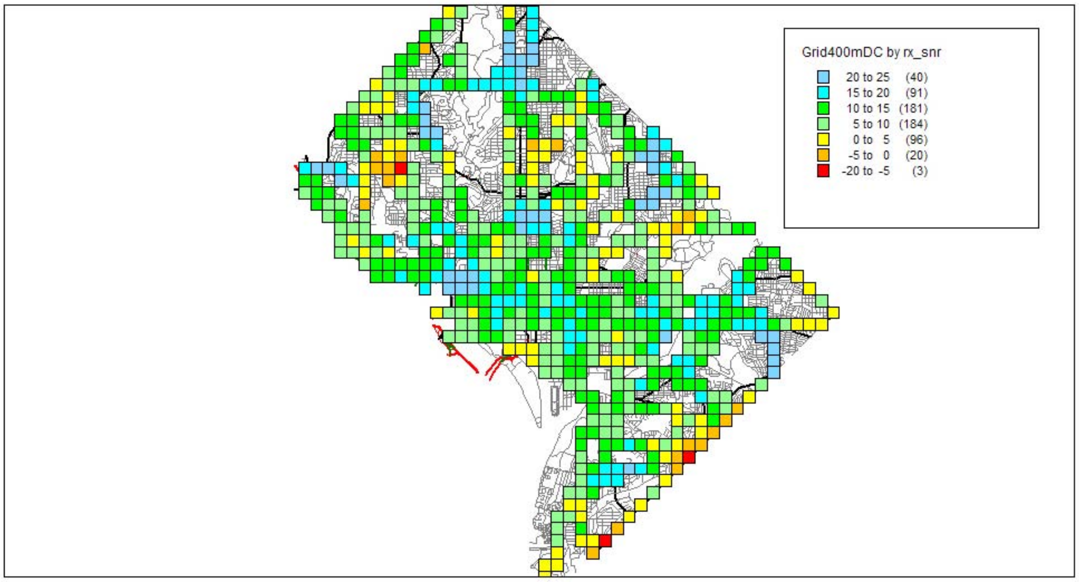

Figure 15: Downlink Signal to Noise Ratio (12 sites)

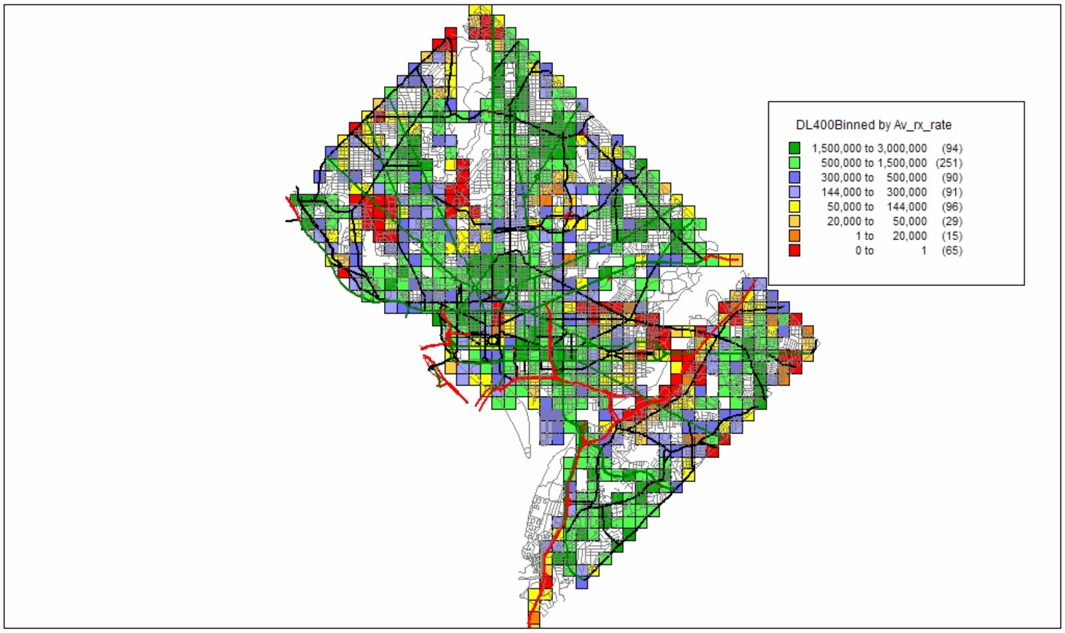

Figure 16: Downlink Received Data Rate (10 sites)

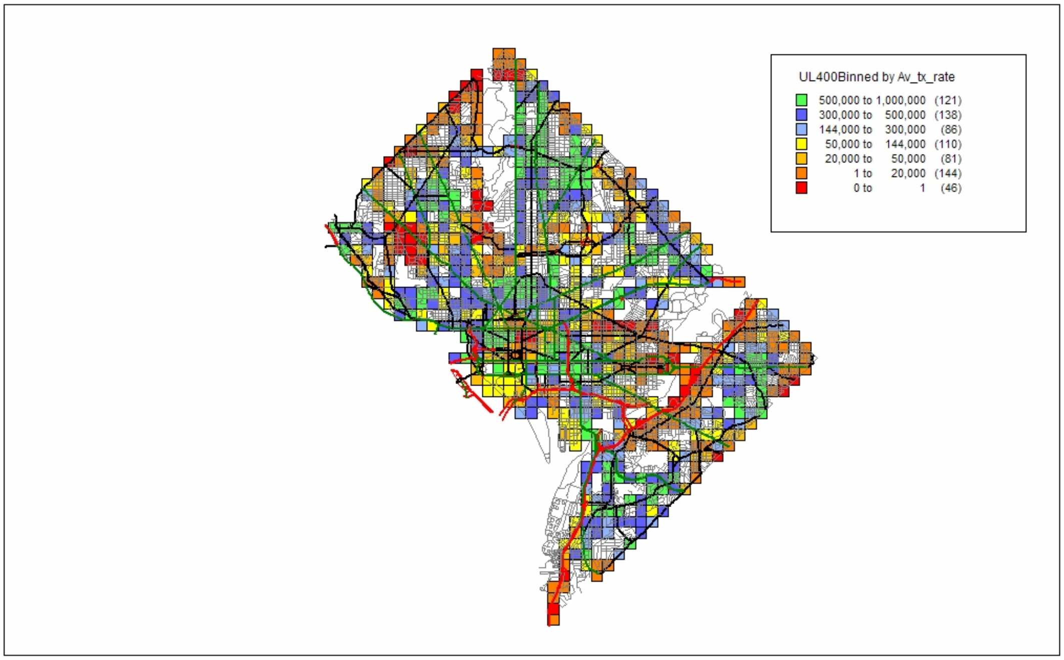

Figure 17: Uplink Transmitted Data Rate (10 sites)

Based on the results, the District began planning to improve the network coverage and capacity performance further by deploying two additional sites (and amend the experimental license accordingly):

- One site was in the vicinity of the White House. The White House area was at the edge of three cells. As a consequence, although for the most part the received level allowed for solid radio connectivity, the available throughput was limited to a range from 20 kbps to 50 kbps on the uplink, and to a range from 20 kbps to 120 kbps on the downlink. Because of obvious reasons, this area required a high network capacity. To support various local and federal agencies during the Presidential Inauguration, the District deployed a temporary single sectored site (based on a Special Temporary Authorization-STA). Following the success of the operations of this temporary site, the District deployed a 3-sector site in this area for the remaining duration of the experimental license.
- The other site was in the vicinity of the RFK stadium to alleviate the coverage issues along the Anacostia River.

Other key performance parameters are summarized in Figure 18.

Metric	Value
Packet delay (Median single user)	30 ms
Dropped pings	2.49%
Access Failure rate (> 15s)	1.75%
System Drop rate (Session Drop and Handover Drop > 2s)	0.203/100

Figure 18: WARN Performance Parameters

APPENDIX E

USER FEEDBACK

The District asked WARN users to complete monthly surveys regarding their satisfaction and opinions with the coverage, reliability, and benefits WARN provides to their daily and emergency operations. The survey included a scoring section and allowed for users to expand upon certain items and specifically requests opinions on areas of improvement. The following are unedited excerpts from the District's monthly user surveys.

WARN BENEFITS

DC Fire and Emergency Management Agency

"WARN has helped me as an F/EMS planner in numerous ways. I attend many meetings throughout the city. In these meetings, I access files via WARN that allow me to make video and graphic presentations and to access other people's information in ways that would not be possible without it. This ability has made my work more efficient.

I have also used the WARN network on multiple National Security Events, special events, and emergency responses to track unit status information in real time, to access the METRO Protect System, to compile data, and access the internet and send and receive emails."—DC Fire and Emergency Services

DC Emergency Management Agency

"WARN has had a tremendous impact in our ability to access and transfer critical information to and from our mobile command center. It has provided our mobile units with a fast, simple, and reliable means through which to send and receive digital information. The ability to transmit live streaming video or access our GIS server from the field, has proven invaluable to senior management in their decision making process. We look forward to the day WARN has expanded throughout the NCR."[53]

DC Fire and Emergency Medical Service

"For F/EMS users, it should be expanded to all EMS Operations Supervisors."[54]

"This system continues to be an asset to our agency. Without it, there are times we would be much less efficient in our operations."—December 2005 User Survey

U.S. Park Police

"Mobile Command HQ used/relied on our WARN connection HEAVILY during the recent IMF/World Bank and Anti-War Demonstrations. The system worked flawlessly in spite of our "difficult" location (adjacent to the West Wing)."—U.S. Park Police

[53] District of Columbia, OCTO, *NCR Interoperability Program FCC Waiver.* (July 3, 2006), at 11-12.
[54] Id, 12.

"During the month of January 2006, the United States Park Police, in coordination with the DC Office of the Chief Technology Officer, installed a WARN connection at the USPP Anacostia Operations Facility. This connection now enables the United States Park Police Command Center, designated as such for large-scale incidents and events, to have direct access into District of Columbia databases, allows for extensive data interoperability with District of Columbia government and public safety partners, and provides a robust platform for continuity of operations should an incident result in the loss of the United States Park Police backbone. This is an outstanding partnership."—U.S. Park Police

SUGGESTED IMPROVEMENTS

The following represents a comprehensive list of all suggested improvements from the WARN customer surveys:

August 2005

"Wants additional training."—HSMP

"More coverage or bigger antennas to expand coverage at the fringes of the covered area."—F/EMS

"More coverage in the SE toward Bolling AFB."—MPD

"Better coverage in 400 block of 8th St., SE."—F/EMS

"Need external antenna."—F/EMS

"Better in-building coverage."—DHS

"Lighter PCs (They are using a *free* but heavy-ML-900)."—EMA

September 2005

"Different antenna options."—F/EMS

"Stronger signals"—F/EMS

"Provide a better alternative to current Greenhouse video software"—MPD

October 2005

"Need more coverage in the SW and SE area of the city. East of the river. Seventh District area" —MPD

"Difficult to say due to short notice of EMA's request. Staff was more than helpful and provided the best possible service. The process of identifying IP's, opening ports, etc. is cumbersome, especially in an emergency situation. Due to short notice 2 cards were not activated." —EMA

November 2005

"Again, nice system, needs more coverage in SW." —MPD

"Not receiving a signal at 12th and Franklin St., NE over to First Street and Michigan Ave NW. Not receiving a signal in the 800 block of 8th St. SE." —F/EMS

"Seems like coverage could be better in certain areas." —F/EMS

"The signals are weak and also the connect. If we connect, it works fast." —F/EMS

December 2005

"No coverage in NE part of the city around Montana Ave and W."—F/EMS

"Better coverage." —MPD

"Speed and coverage good. Coverage can be improved." —F/EMS

January 2006

"Wider coverage when system gets more sites. Lower SW part of the city still needs coverage. How about a tower at Hadley Hospital." —MPD

"For F/EMS users, it should be expanded to all EMS operations Supervisors. The software from Intergraph to access the CAD and AVL would help tremendously." —F/EMS

"Speed and connections." —F/EMS

"Not sure if I've asked for this but a detailed coverage map (GIS layer)." —EMA

"We are still having coverage and speed issues in certain areas of NW. I have provided a map and highlighted the areas of no coverage compared to the old multicast system." —USPP

"Get it to work in COG and at my house in MD :) Keep up the good work guys." —F/EMS

February 2006

"More Coverage." —F/EMS

"Speed and area coverage can be improved." —F/EMS

"My computer has been down so my usage has been limited due to some software/hardware issues. I have had problems when logging into Packet Cluster while the WARN card is connected (locked in). When it is disconnected, I can log in?? Hopefully once I am up and running, I will have more feedback." —MPD

"In order to have effective use of Pictometry we will need to pay to have the Pictometry image library compressed." —OCTO

"Allow DCFD (FEMS) VPN users access to Greenhouse." —F/EMS

March 2006

"Expand." —F/EMS

"It will be great if speed can be fast." —F/EMS

April 2006

"It is a wonderful system and it should have a larger area of coverage." —F/EMS

"Connection Faster." —F/EMS

May 2006

“A site is needed in lower SE for better coverage.” —MPD

“Would like to get links to all public video transmissions under DC Control for special events.” —MPD

June 2006

“Perhaps more antenna strength.” —MPD

“Low signal quality.” —MPD