GOVERNMENT OF THE DISTRICT OF COLUMBIA
OFFICE OF THE CHIEF TECHNOLOGY OFFICER

Suzanne J. Peck
Chief Technology Officer

August 20, 2005

Federal Communications Commission
Experimental Licensing Branch
MS 1300E1
445 12th Street, S.W.
Washington, DC 20554

Re. Experimental Radio Station Construction Permit And License
Call Sign WD2XHO
Third Progress Report

Dear Madam/Sir:

Pursuant to the special conditions included in the grant of the experimental radio station and construction permit and license for WD2XHO (FCC File 0042-EX-ML-2004), please find attached the Third Progress Report of this experiment.

Should any clarification be necessary, please do not hesitate to contact Guy Jouannelle at 202-727-7796.

Sincerely,

Robert LeGrande, II
Deputy Chief Technology Officer

**The Office of the Chief Technology Officer**
**of the**
**District of Columbia (OCTO/DC)**

# THIRD PROGRESS REPORT

**on the**

**Construction and Operation**

**of the**

**Experimental Wireless Accelerated Responders' Network**

**Experimental Radio Station License**
**Call Sign WD2XHO**

# Table of Contents

## Background

The District of Columbia has recently completed an analysis of its public safety wireless data network deployment options and has determined that the spectrum and technologies on which they are based do not fulfill the pressing need of first responders today, much less the increasingly complex environment envisioned for the near future.

In order to demonstrate that affordable technologies exist today to support the critical public safety applications, the District has decided to deploy a wide area (within Washington DC city limits) broadband wireless data network that will serve as a pilot for next generation of public safety applications. The intent is to specify technology and features that best suit public safety applications' requirements. To this end, the District has filed for an experimental license in January 2004. The FCC has granted this experimental license (Call sign WD2XHO) in February 2004. As the experiment will use the 700 MHz upper-band, an additional outcome of the experiments will be an evaluation of the impact of interference received from/created into TV stations broadcasting in this band.

The Office of the Chief Technology Officer of the District of Columbia (OCTO) selected Motorola and Flarion Technologies to provide, install and support a 12-site Flash OFDM broadband wireless network, WARN (Wireless Accelerated Responders' Network).

In order to allow the vendors to deliver the equipment on an expedited fashion, a modification of the experiment license was filed and granted in August 2004. The modification did result in swapping uplink and downlink frequencies.

At the time of the filing of the previous report in February 2005, the network was operational and had been successfully used by public safety officials during the Presidential Inauguration and the President's State of the Union Address. In March 2005, the District filed for the licensing of two additional sites to enhance the coverage and capacity of the network. The FCC granted those licenses as well as an extension of the experimental license.

## Network Infrastructure

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 access through the District's private WAN to other District agencies and the Internet for WARN users. Applications servers are either located in the WARN network or in the agencies' WAN. Proper security policies, appropriate firewalls' configurations, and dedicated links limit the access of those applications to the relevant end-users.

A detailed description of the network architecture is included in the second Progress Report of Experimental Radio Station Construction Permit And License (Call Sign WD2XHO) filed in February 2005.

### *Coverage:*

As expected, the adjunction of two sites has improved the coverage and capacity of the network in key geographical areas of the city.

### RFK Stadium Neighborhood:

The addition of one site on the RFK stadium did alleviate coverage issues experienced along the Anacostia River.
As this site took over a significant part of the traffic from its neighboring sites, its operations eventually resulted in enhancing the available capacity in the US Capitol area.
Finally its location at the stadium, enables the support of critical first responders' communications necessary during the Nationals baseball games. During those games, the DC Emergency Management Agency (DC-EMA) , the DC Metropolitan Police Department (DC-MPD) and the DC Fire and Emergency Medical Services (DC-FEMS) are deployed on site with their command buses, generating therefore a high traffic demand. The support of such a demand was not possible before the operations of this additional site.

### White House Neighborhood

One sector of an additional site in the White House vicinity has been operational for several months. It covers the White House and its grounds, as well as part of World Bank neighborhood. The load of this site has been increasing significantly, in particular during major public safety related events. Adjunction of two additional sectors, currently under permitting boards review, will alleviate those capacity issues in the coming weeks.

### *Network Performance*

Since the second progress report, various tools have developed to monitor the performance of the network, and the activities it supports.

Those tools use the performance data recorded at each base station as well as using the traffic logs on both AAA servers. Those tools have allowed us to produce the reports and graphs below, and derive network usage trends.

This analysis show that although the number of users in the last six months was still very limited, more than 56 Giga Bytes of data were transmitted on the uplink, and more than 66 Giga Bytes of data was transmitted on the downlink (see table below).

| | Uplink traffic volume (Bytes) | Downlink traffic volume (Bytes) |
|---|---|---|
| **Agency 1** | 46,707 | 39,093 |
| **Agency 2** | 1,311,355 | 4,337,956 |
| **Agency 3** | 130,302,607 | 213,034,837 |
| **Agency 5** | 21,680,038 | 228,803,530 |
| **Agency 6** | 675,339,283 | 375,348,476 |
| **Agency 7** | 2,378,566,761 | 11,851,992,219 |
| **Agency 8** | 537,806,779 | 2,183,555,257 |
| **Agency 9** | 27,500,362 | 319,359,988 |
| **Agency 10** | 9,161,849 | 43,575,841 |
| **Agency 11** | 1,184,698,665 | 1,774,803,797 |
| **Agency 12** | 33,146,598 | 213,264,098 |
| **Agency 13** | 75,399,886 | 271,647,227 |
| **Agency 14** | 50,490,271 | 354,101,317 |
| **Agency 15** | 35,602,777,367 | 35,112,282,486 |
| **Agency 16** | 448,347,676 | 674,916,511 |
| **Agency 17** | 11,052,706,293 | 249,404,497 |
| **Agency 18** | 302,686,293 | 2,009,800,840 |
| **Agency 19** | 3,806,398,135 | 10,392,394,304 |
| **TOTAL** | **56,338,366,925** | **66,272,662,274** |

**Table 1: Volume of traffic transmitted between Feb 20 2005 and February 14 2005.**

Moreover, Figure 1 below depicting the evolution of the traffic volume during those six months shows that the daily usage of the network is increasing consistently.

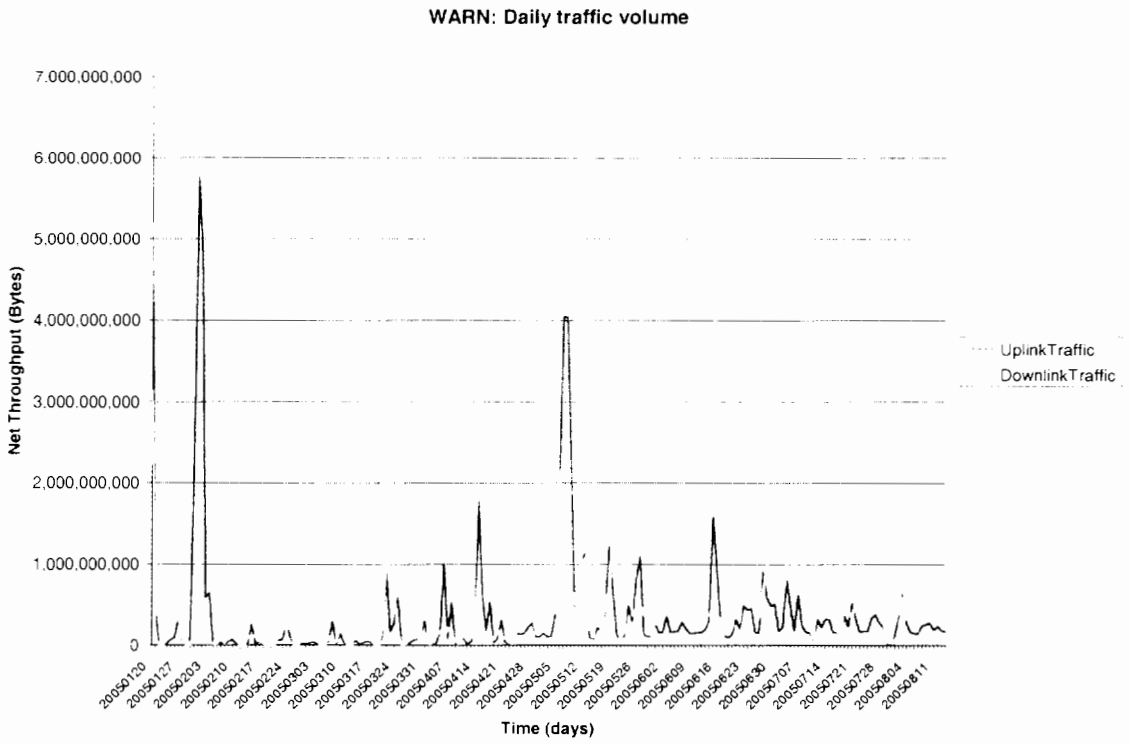


**Figure 1 - Daily Traffic volume (Bytes), January 20, 2005 to August 15, 2005**

The following graphs depict the load on the system, and the total throughput experienced on daily basis on the system. It is clear from those graphs that not only the daily traffic is increased as a whole, but its geographic distribution expands as the number of sectors heavily loaded increases. As agencies expand the usage of the network, traffic, load and throughput are expected to grow accordingly.

It is also remarkable that unlike the traditional internet traffic, those graphs show equivalent traffic requirements on the uplink and downlink.

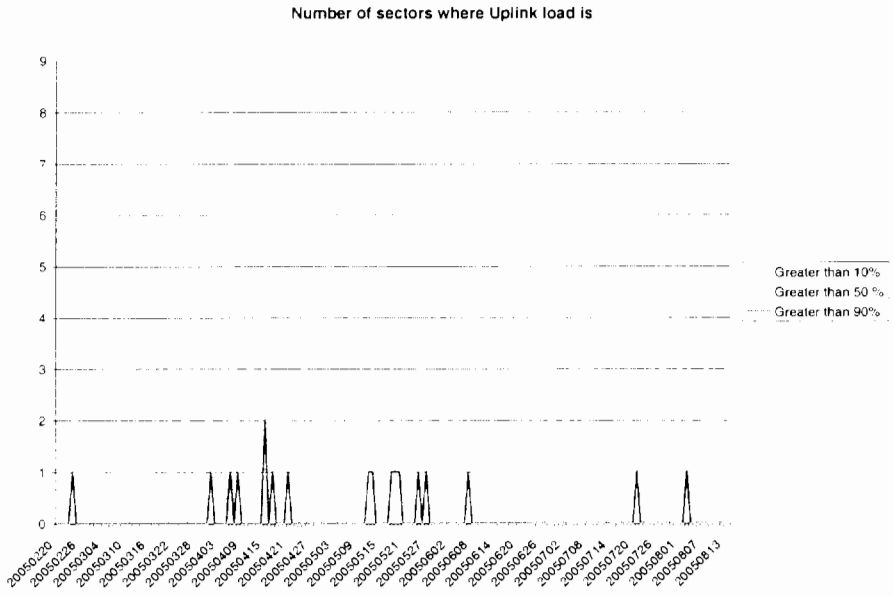


**Figure 2: Uplink Load**

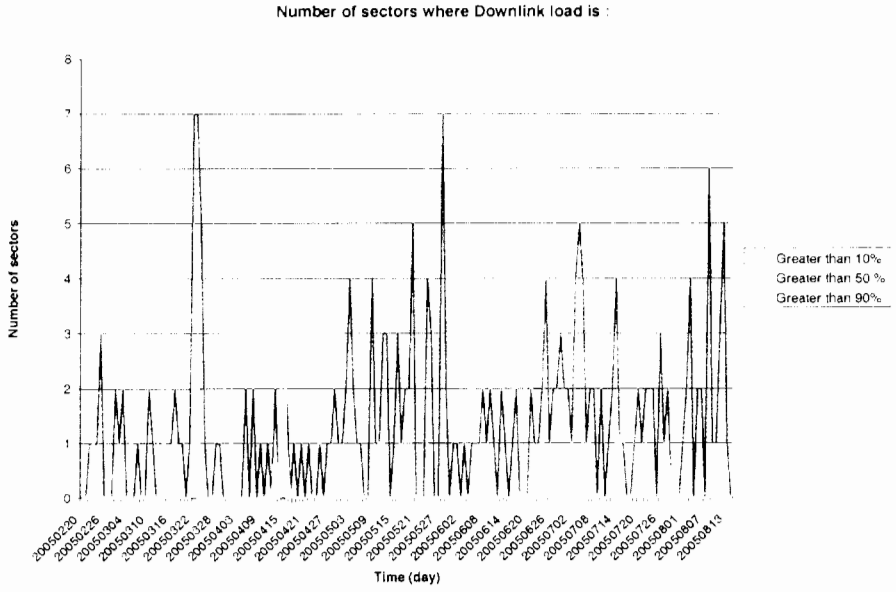


**Figure 3: Downlink Load**

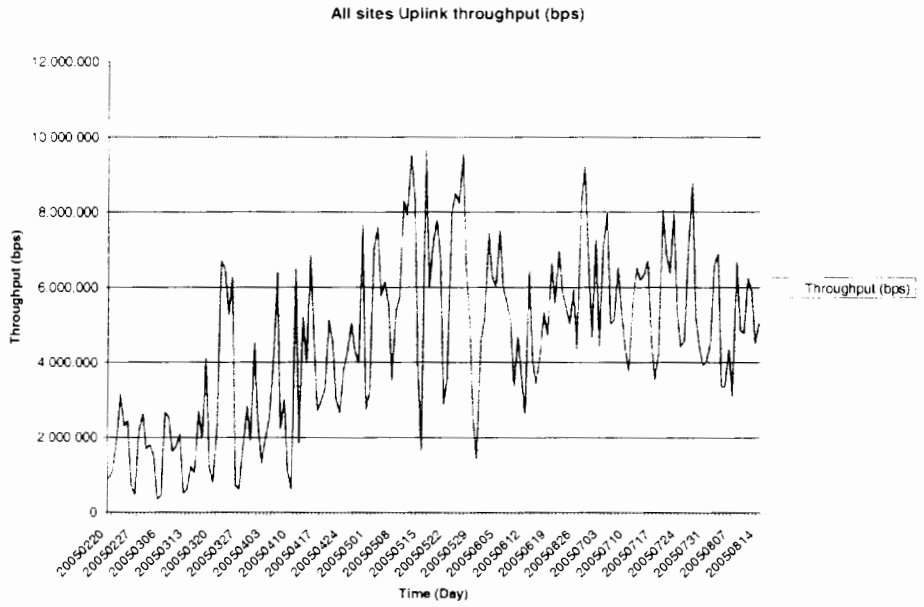


**Figure 4: All sites Uplink Throughput**

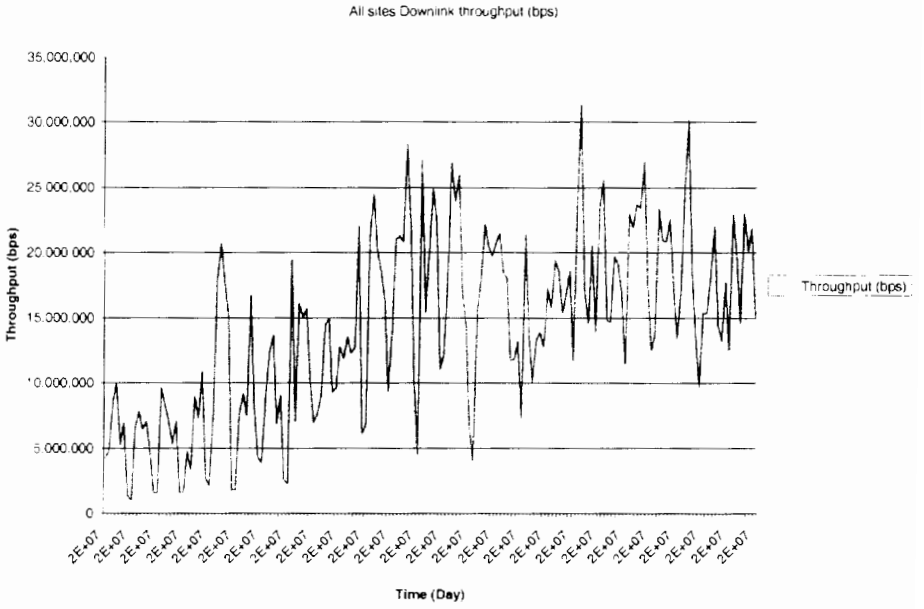


**Figure 5: All sites Downlink Throughput**

## Network Operational Experiment

This section describes the operations of the WARN network from a user prospective.

It first describes who the users of the network are, and what applications they are using. It then describes applications specifically used for the 4th of July.

### *Usage of WARN*

The WARN pilot broadband wireless network was accepted from Motorola/Flarion on December 31, 2004. At the same time, 180 PCMCIA cards and 20 PADs (external modems with Ethernet and USB ports) were delivered. Since that day, 115 WARN PCMCIA Cards and six pads have been distributed to users. Participating agencies include the following: DC MPD, US Secret Service, DC EMA, DC F/EMS, US Park Police (USPP), the Washington Metro Area Transport Authority (WMATA), DC Department of Corrections, DC Department of Youth Rehabilitation Services, DC Addiction, Prevention, Recovery Agency, US Federal Protective Services, Department of Homeland Security, Office of the Medical Examiner (OCME) and Alexandria Police Department, Fairfax County, Prince George's County Health Department, and the Maryland Institute for Emergency Medical Services Systems.

The US Park Police (USPP) is a very active user of the system. Recently, they apprehended an individual in Rock Creek Park who had an outstanding warrant. By utilizing the WARN card, the Police 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 are jointly evaluating and determining best practices in the transmission and use of video from a helicopter. Requirements addressing this specific issue will be developed in the coming month as it appears all first responder agencies are interested in pooling resources and sharing this type of information on a regular basis.

Another key user of the system has been the DC FEMS department. They are actively using the WARN cards in a variety of services, from their Public Information Officer using it to transmit pictures to the media outlets, to their Arson department filing reports in real-time, to their Hazardous Materials department testing out ways to decrease the time required to investigate bio-chemical alarms. Additionally, the FEMS equipped their command bus with the capability to communicate on the WARN network. DC-FEMS utilized the system on site at such incidents as the mercury spills at Cardoza High School that occurred recently. Following the success of these operations, FEMS has requested additional cards to be deployed throughout the agency.

Additionally, the WARN system has been demonstrated to a number of public safety agencies, raising keen interest. Those agencies include the Department of Homeland Security, NTIA, the DC Department of Health, the Prince George's County Health

Department, the FCC (Media Bureau) as well as, staff members of the Senate Commerce and Energy Committee. Technologies demonstrated over the network included Greenhouse and LiveWave (video applications), I-Net Viewer (GPS locator) and HazardPoint (Diagnostic testing).

While supporting Local and Federal agencies in implementing and operating their applications, the program is continuously fine tuning the configuration of those applications, and evaluating with vendors alternative and creative solutions meeting first responders' requirements.

In particular, streaming video is a crucial application for first responders. Those video applications are particular challenging in terms of throughput and network load, and therefore drive the dimensioning of the network and/or the associated public safety spectrum requirements.

This is the reason why this pilot program, in conjunction with the first responders, dedicates significant efforts to review and evaluate the video applications available on the market, and work with the vendors to improve their products to match public safety mobile communication needs.

For instance, with the addition of the DC Department of Corrections as a user, we have added the product, KaptureNet as another video surveillance application to be used over the network. The Department of Corrections and OCTO are currently working with the vendor to optimize their algorithms and ultimately provide the adequate service to the end-user. The purpose of the camera is to help provide incident control during the transportation of inmates. The video is recorded and downloaded at a designated site, but it can also be accessed wirelessly and instantly when necessary. The unique aspect of this product is that it combines a GPS locator with the video. As a consequence, the department knows where their vehicles are at all times and essentially "check-in and look" whenever they want to do so.

Our research shows that an increasing number of video products are maturing and becoming better positioned for the public safety mobile wireless environment. Bandwidth requirements greatly vary with the vendors' solutions, as does the quality of the video itself. The flexibility of the application to match the quality of the image (and therefore the required bandwidth) to the specific need of the first responder is a key evaluation criteria of the application.

## ***Fourth of July:***

Major events require special attention as they drive the highest demand on the wireless network. Most recently, WARN was able to support a number of these agencies during the Fourth of July celebrations on the Mall.

The agencies supported mainly included :

- US Park Police
- DC EMA
- DC FEMS
- DC MPD

The applications deployed were:

- **I/Netview**: This is an application allowing the tracking and monitoring of vehicles using remote GPS. This application was available in a command bus.
- **LiveWave**: This is a streaming video application using motion jpeg to code the images. Typically, this application is used to send streaming video feeds from mobile cruisers to a server. It is 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 requires up to 350 kbps.
- **Greenhouse:** This is another streaming video application using mpeg4 as a codec. It supports also peer-to-peer video communications. Its usage is very similar to Livewave's. Throughput requirements range from 100 kbps to 150 kbps per video feed.
- **Traffic Land**: This application includes a set of DC-DOT cameras located at strategic locations (crossroads, sensitive buildings, etc.) and connected to the District WAN. It is possible for authorized users (command bus) to access those cameras and download the images. In the current status of this application each video feed requires about 45 kbps.
- **CapWIN, JUSTIS and WALES** are application enabling regional public safety users to query several regional public safety data bases, and exchange messages.
- **Internet:** General internet access in particular access to live weather updates, and other information data bases.

During the Fourth of July, OCTO personnel were stationed at the US Park Police's command bus in order to assist in the set up and maintenance of the system. With a combination of four agencies heavily using the network, it was a vital implementation of the system. Through the sharing of valuable resources such as video, a very real savings in time, money and personnel was realized.

Moreover, during this event, the network enabled the deployment and the usage of those applications in a wide geographical area. Support of those applications would have not been possible with the traditional wireless technologies available to public safety, as the following testimony enhances:

"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 of Columbia including the Rock Creek area. The tests were met with very positive results. These MDCs 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.

The United States Park Police was extremely satisfied with the results of this next step in testing and deploying this critical dedicated public safety network.

Respectfully,

Lieutenant David J. Mulholland
Commander, IT & Communications
United States Park Police"

## Next milestones

In the coming months, OCTO intends to further improve the performance of the network and the service to the Capital first responders.

- Deploy additional cards to satisfy the growing demand of local and Federal public safety agencies.
- Review, test, optimize, and deploy additional applications, in particular video applications,
- Rollout of two additional sectors on the White House site