

Sponsored By:

***NORTHROP GRUMMAN***

The logo for Northrop Grumman, featuring the company name in a blue, italicized, sans-serif font. A thin blue curved line starts under the 'N' and sweeps under the 'M'.

**Municipal Wireless Snapshot Report™**

# **When Crisis Hits the Fan – Muni Wireless to the Rescue**

*May, 2007*

**By Craig Settles**  
President  
Successful.com

# Table of Contents

<b>Introduction .....</b>	<b>page 3</b>
<b>I. The muni wireless-driven crisis response solution .....</b>	<b>page 5</b>
Technology components .....	page 5
Setting the stage for crisis response .....	page 6
Scenarios for improvement.....	page 7
<b>II. Morrow County – the gold standard for muni wireless-driven crisis response.....</b>	<b>page 13</b>
Meeting the security challenge.....	page 14
Beyond WiFi, other options .....	page 15
<b>III. Checklists for municipalities, businesses, colleges and others .....</b>	<b>page 16</b>
Network considerations.....	page 16
Security preparations .....	page 18
Putting the right information in place.....	page 20
Technology considerations for end users .....	page 21
<b>IV. In the final analysis .....</b>	<b>page 24</b>
Reality check .....	page 24
Show me the money – it’s everywhere .....	page 25
This is a teams effort .....	page 25
The seven P’s are critical.....	page 26
<b>V. Conclusion.....</b>	<b>page 27</b>
<b>For more information .....</b>	<b>page 28</b>

**All views, opinions and recommendations expressed in this report are solely those of the author and the individuals interviewed.**

## **Introduction**

---

If you work from the premise that every minute saved could be a life saved in a crisis response situation, then you probably agree that proven technology that saves precious minutes deserves priority attention. Municipal wireless is the centerpiece of a technology solution to crisis management that many cities and counties need to consider ASAP.

Recent events at Virginia Tech, the San Francisco Bay Area and several other U.S. cities highlight the Achilles heel in local and regional public safety – in spite of 9/11 and Katrina, most governments are not prepared to adequately deal with large-scale catastrophes. Many law enforcement and emergency responders do a great job working with what they have, but they aren't getting everything they could to meet the needs at hand.

Three major problems face typical crisis response and communications operations when a major man-made or natural disaster strikes.

1. Emergency responders and even those victims of the crisis don't know everything that's going on in the first minutes or even for a full hour or more of a crisis. Valuable time is lost, everyone involved operates in confusion and individuals can't take additional actions that prevent serious injuries or deaths.
2. The appropriate responding agencies, whether local, state, federal or different departments within the same jurisdiction, can't communicate with each other because they use different communication equipment.
3. Compounding this problem is the fact that those in need of being saved or treated often can't communicate with their rescuers.

The real tragedy is that many components of a solution to these problems already exists, yet some politicians and managers of emergency response organizations don't understand the life-saving opportunities these technologies represent. IP (Internet Protocol) communication, broadband wireless (including WiFi, cellular, WiMAX and other wireless options) digital video and audio, basic database technology and municipal wireless networks are the core of the solution.

Although the design and implementation of a solution using these components can be time-consuming and require a substantial amount of multi-agency and multi-constituent coordination, the business case is quite simple. By building the right network to enable applications and users to wirelessly share text, video and audio via standard computing and communication devices, creating databases of appropriate information and developing a tech-driven crisis response plan, you can reduce pain, misery and death.

The right networks are the municipal wireless networks that hundreds of local governments currently are considering. These networks are based predominantly on WiFi technology, but also include digital cellular technology and WiMAX. To be clear up front, these networks by themselves won't prevent crises and disasters. However, with the right applications running on them, these networks can dramatically reduce the impact by increasing the speed and effectiveness of personnel responding to these tragedies.

Also, let me be clear up front, before the hue and cry from security experts start yammering that municipal networks are not secure enough for these types of applications. Security is a serious concern, but these networks can be made more than secure enough for the crisis response solution I'm about to present – and I have proof.

Given the seriousness of crisis response, you may want to re-think your government's role in the network's ownership and management, particularly with regard to actions you take and contractual obligations you specify to ensure quality of service. The scenarios I present of how muni wireless can improve crisis response reinforces the importance of building the right network for the job and not leaving this solely in the hands of third parties.

*This is one of a series of qualitative research and analysis reports that provide a snapshot of major issues impacting municipalities' pursuit of broadband wireless networks. Each report expands on a theme presented in **Fighting the Good Fight for Municipal Wireless**, my book that helps readers understand the business and political issues that should be addressed when developing and deploying these networks.*

## **I. The muni wireless-driven crisis response solution**

---

This section presents the big-picture view of how these networks can ease suffering and save lives. Section III describes the framework for deploying a network and related applications so they function as a cohesive crisis response tool.

### **Technology components**

Accessing as well as sending text, audio and visual data via the Internet and intranets is made possible because of IP. Whether you use a Web browser or software applications, build Web sites or intranets, use e-mail or instant messaging, if these tools are built to support the IP standard you can access data and communicate over a network that enables IP-driven communication. The network – Internet and intranets - can be wireline or wireless operating indoors or outdoors.

Anyone on the planet using a desktop, laptop, smartphone, dumb phone or any other device and widget that can reach and transfer data over an IP-based network can communicate with any other person using a similar device or widget. These individuals also can locate, monitor and manipulate through the network inanimate objects such as firefighting equipment, buildings and vehicles equipped with sensors that send and receive digital data over the network.

By enabling people to use an IP network without the need for a physical wired connection, as is the case with municipal wireless networks, individuals anywhere can access data on any Web servers and intranets at any time as long as users have wireless coverage. In similar fashion, people can send messages and communicate in real time with others using the Net. Just as IP is a standard for the technology that enables communication between points on the Internet and intranet networks, WiFi is a widely adopted standard that enables computing devices, sensors and the like to wirelessly access these networks. Other wireless standards include cellular data, such as CDMA, UMTS and WIMAX.

The great thing about IP and WiFi is that hundreds of millions of computing devices and widgets are built to support both. So, how does all this play into crisis response? When you build a network over which so many existing devices and yet-to-be-made gadgets can talk to each other, you enable a host of benefits that resolve these two key problems:

- 1) emergency responders often can't talk to each other; and
- 2) those directly involved in a crisis often can't reach responders or information that can help them.

Besides supporting WiFi-enabled devices, many municipal networks use a design scheme often described as mesh networking. A large number of access points (radio transmitters) cover the city and interoperate in such a way that, if one access point or a group of them fail, data being

communicated is directed around the failed equipment. What's more, mobile access points can be brought into an area to temporarily replace non-working transmitters.

Alternatively, WiMAX and cellular data technology can be deployed to cover a much wider area and at higher bandwidths than those of typical WiFi access points. This reduces administrative overhead and increases performance of the network. New York City chose UMTS cellular data technology to provide a comprehensive city-wide secure broadband wireless network for its public safety and other city agencies.

The following describes the benefits an effective municipal wireless network can deliver. The examples are based mainly on real world applications that are in place, though a few depend on products still in development.

### **Setting the stage for crisis response and communication**

A fair number of crisis response applications a wireless network can deliver depend on constituents putting certain technologies and data in place, particularly in educational facilities and commercial buildings (i.e. hotels, business campuses, industrial parks).

There needs to be an interlaced network of video cameras that can be activated in event of an emergency and accessed from the municipal network. A highspeed office WiFi network should be in place throughout these facilities, either as part of the organization's main computer network or as separate emergency-use network. Users on this and the municipal network need to be able to access an easy-to-navigate database of floor plans, escape routes and other information to help those affected by a crisis and emergency responders to take appropriate action.

Corpus Christi did something you should consider to not only facilitate crisis response, but also resolve the issue of municipal networks coverage not reaching above two stories. This city put scaled-down outdoor access points in the floor spaces of government buildings and linked them to the muni network. These transmitters in high-rise commercial and residential buildings can provide the horsepower needed to drive applications and give individuals access to the outside world when a crisis strikes. Alternatively, Meraki (<http://meraki.net/>) markets an access point technology that can boost indoor coverage.

In addition there should be a central text messaging and instant messaging application that can reach people within the organization (students, employees, event attendees, etc.) as well as communicate externally to emergency response agencies. Further enhance IP-based communication with a basic Voice over IP (VoIP) application such as Skype that everyone who is part of the organization can use. VoIP enables non-mission critical communication among teams of people and complement dedicated radio channels.

Finally, write a detailed plan for when and how to use these technologies, and develop an awareness campaign so everyone located at the premises knows the procedures for using the technology, accessing information and communicating with others. Ideally, have some synopsis of the crisis response plan in a digital format that people can load onto their mobile devices. Have a version for some of the more likely emergencies, such as earthquakes, flooding and armed assault.

Many of the people within a facility or campus, including the general public, have smartphones or cell phones. An increasing number of phones are sold with multi-mode capability, enabling roaming between commercial networks and private WiFi, WiMAX or other private network technologies and frequencies. Design emergency communication to reach these small screens. Workers and students are likely to also have laptops, but except at their desks, coffee shops and the like, these might not be convenient to use during the initial stages of a crisis.

With these and other appropriate resources internal to organizations and building complexes in place, let's play out various crisis response scenarios.

### **Scenarios for improvement**

#### *Muni WAD (Wireless Aided Dispatch)*

At Virginia Tech, law enforcement personnel were held up for five minutes because the doors had been chained from the inside. Officers had no way to know before arriving and probably no precedent for this in similar mass shootings, so they lost time getting the proper equipment. Meanwhile the gunman was shooting someone (estimated) every 30 seconds.

When the gas tanker truck ran into the freeway structure in Oakland, CA, setting off a huge blaze, calls pouring into 911 were confused and conflicting because at 3:00 a.m., excited and without specific road signs, people didn't know the exact location of the incident. Though response by emergency personnel was reasonably quick, time was still lost.

The people at the scene when a crisis breaks are the best sources of information to aid dispatchers send the right people and equipment. However, except for the most levelheaded, they are often the most unreliable because of the stress and distraction dealing with the crisis. The next best thing to help dispatchers is to have people and/or wireless sensors at the scene trigger technology that aids dispatchers.

As a crisis unfolds indoors, any individual with a WiFi-enabled device should be able to access the organization's network and trigger video cameras to switch on and stay active until the crisis is over. These folks should also have access to contact information to alert appropriate people within the facility or organization who then establish a link that police access to communicate through voice or text with the victims of the crisis and others at the scene. In facilities that are empty during the night and weekends, sensors detecting motion or monitor environmental

conditions such as sudden increase in heat, chemicals in the air, etc. can trigger similar actions.

For outdoor areas, the networks' access points can pinpoint WiFi-enabled mobile devices of people who use the network to report emergencies. Combined with video cameras whose locations are mapped into the network and individuals with mobile devices' that can take pictures or live video, both dispatchers and first responders can see exactly what they're dealing with and possibly pin down the exact location.

#### *Police, SWAT teams, other law enforcement agencies*

As police are en route to the scene use the municipal wireless network to view streaming video from the scene, and download relevant floor plans plus pictures of various parts of the facilities so they can see what they're walking into. They also access documents such as an inventory of hazardous materials, utility shut off valves, lists of contacts, employee lists, class schedules and whatever other data helps them know about the premises and the people involved.

The ability to tap into a text or instant messaging application is essential because it may not be safe for people hiding in locked rooms and closets to speak, but they can send written messages. It also allows officers to send silent messages to guide people out of areas responders know to be secured. As more cell and smartphones incorporate GPS, it's possible that responders can also track victims who may be outside. VoIP capability allows direct voice communication to victims when possible, and can provide backup for land mobile radios or a platform for interoperability among agencies with disparate radio systems.

Once communication and visual contact is made with those in the crisis situation, police can use the muni network to link with fire and emergency medical units, building inspectors, utility companies and other departments or agencies using IP- and wireless-enabled devices. Text, voice, video conferencing and database access are applications everyone can share in an encrypted format as long as those involved use standard computing and mobile devices.

Officers traveling with mobile access points can set up communication centers wherever these transmitters are placed, and be able to move them continually as needed or bring in network access to the organization if their network becomes disabled. Sensors placed on officers and GPS capability allow officers to be tracked as they move about within the facilities. Even now, companies are developing personal sensors responders can wear to monitor heat, chemicals in the air and other environmental conditions that can pose problems for officers. These types of sensors for buildings are already in use.

Wireless robots with video cameras and microphones can be sent ahead of officers to secure areas, locate victims and target perpetrators. Plans are afoot in some cities to acquire wireless model-sized mini-airplanes or helicopters with video cams that can fly over areas and give officers an aerial view of situations.

### Emergency medical service (EMS)

EMS personnel receive the same benefits as police while on their way to deal with a crisis. They can see video from the scene, access [plus assess] important information about the facilities and all of the same information databases. Encrypted databases of residents in multi-unit dwellings, particularly the elderly and those with mobility problems, can tell responders the location and medical conditions of these individuals.

Once EMS staff arrive on the scene they can use video feeds to locate injured or wounded victims who are trapped in parts of a building, or in outdoor areas that may be cut off from immediate access by responders. Talking a victim's friend or colleague through procedures for applying correct pressure to a wound or administering CPR can buy valuable time and save lives. One of the Virginia Tech victims, a former Boy Scout, saved his own life by applying a tourniquet to his leg wound, but the average person might not know this. Responders can also relay video feeds to hospitals so ER staff can provide additional guidance to them or directly to victims.

Corpus Christi is driving an effort to have citizens authorize wireless access by EMS and ER personnel to citizens' medical records with data such as existing medical conditions, medications they may be taking and other data that facilitates faster, better treatment. Some of this data is also being stored on individuals' medic alert bracelets so EMS staff can scan and send this data to ER doctors if patients are unable to speak. These types of applications allow EMSs to begin more complete treatment before transporting patients and thus save more lives.

In fires, floods and other disasters, personal sensors allow those at command centers to keep track of personnel and better guide them to victims as well as keep them away from dangerous areas. Recently several individuals associated with UC Berkeley were designing headgear that incorporated a video camera, microphone and earpiece so the wearer can wirelessly send video and speak from a site. People in another location see what the wearer sees and communicate instructions to them in real time. Another company sells an eyepiece attached to a visor so the wearer can view data from a computer screen accessed wirelessly. These James Bond-type technologies can create more effective EMS personnel and emergency procedures.

### Firefighting personnel

While their trucks and equipment are en route to a fire or other disaster, firefighters see into burning buildings, either in real time or through floor plans, pictures and other visual aids, which is invaluable. They are better prepared upon arrival and fire chiefs receive a faster, more accurate assessment of what additional equipment to send out.

Wireless access to databases with floor plans, schematics, inventories of items on premise that might cause problems and summaries on occupants (numbers, locations, health conditions for those in healthcare facilities, etc) help responders refine strategy, also while en route. A

central database of techniques used in previous similar emergencies and details on the latest response tactics are very useful, especially for rookies and fire departments in smaller or rural communities.

Assuming the various city departments have shared access to data, firefighters access building inspection records to see what actions have been taken in the past at the location. They may need to access details from other departments or agencies in other jurisdictions including Parks & Rec, traffic control, transit authorities, county inspectors, the FBI and Homeland Security.

Air and sea have to be taken into account. Firefighters assigned or responding to airports or aircraft-related emergencies should have access to information specific to the aviation world that have a bearing on those responses. Here too, wireless access to databases of best practices, such as fighting fuel fires and handling air crashes in residential areas, help those whose don't have a lot of firefighting experiences in this area.

With the muni network firefighters are also prepared for other airborne threats such as chemicals and biological agents. Atmospheric and ground-embedded sensors wirelessly track anything dangerous that leaks into the air. On the waterways, wireless communication also plays a role keeping those on fireboats in the communication loop.

Once on site, firefighters immediately set up a command communication network using mobile access points and tapping into the muni network and the facility's network. Personnel from police, EMS, agencies and fire departments from other jurisdictions and additional organizations tap into the command network so everyone is working from the same page.

GPS, the muni network and personal sensors enable the communication center to track personnel as they move about inside buildings and into remote areas. Video cameras in ruggedized mobile devices enable commanders to see what firefighters see so they better direct operations. Peer-to-peer networking capabilities enable these devices to keep everyone in touch even if they are out of range of the muni network or main access points are disabled.

### *Traffic Control*

People often forget that controlling traffic during and after a crisis is critical, which was well apparent with the lead up to Katrina when highways trapped huge numbers of people trying to escape. The muni network and streaming video gives traffic controllers a [low-flying] bird's eye view of traffic conditions around an emergency scene, plus data coming in from traffic sensors and other video cameras provide a picture of adjacent areas. Controllers remotely can start immediately changing lights and taking other steps to help evacuate areas as well as guide emergency responders to the scene faster.

A software application that sends text or instant messages over the network to subscribing drivers allows the city to immediately push out

warnings and updates to alert drivers to dangers and direct them to appropriate routes. Those who have PDAs or other mobile devices with wireless and GPS features can also plot their own directions if they aren't linked to the government's alert system.

#### Public works and public safety

Another group of unsung heroes in emergency response are the hundreds or thousands of local, county and state public works and utility employees who handle streets, highways, gas lines, electricity delivery and other critical resources. Many natural - and a few human-generated - disasters can wipe out a community's ability to access one or more of these resources. In events such as earthquakes, the greater disaster is not the immediate damage but the domino effect resulting from exploding gas mains, water contamination and the like.

Any credible crisis response includes public works and utility companies, though I expect they'll often be under the command of law enforcement or firefighting managers at the scene. First responders on their way to an emergency need to have real time, high-speed wireless access to data resources that public works and utilities maintain: maps, schematics, aerial photos, underground pipes, structural data, etc.

These two entities work with traffic control to strategize on how to get crews and equipment to where they need to be as fast as possible. Mobile devices these crews carry provide real-time video and voice from disaster areas so their managers in the main offices provide guidance as needed and better coordinate with emergency responders.

The crews also benefit from immediate wireless access to documents and graphics so they can pull up information they need without losing time searching through paper documents, some of which may be limited or outdated. When equipped with GPS capability, the mobile devices they use also enable management to keep tabs on workers who may be in dangerous areas.

#### The general population

In locations vulnerable to earthquakes or hurricanes and resulting floods, the destruction of highways, freeways and city streets is going to lead to crises within a crisis as segments of the population become isolated from emergency responders and equipment. Heart attacks, accidents, fires, childbirth and other personal crises may need to be handled by individuals for some period of time until resources can be directed to them. Wireless may be their only lifeline.

One practical option may be for average users with mobile devices, and in some cases desktops when there is power, to link to the muni network to contact medical professionals and EMS personnel by some combination of text, voice, video and digital pictures. Since communication is over the Internet, those medical resources don't even have to be in the same city as users. Though far from ideal, everyone has to accept that in a crisis some care is better than no care.

Likewise, wireless may be the only access to information that people need to avoid making a bad situation worse, such as how to detect gas leaks and address the many challenges of surviving when cut off from basic needs and services often taken for granted. Unfortunately, the effectiveness of the technology depends upon access to electricity, but even a 12 – 24-hour period of intermittent access to the network can ease some of the problems.

Any number of early warning applications are possible given the technology capabilities at hand. Once the muni network is in place, local governments can institute a subscription service similar to what airlines use to alert customers about delayed or canceled flight. Without knowing where subscribers are located, software automatically pushes messages out to their devices based on what type of alerts subscribers want.

With the coordinated efforts of all of the previously described departments and agencies, a variety of alerts can be programmed to go out as requested and/or appropriate. Constituents, employees, students or other segments of the population can have an option to proactively tie into a portion of a crisis command center set up for constituents to communicate with emergency responders.

## **II. Morrow County – the gold standard for muni wireless-driven crisis response**

---

Morrow County, Oregon has built one of the most extensive muni wireless networks in the world. The driving force behind this network was for rapid emergency response and public evacuation in event of several significant crisis events. Their story defines the use of muni wireless as the foundation of crisis response using multiple technologies. It is also the proof I mentioned earlier of the ability to make these networks abundantly secure through practical steps that any municipality can duplicate.

The Morrow County Emergency Management Center's (MCEMC) team of first responders relies on a 700-square mile hybrid WiFi/WiMAX network to manage a myriad of monitoring and emergency response resources. A software application and sensor devices that monitor the atmosphere for chemical spills are the nucleus of the emergency response system. It not only detects, but also plots out in which direction a chemical spill will travel and how fast. The data is automatically routed to field staff's laptops.

Morrow County is the site of the Umatilla Chemical Depot that holds about one-third of the U.S. remaining stockpile of chemical warfare materials. This county is home to the Hanford Nuclear Reservation. They also operate a nuclear power station. One of the major east-west rail lines in the western U.S. runs through the county. Morrow County hosts major natural gas and energy production and distribution facilities.

Cameras linked to the network stream real-time, full-speed color video to monitor these facilities, and can be remotely controlled to turn and zoom in on specific areas. The same type of cameras monitors the highways since in the event of a chemical disaster the staff has about 10 minutes in which to respond. If they need to quickly evacuate residents, MCEMC relies on those cameras and the network to remotely re-direct traffic by controlling traffic lights, drop-arm barriers and billboard-size electronic message signs that can post new text as needed.

MCEMC deployed WiFi access points mounted on buoys on the rivers and waterways to provide warnings to watercraft as well as back up to land-based WiFi points. This same system can operate un-manned fireboats to fight hazardous materials fires on or near shores.

The main PBX phone lines all have VoIP capability that also provides backups to the cell phones, so workers with dual mode phones have greater assurance of connectivity. Emergency response vehicles are equipped with mobile WiFi access points, plus the network was designed to handle hand-off along the highways using 66 towers with long-range antennas. Responders can stay connected to the network while driving up to 100 mph.

## Meeting the security challenge

The network is HIPAA-certified safe so patient data can be wirelessly transmitted while en route to hospitals. On top of that, the network also complies with the Federal Information Protection Standard (FIPS 140-2). Passing muster for both of these intensely high levels of security is equivalent to simultaneously parting the Red Sea and walking on water.

MCEMC doesn't worry very much about security being breeched, or network failure at a critical time. When MCEMC Director Casey Beard was an Intelligence officer for the U.S. Army, someone in the military went into hyper-security mode because it was possible, with the right equipment, to monitor a person's PC keystrokes in order to figure out passwords and such.

"We had all of these lead shields brought in for the walls, PCs were put inside special metal boxes and so on. Then one day I was thinking about it and realized that, sure, you could intercept keystrokes. But you'd need a lab environment to do it, which would require a semi trailer full of high tech gear and a bunch of antennas on the outside, and it would have to be parked almost in front of the building. Something like that sitting outside would be pretty obvious, I think. Historically with technology, the threats are often greater than the reality."

Casey believes any network is as strong as its weakest point, so his team strengthens the weak spots. They bought two commercially available WiFi security applications and later hired a security team to come in with special equipment to try to hack the network, which they couldn't do. MCEMC constantly follows all of the standard security practices such as hounding employees to secure passwords, not link into access points without the appropriate security features enabled on their devices, etc. "There's always going to be a tradeoff between being able to use information and protecting it. If you want total security, then don't use technology at all."

To fortify the network against natural disaster strikes, MCEMC relies on two massive fiber networks that come in from Portland. The WiFi mesh integrates with these networks and also has the access points densely deployed to provide overlapping coverage over many areas. There are trickle charge batteries that back up access points for eight-to-twelve hours. In some cases solar panels recharge the batteries, plus uninterrupted power supplies and standard generators provide yet more backup. The access points are placed to minimize vandalism, and the mobile access points offer yet another level of redundancy. If all else fails, Casey says they keep an adequate supply of white boards and grease pens.

Telecom industry reps and other anti muni wireless people are fond of saying that WiFi isn't more reliable than any other communication option because when Hurricane Katrina hit, the entire communication structure collapsed. This is true. But the day following it, the mayor managed to get in touch with the world by going down to an office supply store and borrowing some WiFi equipment.

WiFi might have collapsed along with everything else, but it was one of the first things to come back online. Roving teams of volunteers in various parts of the devastated areas brought in WiFi equipment and VoIP gear to connect displaced relatives with their loved ones. Even when cell phone calls weren't getting through, text messages were.

### **Beyond WiFi, other options**

While WiFi networks are certainly enjoying a great deal of popularity for public access, they may not always be suitable on their own for public safety and crisis management applications. Often public access networks, whether WiFi or commercial wide area technologies, are designed with the goal of serving the most people possible for the least cost. So care must be taken in choosing and/or designing a network to support mission critical public safety applications. In particular, key design requirements for such a network are primarily driven by coverage, mobility, reliability, survivability, performance, and security, as described below:

- ▶ Coverage - The system must provide high coverage of the areas serviced by Police, Fire/EMS, and other government user agencies. This includes large areas, as well as sparsely populated regions, hills and valleys, or "urban canyons" caused by many tall buildings.
- ▶ Mobility - The system must provide continuous mobile connectivity at high vehicular speeds.
- ▶ Reliability - The system must be highly reliable, that is, be built with redundancy and robustness, such that it automatically recovers when equipment or communication paths fail.
- ▶ Survivability - The system must be survivable, especially to hurricanes and other natural disasters, and immune to long term power outages.
- ▶ Performance - The system must have sufficient performance and capacity in all areas to support public safety applications and users at times of peak usage such as during a major emergency like a plane crash, terrorist attack, hurricane, etc.
- ▶ Security - The system must provide information security in order to protect the highly sensitive nature of the data that will be transmitted over the airwaves.

Other wireless network technologies, such as UMTS and EV-DO used in commercial cellular networks, can be owned and operated by municipalities to support the requirements posed by mission critical deployments and/or large coverage areas. For example, the Northrop Grumman Corporation is building and maintaining a citywide high-speed secure wireless data network for New York City's public safety personnel.

### **III. Checklists for municipalities, businesses, colleges and others**

---

This section gives you a general overview of primary elements that should be included in any comprehensive crisis response plan involving municipal wireless.

#### **Network considerations**

##### *The Plan*

Based on statements by various cities' officials, it's not clear to me that some of these network RFPs are backed by much more than a good idea and a basic sense of what civic leaders think is important. For a network to play a significant role in crisis response, a lot of thinking, discussions and more thinking must go into developing a comprehensive plan that takes into account both technology and the logistics of dealing with a crisis.

This planning must involve a host of people from local government, businesses, schools, colleges and other constituent groups. It needn't take many months to complete, it doesn't have to be hundreds of pages long, but it should be comprehensive and at the same time flexible enough to address the rapid evolution of technology.

##### *Speed*

Generally, access speed of 1 megabit per second (Mbps) up and down between users and the network is considered fast, and is one of the standard requirements in RFPs. However, for many of the bandwidth intense applications described in this report, you should consider 2 Mbps as adequate for the present, but by the end of 2008 I believe it will become apparent that greater speed should be the norm to support important applications. As applications like video and VoIP become the norm, performance demands will be even greater, so the technology must have a realistic roadmap of performance and feature enhancements.

##### *Coverage area*

In order to be effective as a crisis response tool, you need coverage just about everywhere emergencies or disasters may occur. This includes some areas that may be sparsely populated, heavily wooded and/or lacking in vertical assets from which to hang access points. Therefore the network designer must take into account these facts and develop an appropriate technology strategy.

##### *Bordering jurisdictions*

Since many emergencies can cross city, suburban or county borders, municipalities need to address the question "what do our responders do if the neighboring jurisdictions have different providers build their

networks? Or maybe that jurisdiction won't build a network at all. At the very least, neighbors should talk during the early days of the project planning to determine if there is a way for everyone to facilitate emergency personnel's network roaming between jurisdictions. Then this could become a component of the respective cities' RFPs.

#### *Reliability, backup and redundancy*

Along with needing to access the network from anywhere, those who are victims of, and responding to, an emergency must be able to get on the network anytime 24/7. This isn't an optional feature. That means key components of the network must have long-term power backup, including access points, gateways, power sources and any assets mounted on public infrastructure (light poles, towers, commercial buildings, etc.). The same applies for databases, network and Internet servers, mobile devices and major computing tools used by emergency responders. EVERYTHING needs a backup.

#### *Technology obsolescence*

One rarely noticed blessing of the Philadelphia network RFP was the requirement for the vendor to present a specific plan for upgrading the entire network by the end of a seven-year period with whatever represents advancements in technology suited to Philly's needs. Leaving it to the vendor to set the specific timetable for the incremental steps to get there, the city protected itself against the kind of tech evolution that makes last year's purchase next year's boondoggle. The technology solution should therefore be one that has a solid technology history and a reality- and standards-based future roadmap.

#### *Network priority access*

There may be several ways to achieve this, but regardless of who owns the network, local government must be guaranteed priority use of the network in times of crisis. The seriousness of the need and the types of applications required to meet these needs means emergency responders can't just hope they get the necessary bandwidth. They must be assured of getting it.

#### *Applications*

Probably the hottest market at the moment is text messaging applications as colleges across the nation scramble to see if this is the magic bullet that will make their crisis plans work. As important as it is to have this capability, cities need to look at several additional applications as must-have products: instant messaging (real-time two-way chatting), voice over IP and video are some of them.

Emergency responders must be able to see, hear AND speak over the network to fully maximize its value in an emergency. No one vendor can address all of these capabilities, but the acquisition of these capabilities must be driven by an all-encompassing plan.

## **Security preparations**

Making a municipal network that local government uses for crisis response secure is a critical responsibility. Morrow County proves that you can get great security through basic software and procedures, yet it still requires a lot of careful thought and planning to get it right.

Security isn't just a question of protecting the network from hackers. You must also protect it from the causes of a crisis. These networks must be operational in the face of natural disasters, terrorist attacks and even large public events or other situations where wide-scale coordination of first responders is a necessity. These networks demand high levels of reliability, survivability and security as well as priority access by emergency responders.

Northrop Grumman, a leader in providing secure broadband wireless networks for mission critical applications, provides the following guidelines that should be part of your network planning.

### *Soup-to-nuts hardware protection*

Secure all components and communication links comprising the entire wireless network from end user to the network operating center (NOC), such as

- ▶ User devices
- ▶ Access points
- ▶ Wireless links between the user devices and the access points
- ▶ Wired or wireless ("backhaul") links between the access points and the back-end network
- ▶ Back-end networks

The wireless network consists of hardware such as servers, gateways and switches. These process the data, users' information as well as signaling and control information that flows through them. Hackers can and will exploit any vulnerability that exists in any of these components, hence the security of the network is only as good as its least secure or most vulnerable element.

### *Security of Wireless links*

Wireless links are much more prone to eavesdropping than landline links. Strong encryption of user as well as signaling information using cryptographic protocols such as AES-256 is essential to protect the privacy of user and data communication.

### *Mutual user device and network authentication*

Crypto-based authentication mechanisms (X.509 or EAP) are required for the user device and network to mutually authenticate each other to establish trust. This will prevent attacks such as client or network impersonation.

### *Message Integrity*

All messages (including data and control messages) that are exchanged during various network processes such as authentication and hand-offs must be protected against tampering by using crypto techniques such as "digital signatures."

### *Preventing Replay attacks*

Replay attacks by rogue clients can be protected by time stamping the messages.

### *End user device*

Protect user devices from network attacks such as viruses and worms by using anti-virus software. Also protect them from unauthorized access. Additionally, in the event the device is lost or stolen, the network should be able to take control of the device to destroy any privileged or proprietary information stored on the device as well as bar the device from accessing the network.

### *User authentication*

Users must be authenticated to their devices through password protection. Users must also be authenticated to the network using string encryption techniques such as 2-factor authentication.

### *Network protection*

Various network elements such as signaling and media servers, switches and routers must be protected against unauthorized access and intrusion through the use of stateful firewalls, intrusion detection systems, anti-virus software etc.

### *Physical protection of the network assets*

The network assets must be protected against unauthorized physical access by implementing strong access control and identity management procedures

### *Public Access*

While it is vitally important to be able to receive information from and provide information to the public, this also poses one of the largest points of vulnerability to a secure network. The publicly accessible portion of the network should be virtually if not physically separated from the portion of the network accessible to public safety and emergency responders. Otherwise the public can inadvertently or intentionally overload the network, thereby impeding communications among the responding team and the operations centers.

### *Prioritization*

It is also crucial to ensure that network resources are available as required by the various users of the systems. Some applications and communications are going to have higher priority than others. For example, communications between emergency responders is vital and needs to be always provided without fail, whereas information updates to community, while important, are of lesser priority. The network must be able to distinguish between different levels of priority and block those communications of lower priority if they are getting in the way of those of higher priority. This is done by establishing and maintaining Quality of Service agreements.

### **Putting the right information in place**

A crucial part of implementing an effective muni wireless crisis response strategy is the information that resides in the databases that law enforcement and emergency personnel as well as crisis victims access. You may want to have one centralized database for emergency responders and government departments involved with managing crises, then siphon off information from this which is appropriate for the general public.

The following is just a small sampling of the information you should have on the central database. But it gives you an idea of where to start. Vendors of crisis management applications, such as Prepared Response, can help you develop a complete list of required information.

- ▶ Maps, floor plans and aerial photos of buildings in malls, school, college and business campuses, malls and streets/highways/lanes that are clearly named. Maps should be to scale. Label any "extra" buildings such as garages and sheds, as well as railroads, road hazards, hills and any other structures in the immediate area of these facilities that should have attention called to them.
- ▶ Indoor and outdoor photos of all buildings in these business or academic complexes.
- ▶ Map and directions to primary and secondary staging locations, as well as areas to observation posts, for law enforcement, fire and EMS personnel.
- ▶ Aerial photos of landing zones, if possible, for medevac helicopters.
- ▶ Maps of security gates, barriers, etc. and procedures for gaining entry if organizations' personnel are not available.
- ▶ Directions to evacuation locations (the site evacuation location is the non-tactical location a school/site should generally already have in place for earthquake, fire, etc.
- ▶ Instructions on evacuation routes from the north, east, south and west to the site evacuation location. Each direction is needed in case of chemical spill, advancing fires and other disasters influenced by wind conditions or additional factors.
- ▶ Updates with recent construction, building closures, roadwork or other factors that might make rooms, facilities, streets, etc. inaccessible.

- ▶ Contact names (with daytime and emergency contact information) of C-level executives, administrators, principals, facilities managers, custodians, on-site security staff directors, on-site crisis coordinators and property managers.
- ▶ Contact information for resources that may not be technically considered emergency response, but could have a role to play, such as utility companies or the transportation company that handles school buses.

### **Technology considerations for end users**

At the scene of a crisis is where the technology rubber meets the road. Some of the technology components you can control, while others are literally in the hands of constituents directly impacted by the crisis. Here is where the KISS factor – Keep It Simple, Stupid – comes into play. Develop plans that make the most of the common technology denominators that encompass the greatest number of people.

#### *Emergency responders*

For first responders and other government employees involved with crisis response, technology requirements are dictated in part by other applications and tasks for which these workers use their mobile devices. Some may carry more than one device, but as long as one of them supports WiFi and IP communication, interoperability between departments and agencies should be assured. Here are some basics to keep in mind.

You should have mounted laptops inside vehicles since, during travel time, personnel other than the driver need to access and easily view documents heavy with graphics, plus video feeds coming from the crisis scene. Upon arrival these laptops may need to be removed and carried around the scene, so ruggedized devices are best.

Tablet PCs are preferred options by workers who have to record information while doing their jobs, and tablets allow people to carry the devices while using only one hand to write or otherwise trigger applications, enter data etc. These should run VoIP software to enable users with headphones to make calls. For even more flexibility, properly configured smartphones with VoIP capability do the same thing, have basic computing and data access capabilities, are more convenient to carry and can be used hands free with headsets and software that responds to voice commands.

Mobile access points should also be in the mix, mountable inside vehicles and transportable so personnel can place them as needed at the crisis scene. Morrow County has 40, which cost about \$4,000/device. Equip workers' mobile devices so they can use Bluetooth or other technology to link to each other. Even if they are in areas where the muni network can't provide coverage, individuals can at least link with each other.

### *Executives, administrators and the crisis response team*

Whether the crisis involves a business park, university campus, the mall or high schools, it helps tremendously if senior executives, administrators and in-house crisis teams are equipped with technology to manage and direct the crisis response from within the constituent organization(s).

Everyone in this category should have a WiFi-enabled smartphone with VoIP capability to give them maximum communication options. Load these smartphones with a streamlined version of the crisis response and communication plan(s), key contact information for executives, managers and the Web staff, plus passwords and log-on procedures for the organization's intranet. In essence, everything needed to manage crisis response and interact with first responders from wherever individuals in this group happen to be.

Smartphones for some or all of your crisis communication staff should have a digital camera and video streaming features. Depending on the nature of the crisis, they may be able to capture and feed initial images to emergency responders. In addition, this team should have WiFi-capable laptops. People may need to write lengthy e-mails and documents, transfer files to the intranet or Web site or conduct video conferences which can be a slow tedious process using smartphones.

### *The organization's intranet*

From an internal infrastructure perspective, the organization's intranet is the most important element after the wireless LAN since this is where you can post information that is important but less critical than what you would push directly to workers, students, etc. This is also where you can direct people when you text or instant message them.

A secure intranet can be your best tool for coordinating your team, and an off-site backup for it many miles away is your best insurance to be able to weather any crisis that comes your way. In fact, consider having a backup of your public Web site (or at least the press center) in the same place, and an outside PR firm that can handle the mechanics of uploading new documents and keeping the online resources humming.

Make the intranet a central repository where press releases, messages from the CEO (president, dean), progress reports and other important materials can be quickly accessed, reviewed and approved. Use this site to inform employees, students and others, calm their anxieties and give your mobile workers an extra communication line.

If you decide to create a backup off-site intranet, whether hosted on your own equipment or by a service provider, determine at the outset of a crisis which intranet will be your primary site. The primary intranet is where all of the document management takes place, and the secondary intranet should only hold final versions of all documents including a dark Web site if you have one. Of course, if this proves to be unwieldy, just go with the one intranet. Once the crisis is over, archive all of the documents since you never know when you will need these again

Consider having several discussion boards on the intranet just for crisis communication. One should be for senior executives or administrators in case they want to create a threaded e-mail discussion with just the management team and key department heads. The organization's crisis communication and response team should have its own. This tool could be useful beyond managing the crisis to keeping the organization itself running during situations in which executives may not be able to get back to the office soon and other forms of communication are uncertain.

## **IV. In the final analysis**

---

The Wall Street Journal article I referenced earlier (**For Two US Cities, The Debate Over Spectrum Is Over**) sums it up best:

“As debate on Capitol Hill and the Federal Communications Commission continues on how to improve communications systems for police and firefighters, some parts of the country are tired of waiting... the time for talk is over.”

We’ve watched enough major natural disasters, shootings, train derailments and other high-profile accidents to clearly understand that every municipality and region is subject to crises for which governments and citizens are not properly prepared. Technology exists that can make us significantly better prepared to deal with the realities of our world, but do we have the vision and the political will to make change happen

### **Reality check**

It warms my heart to see the recent events in which leading vendors have put local governments on notice that there’s really isn’t a free lunch when it comes to municipal wireless. These networks cost money and cities have to step up to the plate to directly or indirectly provide funds to make these projects happen.

It’s time to move past viewing these network projects as an avenue for politicians to promise the equivalent of a “chicken in every pot” and see them for what they really are – serious infrastructure as vital as highways, water and electricity. In the context of crisis response, lives may literally come to depend on it. Is this something you want built on the cheap? Is it in the best interest of your citizens to have the network owned and managed entirely by an entity that has to make a profit on the use of that network?

The building of municipal networks must not be made the centerpiece in some harebrained ad gimmick, nor a resource under the sole control of entities whose ultimate allegiance is to stockholders and profit margins. If a vendor or service provider decides to stop running the network or limit areas where it operates because they’re not making a profit, you and your citizens will be left vulnerable.

If cities are going to be a customer of infrastructure, be a strong customer with leverage to demand and get the quality product you need. If municipalities are to be the public partner with private companies, than be a real partner with a management role by bringing real (read: money) assets to the party. Adequate crisis response is not a nice-to-have; it’s a must-have. Lives are at stake here!

### **Show me the money – it's everywhere**

Some municipalities have squandered valuable time they could have been advancing the types of crisis response solutions described here because they were seduced by the chimera of "free." Or paralyzed by the "We Have No Money" blues. Folks, it's time to zip up, buck up and stop crying the blues.

The U.S. government is waving billions (seriously!) of dollars around waiting for people to come to them with plans for helping local and regional governments create interoperable communication to respond to crises and natural disasters. The Justice Department has money for improving the effectiveness of local law enforcement agencies.

If politicians chasing freebies in 2006 spent as much time chasing grant money, they'd be able to pay for these networks. What's \$10 million to an agency holding \$1 billion in funds? Though they're rarely in the news, there are cities that used these funds to build public safety networks. Find them. Talk to them. They'll tell you how to get it done.

In addition to grants, talk to the biggest companies in your city or county. After the Trade Center disaster, many executives are acutely aware that effective crisis response is definitely in their best interest. Ask your business community who's willing to stand up and contribute financial and technology resources to the muni network. There'll probably be some takers. But if you don't ask, how will you know?

Government use of municipal networks offers governments significant opportunities to cut costs, improve operations and in the area of crisis response, save lives and property. There is an ROI (return on investment) here that can help you get the money you need, particularly when cities take a broader view of the financial picture. One city I did a workshop for said "we probably can't afford to pay for the whole thing, but if we can find other sources for \$3 million, we might be able to justify the other \$1.5 million with all the benefits the city can receive?"

If you have a good vision, money becomes the lesser challenge. The bigger challenge is actually people.

### **This is a teams effort**

That is not a typo. Besides a management team to drive the overall crisis response project, implementing the kind of plan outlined in this report requires teams of people in various sectors of government and among constituents. Unfortunately, this threatens to be the fatal Achilles heel. You're going to need a bunch a carrots and a massive baseball bat to meet this challenge.

For a goal as compelling as more effective crisis response, it's amazing how many great ideas are derailed by turf wars, budget wars, an unhealthy FUD factor (Fear, Uncertainty & Doubt) and plain ole spitefulness. Whether between cities and counties or departments within the same government, these challenges await you. So prepare to deal with them from the start.

From the get-go, be committed to finding common ground. You may have to be content with cooperation that's no more than the different departments agreeing to use devices that support IP, with no consensus possible on personal hardware. Private businesses may only agree to use in-house video cameras if they are linked directly to the city network, but won't allow you access to their networks. Maybe you have to build a separate public safety network to get law enforcement buy-in.

Whatever the politics of your hometown or county, keep your eye on the prize of getting multiple teams pulling together over some common ground to achieve the common good. Once you flesh out and get commitments to technology and tactics that can integrate various stakeholders' efforts, build from there. Once the network is in place and one or two main applications are in place, you should be able to build on this with additional technologies and applications.

### **The seven P's are critical**

In high school, one of my teachers drilled into our brain the seven P's: proper previous planning prevents pitifully poor performance. Nowhere is this truer than with municipal wireless and crisis response. To reach the full potential outlined in this report, you can't get there from here without clear plans. They don't have to be long, elegantly worded documents, but they do need to be comprehensive, logical and spell out tactics in a straightforward manner. In other words, the antithesis of most government plans.

Planning by committee is never easy, but here are some steps to help. It took delegates only four months to write the U.S. Constitution, so there's precedence for expedient writing of a significant government plan.

- ▶ Have one main cat herder with just a couple of assistants (this is the type of project for which the phrase "herding cats" was invented);
- ▶ Divvy up and assign responsibility for sections of the plan to the teams from departments and constituent groups who will contribute to, or be affected most by, respective parts of the plan;
- ▶ Select someone from each team with good cat herding experience to head up their efforts;
- ▶ Chose the person on each team to write their part of the plan who lives and dies for brevity;
- ▶ Integrate the main cat header with the task force, committee, consultant or whomever is doing the needs assessment and developing the RFP for the muni network;
- ▶ Set an aggressive timeline for plan completion and give someone power to hold people to these;
- ▶ Make sure there's a clearly written vision statement, description of common ground and succinct layperson's glossary of the technology involved in crisis response that serves as the bible to guide every team; and
- ▶ Follow basic business 101 rules for planning.

## V. Conclusion

---

This Snapshot Report, of course, is a somewhat cursory look at what is a complex, multi-faceted exercise. But I think you get my bottom-line that planning is critical to success and this report starts you in that direction. More important is the fact that crisis response is something too many local, regional and federal government departments are not prepared to adequately address, and something must be done.

Now is the time to harness the intense efforts in Congress to address communication interoperability, as well as the widespread drive by governments to build municipal networks. Entities are moving in various directions, but with one common goal – create a technology infrastructure that serves the best interest of constituents. Unfortunately, as the 70s song made clear, communication is the problem to the answer. We need more people on the same page.

There are some common technologies available that can help us reach the promise land of greatly improved crisis response and communication. But we have to help a lot of people locally and nationally reach common ground on the way to get there. Municipal wireless represents one clear patch of that common ground.

## For more information

---

### **About the author**

For 20 years Craig Settles' consulting services, books and workshops have helped organizations worldwide understand how to use technology to make money, save money and run a better business. Mr. Settles authored *Fighting the Good Fight for Municipal Wireless* and several in-depth reports ([www.successful.com/snapshot.html](http://www.successful.com/snapshot.html)) to help local governments better plan muni networks. His next book tackles piloting and deploying government and business mobile applications.

To get more information about ***Fighting the Good Fight for Municipal Wireless*** go to [www.successful.com.fgfsummary.html](http://www.successful.com.fgfsummary.html)

Find out how you can get valuable on-site workshops to help your department managers and IT develop the business case for municipal wireless and for mobile government workforce applications. Visit <http://www.successful.com/workshops.html>.

### **About the sponsor**

#### **Northrop Grumman**

Northrop Grumman Corporation is a \$30 billion global defense and technology company whose 122,000 employees provide innovative systems, products, and solutions in information and services, electronics, aerospace and shipbuilding to government and commercial customers worldwide.

To learn more about Northrop Grumman municipal wireless solutions, we invite you to visit [www.northropgrumman.com](http://www.northropgrumman.com).

### **Don't miss the next great report**

Visit [www.successful.com/snapshot.html](http://www.successful.com/snapshot.html) to get copies of Craig Settles' previous Municipal Wireless Snapshot Reports. Call 510-536-4522 or e-mail [craig@successful.com](mailto:craig@successful.com) to be notified about future reports. Your feedback is always welcome, as well as suggestions for future topics.