Federal Communications Commission

700 MHz Public Safety / Block D Proposed Spectrum Management Plan Response to FCC 08-128

WT Docket No. 06-150

PS Docket No. 06-229

(360) 584-7900
www.ComCentricUSA.com

(206) 686-6543
www.icongroupe.com

June 20, 2008

June 20, 2008

Kevin J. Martin
Chairman
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Dear Mr. Martin,

The following pages constitutes our response to Dockets No. 06-150 and 06-229 in the matter of the 700 MHz Block D / Public Safety Spectrum Management Policy. The purpose of this document is to provide the FCC with an alternate proposal for constructing the National Public Safety Broadband Network.

The owners of ComCentric have served our country as first responders and emergency communicators, and we have recruited the nation's most experienced engineers and computer scientists to develop the National Public Safety Broadband Network.

The 700 MHz spectrum presents our generation with a once in a life time opportunity to solve the nation's interoperability problems and quickly build a national response to imminent threats. We can not afford to let this opportunity slip away. Thank you for your consideration.

Please contact Mark Gilbaugh at 360-584-7900 for any question concerning this proposal.

Sincerely,

Mark Gilbaugh
President
ComCentric Inc.

Table of Contents

1. Executive Summary **1**

2. Network Requirements **4**

2.1 Network Speed
2.2 Network Coverage
2.3 Network Reliability
2.4 Network Hardening
2.5 Network Security
2.6 Network Prioritization
2.7 Network Efficiency
2.8 Network Sensors
2.9 Customer Devices
2.10 Public Notification
2.11 Physical Security

3. 700 MHz Spectrum Management Plan **6**

3.1 IP Based Communications
3.2 Spectrum Management

4. Financing the Network **11**

5. Key Personnel Biographies **12**

COMCENTRIC

1.0 Executive Summary

Recent natural disasters and acts of domestic terrorism have demonstrated that our country requires a national broadband public safety network. Implementing additional narrow bandwidth solutions and patching together legacy land mobile radio systems constitutes a Band-Aid solution and fails to solve the fundamental problems associated with achieving a national response to imminent threats.

Paradigm Shift

In order to secure the homeland and resolve the nation's interoperability problem, leaders at every level must experience a paradigm shift from a centralized system with individual channels to a distributed system with a broadband packet switched network.

Public Safety communications systems currently deployed are based upon the P-25 digital trunking radio standard. These systems utilize narrow channel spacing to deliver more channels and time domain multiplexing to accommodate additional users. As with legacy Time Domain Multiple Access (TDMA) cellular systems, history demonstrates that network operators will eventually exhaust the finite resources of time and frequency spectrum.

In the 1960's Paul Baran developed packet switched networks which were the fundamental building blocks utilized in the ARPANet architecture and which now fuel the Internet. Baran's theory was not appreciated during that era, but distributed switched packet networks are the basis for modern data communications and have withstood the test of time.

In order to achieve optimum spectrum efficiency and provide the network redundancy required by the public safety community, land mobile radio must also transform from circuit switched type network to a packet switched network. The 700 MHz public safety spectrum offers our nation a once in a lifetime opportunity to build a new type of land mobile network which will be used to form a national response to natural and man made threats.

700 MHz Spectrum Management Plan Recommendation

ComCentric believes that the 4G public safety network will require additional frequency spectrum and therefore recommends that the FCC allocate the entire 34 MHz of the Public Safety and Block D 700 MHz spectrum towards such a nation-wide infrastructure design. Such an allocation would allow the 4G/IP based architecture to create non-overlapping channels operating within a self-healing mesh configuration allowing it to provide redundant and ubiquitous coverage while providing data rates greater than 1 Mbps to the network edge.

The ComCentric engineering and information assurance teams have developed a comprehensive data management and communications plan designed to create the new 4G self-healing network systems architecture.

Financing the Network

The nation wide network built to public safety standards is expected to cost more than $20 billion. ComCentric has partnered with the Icon Groupé and expects to pay for the network through a combination of outdoor advertising and network user subscriptions.

Uniformed public safety officers and their direct support are the primary users of the network. Secondary users of the network should be utility and transportation workers. These personnel are instrumental in responding to a national threat and must be accessible from the national network. This strategy increases the effectiveness of the incident commander, increases the network efficiency, and broadens the subscription base. Network prioritization and quality of service will ensure that first responders will have priority access to network resources.

Our public / private partnership exchanges broadband connectivity for space on public property. This strategy provides participating cities with the benefits of digital signs for public transportation schedules, traffic reports, amber alerts, and emergency notification while advertisers reach their target audience.

Snohomish County Broadband Pilot Project

In 1999, Snohomish County, Washington created the Snohomish Emergency Radio System (SERS) and has pooled resources in order to build a $34.2 million, 800 MHz trunking radio system. This system has 23 towers and services 9 law enforcement agencies, 27 fire fighting agencies, 2 E-911 Dispatch Centers, the Snohomish County Department of Emergency Management, and the County Medical Examiner.

In 2006 SERS decided to extend their services to include broadband data, and they issued a request for proposal for a pilot project utilizing existing commercial technology. ComCentric was awarded the contract for the Snohomish County Regional Interoperable Wireless Data Pilot Project in 2007. This pilot project allows first responders to seamlessly roam between municipal Wi-Fi, EV-DO, and private radio networks while providing network security.

700 MHz 4G Pilot Project

ComCentric proposes that Snohomish County be utilized as the testing facility for the 700 MHz National Public Safety Broadband Network Pilot. ComCentric has been granted access to 23 modern tower sites with redundant microwave backhaul links and the Icon Groupé has offered access to their 21 outdoor media signs already constructed in the county.

According to “Why We Can’t Talk” written by the National Task Force on Interoperability, the greatest challenge to Interoperability is not technology, it is politics. The Snohomish Emergency Radio Service has demonstrated that they can manage the local political situation and force over 40 public safety agencies and over 8,000 network users to work together while sharing public safety resources.

Public Safety Spectrum Licensee

ComCentric believes that the Public Safety Spectrum Trust represents the interests of the first responder community. This agency should be kept in place as the Public Safety Spectrum Licensee and as a non-profit oversight committee to work hand in hand with the network operator.

The agencies operating expenses should be covered by a percentage of network subscriptions. This strategy ensures that the licensee is financially compensated for building the network that meets the needs of first responders and leverages their position in the public safety community to recruit new departments to the network.

ComCentric's Qualifications

ComCentric is a veteran owned business located near Olympia, Washington. The owners have served their community as first responders and emergency communicators for FEMA, WA State Emergency Management Department, and routinely provide emergency communications equipment and support to the US Forest Service for wildland fire fighting. Our staff has an extensive history of emergency response and assisting with natural disasters.

ComCentric is dedicated to providing the finest unified command, control, and interoperable communications system to protect and serve those who protect us, the first responder and to support the requirements of the Department of Homeland Security. ComCentric has recruited some of the nation's premiere engineers and computer scientists to design and build the nation's next generation public safety broadband wireless network.

Icon Groupé Qualifications

The Icon Groupé is the fastest growing outdoor media company in the nation headquartered in Seattle, Washington. The Icon Groupé is a privately held corporation with over 1,200 media outlets in major markets across the country. The company is owned by some of the most experienced former advertising executives from Clear Channel Outdoor and The Ackerly Group.

The Icon Groupé is pioneering the concept of providing technology for first responders in exchange for advertising space on public property. The company has initiated a Green policy and is a leader in the development of energy saving and aesthetically pleasing technologies.

2.0 Network Requirements

Cellular networks will not provide the level of redundancy, reliability, and security required for Public Safety networks. The 700 MHz Public Safety Wireless Network should be based upon 4G technology implemented in a wireless mesh architecture with microwave / satellite backhaul and ad-hoc support to produce an entirely redundant network.

2.1 Network Speed

The Public Safety Wireless Network should deliver a minimum of 1 Mbps data transfer speed at 5 miles in a handheld to base station, line of sight environment. The use of vehicle mesh radios and automatic gain control should extend the portable radio over 8 hops and 100 miles while conserving battery life and network congestion.

The network core should be based upon a fiber mesh backbone with a minimum network speed of 10 Gbps. On top of the fiber backbone, an Ethernet microwave mesh backhaul should be built to interconnect towers at a minimum speed of 100 Mbps. From the main tower sites, the 700 MHz mesh should provide coverage directly to the public safety officer and their vehicle with minimum speeds of 1 Mbps.

2.2 Network Coverage

The Public Safety Wireless Network should deliver a minimum of 98% of the population with terrestrial links and 100% of the geographic area with “in motion” satellite connectivity for rural public safety officers.

2.3 Network Reliability

The Public Safety Wireless Network should deliver a minimum of 99.9% reliability based upon mesh architectures at the backbone, backhaul, and distribution layers.

2.4 Network Hardening

The Public Safety Wireless Network should be built to be environmentally friendly and utilize green power. The sun generates 86,000 terawatts and the wind generates 870 terawatts of power, and this energy should be utilized as the primary power source for each tower site with grid and generator backup. Solar and wind energy will power the Public Safety Network indefinitely during grid shortages and blackouts.

2.5 Network Security

The Public Safety Wireless Network will be a national asset and should be built as a totally private network with no physical connection to the Internet, and a minimum of 128 bit AES encryption should be utilized for network traffic.

The Public Safety Wireless Network should utilize biometric keys for customer device access to enable a combination of hardware and software security.

2.6 Network Prioritization

The Public Safety Wireless Network should be built with at least 20 levels of automatic network prioritization. When networks are stretched to their limits, transportation workers and users outside of public safety will automatically be limited access. This removes the need to activate an emergency mode or the requirement for a presidential directive.

2.7 Network Efficiency

The Public Safety Wireless Network should implement automatic channel selection, dynamic channel spacing, and automatic gain control to maximize spectrum efficiency, optimize network speeds, and ensure total customer satisfaction.

2.8 Network Sensors

The Public Safety Wireless Network will deploy towers and connectivity across the country and should provide biological, chemical, and nuclear weapon sensors for use by Emergency Operations Centers and the Department of Homeland Security.

2.9 Customer Devices

The Public Safety Wireless Network should offer comprehensive Land Mobile Radio over IP devices with long run times for uniformed officers and small phone devices for administrators, under cover officers, and volunteer fire fighters.

Satellite equipped handsets are only usable outside and are rendered useless inside buildings. Mobile vehicle radios should act as repeaters for portable radios and satellite uplinks should be installed in a percentage of vehicles from each department to provide a redundant backhaul link for the self healing wireless mesh.

2.10 Public Notification

The Public Safety Wireless Network should be built with the ability to incorporate public notification systems as an extension of the Emergency Broadcasting System. This system should include GiantVoice systems and digital signs to support emergency notifications and evacuation routes.

2.11 Physical Security

Physical security for the network should be a primary concern and alarms and video cameras should be deployed at each site for instant notification of an intruder.

Technicians working on the network should be thoroughly screened and should be required to obtain a Secret security clearance. Any technician unable to obtain a clearance should not be allowed un-escorted access to any facilities.

3.0 700 MHz Spectrum Management Plan

In 1996, the Public Safety Wireless Advisory Committee (PSWAC) advised the FCC that by 2010, an additional 97.5 MHz of frequency spectrum would be required by the Public Safety community. In addition to the 50 MHz of 4.9 GHz spectrum previously licensed, 24 MHz of the 700 MHz has been allocated for public safety leaving a deficit of 23.5 MHz.

National Threat Analysis

The bombing of the Murrah Federal Building and the terrorist attacks of September 11th have highlighted the largest problem to ever face the first responder community, Interoperability. The inability of first responders to communicate between agencies has resulted in the loss of property and lives, and until this problem is solved, we will continue to pay the price.

During Hurricanes Katrina and Rita this problem was once again brought to the forefront. First responders from all over the country rushed to the aid of those who were trapped, but each individual agency maintains their own communications systems. The lack of integrated communication between agencies made these disasters worse by limiting critical aid.

After Hurricane Katrina, almost 3 million customer telephone lines and 1,000 cellular telephone sites were out of service. These cell sites require weeks to engineer and configure. After three weeks, only 60% of the cell sites in New Orleans were back in service. First responders need their systems operational and do not have time to wait for system repairs.

Many first responder agencies have started transmitting emergency communications over internet virtual private networks to reduce costs. While VPN tunnels provide security, the internet provides no assurance for connectivity or quality of service. The Slammer worm attack of January 2003 infected 75,000 hosts in less than 10 minutes, and the effects to internet traffic were far greater than the Baltimore tunnel train wreck which destroyed a critical fiber link.

To date, domestic terrorism has only yielded small attacks on specific targets. The worst case scenario would include simultaneous physical and information attacks. This would not only leave the country devastated, but would leave us without the means to communicate.

3.1 IP Based Communications

Modern Public Safety communications are based upon digital trunking radio. This system utilizes narrow channel spacing to deliver more channels and time domain multiplexing to accommodate additional users. As with legacy Time Domain Multiple Access (TDMA) cellular systems, the network operator will eventually exhaust the finite resources of time and frequency spectrum.

In order to combat the nations' impending threats and resolve the interoperability problem, leaders at every level need to embrace the transition from

individual narrow channels to broadband packet switched networks. This change in mind-set from inefficient narrowband networks to 4G packet switched networks will provide nation-wide broadband service utilizing 34 MHz in the 700 MHz spectrum.

Opposition to Technology

Premature IP telephony deployments by companies such as Vonage and Packet8 have created many objections to Voice over IP communications in the first responder and E-911 dispatcher communities. These initial services did not provide automatic number identification, automatic location information, packet prioritization, or quality of service optimization. Call takers and dispatchers were forced to manually enter phone number and location information while overcoming poor call quality. These barriers have slowed down the 911 dispatch process and we may never know how many lives have been lost.

Digital cellular phones have also created a mistrust of commercial communications systems, and first responders are reluctant to rely on cellular communications. Legacy analog cellular systems were large and bulky, but would transmit up to 20 miles with high power transmitters. In the quest for smaller appliances, the battery capacity and power output of modern cell phones have been reduced significantly. While consumers accept dropped calls as an inconvenience, lives hang in the balance when first responders are faced with lapses in coverage.

Benefits of IP Based Communications

Properly engineered Voice over IP (VoIP) and Radio over IP (RoIP) systems provide quality of service, traffic prioritization and redundancy with a 99.999% guaranteed uptime. Since communications are totally IP based, traffic may be sent over satellite or terrestrial links, and systems may be hosted on redundant servers spread out across the country.

Wireless communications systems rely on radio towers and tall buildings to project network coverage. IP based systems operate over multiple back haul transport media and satellite "comms on the move" technology should be utilized to supplement terrestrial links. Installing "in motion" phased array satellite uplinks on SUVs allows search and rescue operations and officers traveling in rural / wilderness areas not normally covered by radio networks to bring the wireless coverage with them. Additionally, satellite equipped vehicles provide alternate backhaul links and automatically repair sections of a damaged wireless network.

The State of Vermont recently implemented the first IP based E-911 system. Their private network consists of 10 Public Safety Answering Points with automatic traffic routing, and redundancy. Each of the 10 sites have the ability to dispatch calls to agencies across the state providing overlapping coverage. The state was reluctantly forced into the technology, but is now very satisfied with the current deployment.

3.2 Spectrum Management

ComCentric proposes that all 34 MHz of Public Safety and Block D frequency blocks be utilized to build the IP based public safety broadband network. Data rates greater than 1 Mbps will be achieved by dividing the 34 MHz of available frequency spectrum into 1.25 MHz / 2.5 GHz 4G channels arranged in a mesh architecture.

ComCentric proposes that all legacy narrowband operations be performed in existing public safety spectrum and that no new licenses be issued for narrowband operation in the 700 MHz spectrum.

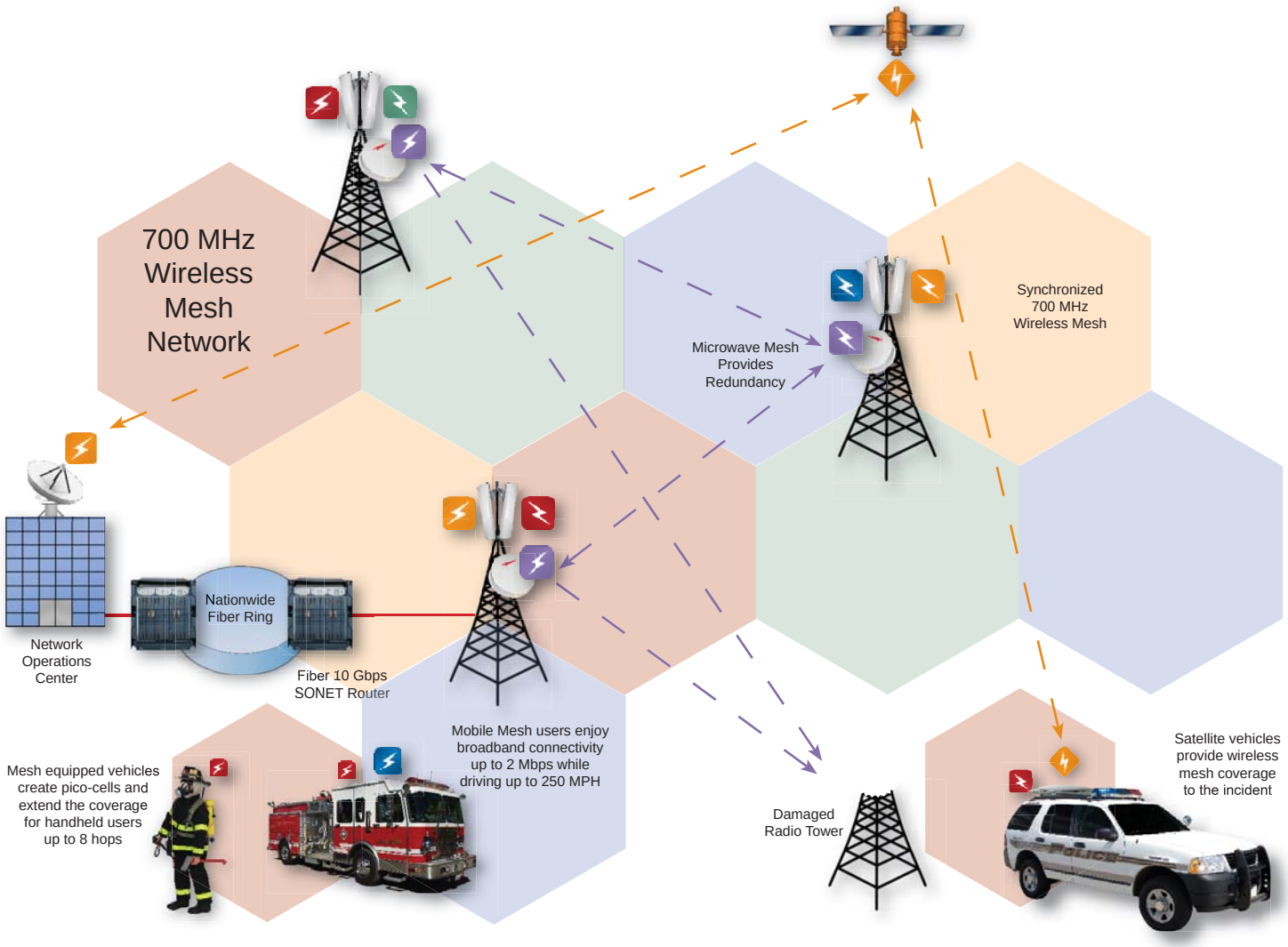


Figure 1- Public Safety Wireless Network utilizes 4G technology in a mesh architecture to provide redundancy and resiliency. Satellite "Comms on the Move" technology provides network access to remote locations as well as an alternate backhaul link to restore damaged infrastructure.

P-25 Communications Standard

The Association of Public Safety Communications Officials (APCO) has established the Project 25 standard for digital interoperable communications. While many states have started to implement state-wide P-25 compatible radio projects, others have discovered that the goal is actually cost prohibitive and only provides limited data capabilities.

Washington State has started planning a state-wide P-25 compatible radio system that is expected to cost $905 million and will not be completed until 2015. This system is expected to serve the Washington State Patrol, the Department of Natural Resources, and the Washington State Department of Transportation.

The Oregon State Legislature recently voted against a similar $665 million state-wide P-25 compatible radio system stating that the system was too expensive for the capabilities provided. Oregon is now searching for alternative technologies.

In order to fight the domestic war on terrorism and provide true interoperability during natural disasters, first responders require broadband data capabilities.

P-34 Communications Standard

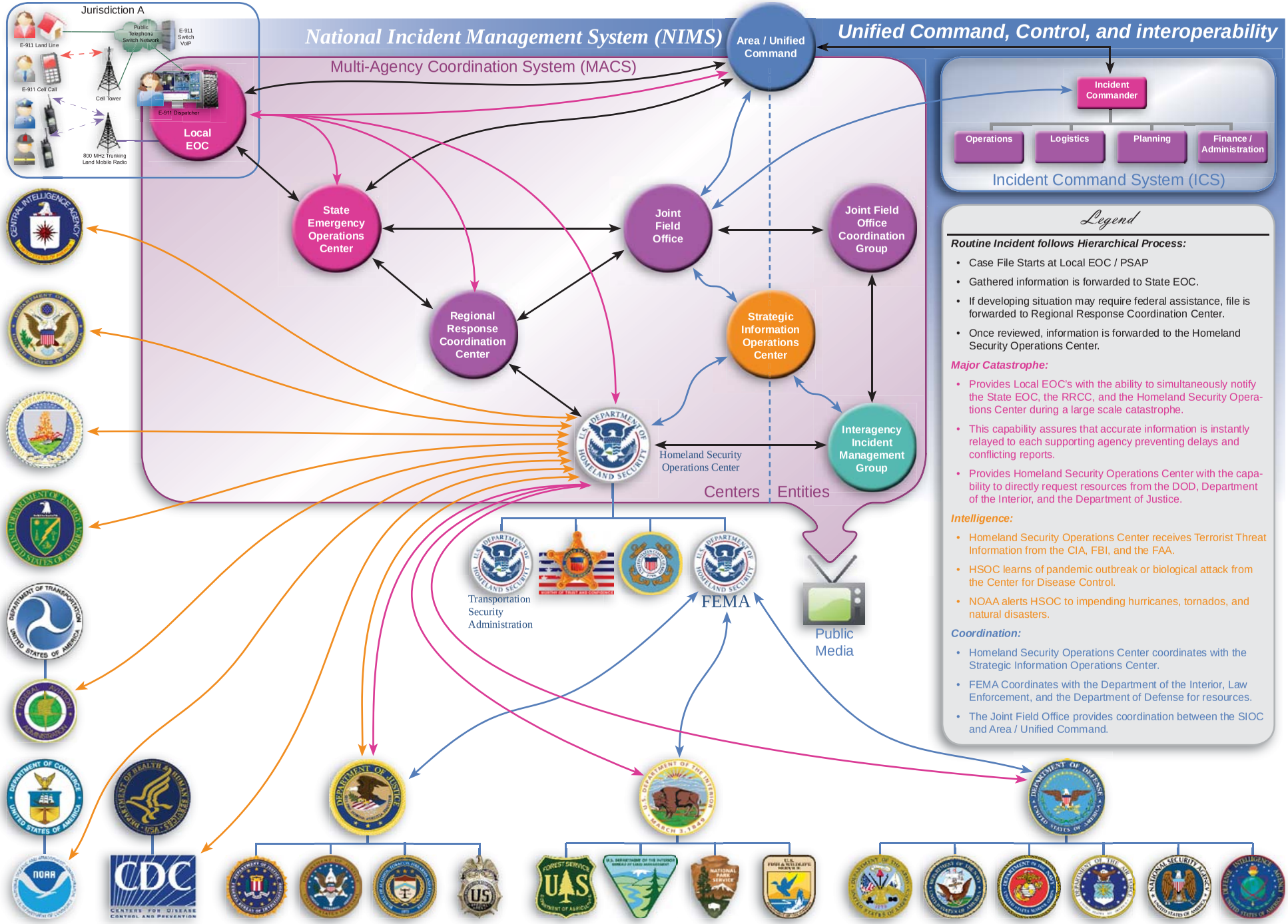
ComCentric believes that a 4G Radio over IP system must be implemented to meet the future needs of first responders beyond the Project 25 standard. APCO has also established the P-34 standard for the Wireless Transport of Rate Intensive Information, and the Public Safety Wireless Broadband Network will provide both the voice and data capabilities required by first responders. ComCentric foresees that all emergency communications and intelligence gathering capabilities will be merged into one network for true interoperability.

This revolutionary handset will replace the cumbersome radio, direct connect cell phone, and Personal Alert Safety System (PASS) devices currently worn by EMT's, police officers, and firefighters

National Incident Management System

The Public Safety Broadband Network must integrate with the National Incident Management System to quickly organize a national response to man made threats and natural disasters.

ComCentric proposes a comprehensive data management and communications platform, to meet the future needs of first responders. ComCentric anticipates that the system will be the visualization and collaboration tool which links legacy and future systems to provide Incident Commanders with the information that they need, facilitate interoperable communications, and manage incident resources.


Jurisdiction A
E-911 Land Line
Public Telephone Switch Network
E-911 Switch VoIP
E-911 Cell Call
Cell Tower
E-911 Dispatcher
800 MHz Trunking Land Mobile Radio
Local EOC
National Incident Management System (NIMS)
Multi-Agency Coordination System (MACS)
Area / Unified Command
Unified Command, Control, and interoperability
Incident Commander
Operations
Logistics
Planning
Finance / Administration
Incident Command System (ICS)
State Emergency Operations Center
Joint Field Office
Joint Field Office Coordination Group
Regional Response Coordination Center
Strategic Information Operations Center
Interagency Incident Management Group
Homeland Security Operations Center
Centers
Entities
Transportation Security Administration
FEMA
Public Media
Legend
Routine Incident follows Hierarchical Process:
Case File Starts at Local EOC / PSAP
Gathered information is forwarded to State EOC.
If developing situation may require federal assistance, file is forwarded to Regional Response Coordination Center.
Once reviewed, information is forwarded to the Homeland Security Operations Center.
Major Catastrophe:
Provides Local EOC's with the ability to simultaneously notify the State EOC, the RRCC, and the Homeland Security Operations Center during a large scale catastrophe.
This capability assures that accurate information is instantly relayed to each supporting agency preventing delays and conflicting reports.
Provides Homeland Security Operations Center with the capability to directly request resources from the DOD, Department of the Interior, and the Department of Justice.
Intelligence:
Homeland Security Operations Center receives Terrorist Threat Information from the CIA, FBI, and the FAA.
HSOC learns of pandemic outbreak or biological attack from the Center for Disease Control.
NOAA alerts HSOC to impending hurricanes, tornados, and natural disasters.
Coordination:
Homeland Security Operations Center coordinates with the Strategic Information Operations Center.
FEMA Coordinates with the Department of the Interior, Law Enforcement, and the Department of Defense for resources.
The Joint Field Office provides coordination between the SIOC and Area / Unified Command.
CDC

4.0 Financing the Network

The nation wide network built to public safety standards is expected to cost at least $20 billion. ComCentric and The Icon Groupé expect to pay for the network through a combination of outdoor advertising and public safety network user subscriptions.

The Icon Groupé is one of the early pursuers of the digital sign combined with public safety technologies. This type of sign adds value to the government while allowing advertisers to reach their target demographic. This strategy allows participating cities receive the benefits of digital signs for public transit schedules, traffic reports, amber alerts, and emergency notification while advertisers catch the eyes of their captive audience.

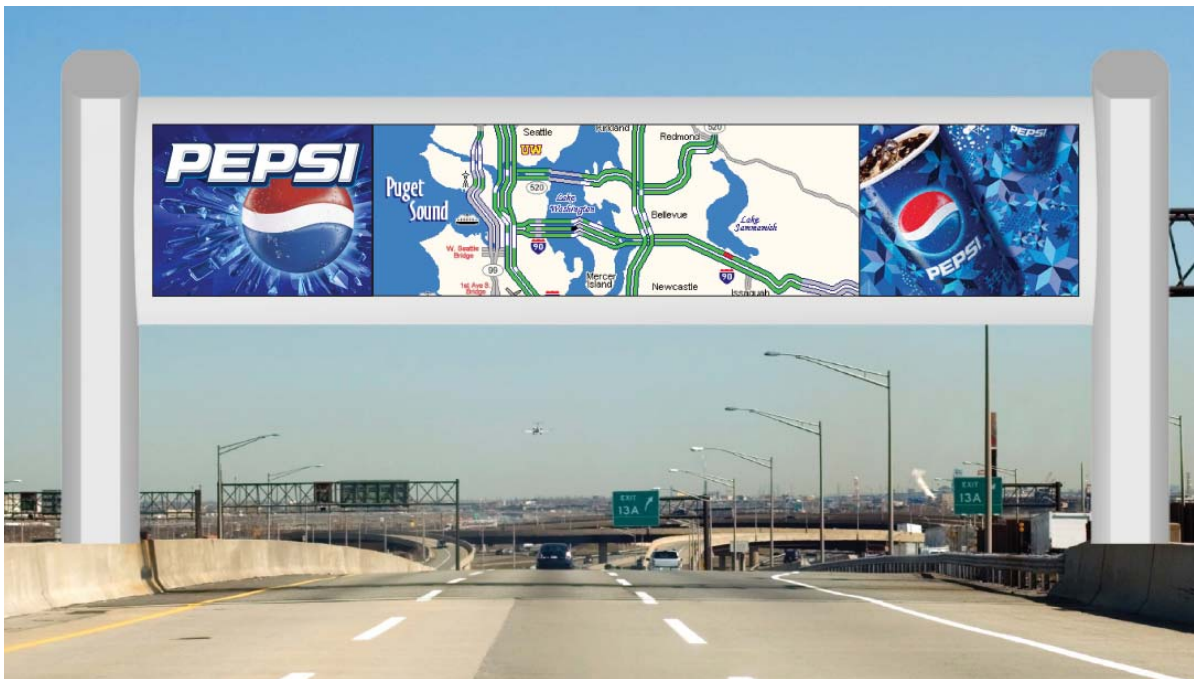


Figure 2- Public Safety Wireless Network incorporates digital signs for public notification

We propose that the Icon Groupé be granted permission by the Federal Government to build solar powered signs on public property in order to provide transmission towers and power necessary for the Public Safety Wireless Network while providing a comprehensive system for public notification. The Icon Groupé is currently engaged in negotiations for similar technology exchanges with cities across the country.

In order to increase the quality of total service and the subscription base, we propose that the public safety broadband network be opened up to all government agencies including Departments of Transportation, Departments of Forestry and Natural Resources, and Utilities. Placing all of these services on one network would provide comprehensive interoperability between departments and a broader subscription base.

5.0 Key Personnel Biographies

Mark Gilbaugh – President

During his career in the military, Mr. Gilbaugh achieved the position of Med-Evac Instructor Pilot in the U.S. Army having been deployed twice to Iraq and serving as a Med-Evac Team Leader, Information Management Officer, Communications Officer, and Military Assistance to Safety and Traffic (MAST) Frequency Coordinator.

Mark has over 12 years of experience in the telecommunications industry engineering networks and PBX telephone systems for state and federal government agencies to include the Tennessee Highway Patrol's E-911 system.

Bruce Gilbaugh – Vice President

Mr. Gilbaugh served as Deputy Chief for NASA's DARTCOM, an emergency communications support element located at Moffett Field, California. This team also supported FEMA's USAR Task-Force 3 in Menlo Park, CA. During his tenure at DARTCOM, Bruce deployed to Hawaii to assist in the rescue efforts after hurricane Iniki in 1991. In 2000 Bruce engineered, built, and deployed a mobile rover data communications test platform for NASA's Haughton-Mars Expedition.

Bruce holds a Masters degree in Telecommunications Management, and has held an FCC Amateur Radio Operator license since 1964. With over 20 years experience in the emergency communications industry, Bruce's emergency communications and project management experience is critical to the success of the Public Safety Broadband Network.

Jim Masten – Chief Technology Officer

Mr. Masten has over 30 years of experience in electrical, computer, communications and systems engineering. His experience in the design of data and communications systems includes computer architecture, ASIC, software and systems. Mr. Masten has a history of detailed design accomplishments that encompasses the systems integration of computer interface and control for such applications as video imaging and special sensor processing.

During his career, Mr. Masten has held the significant responsibility to lead the development of both products and technologies for two major international corporations. While at Honeywell, Mr. Masten led the corporate systems engineering technical review committee. Later at Alliant Techsystems, Mr. Masten provided personnel management and technical direction for the corporate embedded processor group. This group delivered specific embedded processor system designs across the corporation for applications such as the US Army mobile 155 howitzer, the Mark 50 Torpedo and the embedded processor systems for several classified video sensor processing applications.

Dawn Myers – Chief Software Engineer

Ms. Myers brings 26 years of experience in interactive systems design, development and management. Previously, Ms. Myers managed the software development group at Alliant Techsystems. In this position she led several special projects for a Navy customer. These projects required a formal analysis and system-design technique that was applied to a large command and control system. This system incorporated electronic, mechanical and human components. Ms. Myers demonstrated an expertise that was accepted by the Navy as valuable and necessary for a successful complex system design.

Ms. Myers had sole responsibility for the development of the first color user interface used onboard a U.S. submarine. She developed the color upgrade to the BQS-14 under-ice sonar and received a special award recognizing her contribution to the engineering challenge.

Guy McIlroy – Senior RF Engineer

Mr. McIlroy leverages over 20 years of experience in developing consumer wireless portable devices. Guy was one of the original wireless network pioneers and was the architect for the Apple Air Port and Apple Newton. He has also served as the Chief Technology Officer for RadioLAN and FreeRein as well as the Architect for Palm.

Guy has 7 patents issues and pending. His extensive experience hardware and software development, acquiring FCC certification, as well as taking products to market is critical to the success of the 700 MHz broadband network.

Earl Boebert – Security Consultant

Mr. Boebert is an expert on information security, with experience in national security and intelligence as well as commercial applications. Currently retired, he was a senior scientist at Sandia National Laboratories. He has 30 years experience in communications and computer security, is the holder or co-holder of 12 patents, and has participated in CSTB studies on security matters. Prior to joining Sandia, he was the technical founder and chief scientist of Secure Computing Corporation, where he developed the Sidewinder security server, a system which currently protects several thousand sites.

Before that he worked 22 years at Honeywell, rising to the position of Senior Research Fellow. At Honeywell he worked on secure systems, cryptographic devices, flight software, and won Honeywell's highest award for technical achievement. He served on the National Academy of Sciences committees that produced Computers at Risk: Computing in the Information Age; For the Record: Protecting Electronic Health Information; and Information Technology for Counterterrorism: Immediate Actions and Future Possibilities. He also participated in NAS's workshops on "Cyber-Attack" and "Insider Threat" and an NAS assessment of FBI data systems.