

Can You Hear Me Now?

Defining Operable Communications Systems

TABLE OF CONTENTS

- 2** A Capacity-Defined Solution Strategy
- 3** Setting the Ground Work
- 4** Tiered Solutions
- 5** Deployable Communications Systems Components
 - 5** BackHaul/Reach Back
 - 5** Local Area Connectivity
 - 6** Routing Capability
 - 6** Bridges and Gateways
 - 7** Client Devices
 - 7** Power and Transport
- 8** Success Stories:
 - Hillsborough County Sheriff's Office — Tampa, Fla., 2004
 - Hurricane Katrina Response: August/September 2005
 - Tennessee Tornado Response: February 2008

Executive Summary

Whether responding to an everyday emergency or recovering from catastrophic disaster, it's nearly impossible for first responders to achieve interoperability if their communications infrastructure is inoperable. Recent events in American history, from natural disasters to acts of terrorism, have heightened an intense interest in finding ways to shore up the nation's communications infrastructure.

At the same time, state and local government have faced their own challenges in coordinating resources to help first responders to an emergency scene help citizens and restore necessary infrastructure. Too often, teams are unable to communicate with each other in a timely and coordinated fashion, delaying aid and potentially costing lives.

This white paper was developed in order to aid state and local government first responders in planning for and selecting deployable communications technologies utilized in response to catastrophic disasters and everyday emergencies. In addition to tactical use by first responders, the white paper can be of assistance to all government agencies, non-governmental organizations and the private sector with respect to improving communications capabilities necessary for a rapid return to normal following a disaster.

.....

A Capacity-Defined Solution Strategy

It is no secret that information technology has risen to the forefront in investments to ensure a safe public future. With national priorities centering on the need to be interoperable — the need to share information and the need to better align perceptions with reality — it is clear that information technology plays an ever increasing role in combating the 21st century threat environment. Much has been written about interoperability, but the concept isn't new. First introduced during action reports following the 1906 San Francisco earthquake and fire, the term re-emerged in 1935 at a meeting of communications professionals serving public safety.

In the past, communications solutions were developed to support specific and separate response functions. The bomb squad brought what they needed, hazmat teams had their solution and hostage negotiators offered yet another tactical deployable communications package. From federal government down to the local level, deployable communications — the strategic coordination of secure, mobile and deployable tactical communications — is now considered the most effective way to help communities in crisis.

“Organizations must take a broad view,” explains Allen Kniphfer, emergency manager for Jefferson County, Ala. “If you focus on the terrorist threat, you are missing the bigger picture and your emergency communications system will continue to fail in other situations. Emergency communications needs to be looked upon as an all-hazards system, because it is the other hazards that your emergency communications system will be used for most of the time.”

Don Sarginson of the Hillsborough County Sheriff's Office (HCSO) in Tampa, Fla., concurs. Sarginson's team is responsible for deploying communication infrastructure to support everything from bomb disposal, Special Response Teams (SRT), hostage negotiation and even the needs of the public information officer (PIO). Additionally, his team is a key player in an eight-county Regional Domestic Security Task Force. Sarginson adds, “We are developing a deployable infrastructure that supports any and all missions regardless of the circumstances. There is a tremendous need to make the scene or critical incident site less complicated. We also must be able to communicate even if there has been a total communications infrastructure failure.” By keeping strategic decision-makers, subject matter experts and other interested

A Top Priority

The idea of a fully interoperable, easily deployed, flexible, scalable and standards-based communications system seems like a tall order. But done right, it is, hands down, the most effective method of combating an emergency.

“Our goal is to be fully interoperable, not only within the state, but with neighboring states and localities,” says Bill Buffington, technical director of the Mississippi Wireless Information Network (MSWIN) project. “We're only about 20 percent implemented today, but when it's finished, we expect full interoperability.”

The state of Mississippi has taken a slightly different route to the same goal, implementing a statewide interoperable emergency communications voice and radio network. The MSWIN allows different systems and departments to communicate, even if those systems are in or from other states.

agency personnel in remote tactical operations centers or linked in via Virtual Fusion Centers, then more resources can be brought into the picture at a faster pace.

The ability to see and hear what is going on at the operational level can be achieved without the delays associated with travel to and from the action. Building a scalable communications infrastructure that mobilizes and demobilizes rapidly, supporting enhanced situation awareness and operational intelligence is the over-arching goal for HCSO.

But it's not that easy. Not only can it be expensive, but it takes some guidance and expertise. Because agencies within jurisdictions own a multitude of technology — much of it older technology that can't be replaced because of funding limitations. Instead, states and municipalities rely on a combination of proven technology and expert advice to develop an interoperable system that works at every level.

“Having data at the touch of a button can be vital in a situation where information and decisions are critical,” says Jeff Webster, an analyst at INPUT, a government-focused market research firm based in Reston, Va.

Setting the Groundwork

Before choosing any technology, a lot of important behind-the-scenes planning and coordination must take place. Because all states have emergency communications plans in place, the process usually starts there. Local municipalities often use the state plan as a starting point but also must involve state officials in their own planning processes.

“It’s important to work with all of the stakeholders and try to have everything worked out in advance about the possible types of emergencies, how they will be addressed and who will participate,” says David Stevenson, managing director for the CJIS Group, a Tallahassee, Fla., research and consulting firm specializing in criminal justice and public safety issues. “It’s only after that coordination that you get into what technology to use.”

Funding also is a significant issue, as costs can easily spiral. For example, the top state and local interoperability systems currently under development include Los Angeles County’s Regional Interoperable Communications System (\$600 million), Maryland’s Statewide Public Safety Communications Interoperability System (\$300 million), Pima County, Ariz.’s Wireless Interoperable Network (\$75 million), and Connecticut’s Statewide Interoperable Communications System (\$10 million).

Once those issues are worked out, the technical components of the deployable communications system take center stage. In general, every deployable communications system should be:

- **PORTABLE/QUICK TO SET UP.** As simple as this sounds, it’s critical. Some deployable communications systems are small enough to fit into a briefcase, but contain all necessary components to communicate with anyone, anywhere. Others are housed in a secure vehicle that can be moved to whatever location necessary.
- **STANDARDS-BASED.** Complying with existing standards, such as the IP standard mandated by the FCC and other standards-based protocols is a major key to interoperability.
- **FLEXIBLE.** The system must be able to work with whatever communications technology is being used by others involved in the effort. That means being able to communicate via voice, video and data over wired, wireless, satellite and microwave-based networks, from headquarters, moving vehicles and under a variety of adverse conditions.
- **INTEROPERABLE.** Without true interoperability, it’s impossible to create real-time communication between multiple responders and agencies. Interoperability means a system that works seamlessly with whatever technology is being used by other participants — everything from radio and non-IP networks to landline phones and satellite networks.
- **SCALABLE AND TIERED.** Because it’s impossible to know the scope of an unknown emergency, it’s critical to make sure that the system can accommodate as many users as possible on the network.

Federal Goals for State and Local Emergency Communications

Following disasters like Sept. 11 and Hurricane Katrina, Congress enacted provisions in 2006 requiring the Department of Homeland Security’s Office of Emergency Communications to develop a National Emergency Communications Plan (NECP). The plan is designed to be comprehensive and focuses on the entire country’s emergency communications capabilities.

That means that along with federal emergency communications goals, the NECP also outlines specific goals for states and municipalities. More specifically, these goals, detailed on a July 2008 memo, are:

- By 2010, 90 percent of all high-risk urban areas must be able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.
- By 2011, 75 percent of jurisdictions not receiving grants from the Urban Area Security Initiative must be able to demonstrate response-level emergency communications within one hour for routine events involving multiple jurisdictions and agencies.
- By 2013, 75 percent of all jurisdictions must be able to demonstrate response-level emergency communications within three hours, in the event of a significant event, as outlined in national planning scenarios.

Tiered Solutions

Regardless of the defined need or proposed strategy for acquisition of tool sets, it is important to look at deployable communications systems as fitting into one of three categories or tiers of use. Tier-3 or strike team solutions are generally placed into the hands of those most likely to be first on the scene. Strike team systems generally support from one to 10 users all working the same mission and generally from a single agency. Strike team solutions deploy and fold up very rapidly and transport easily via sport utility vehicle, automobile, all-terrain vehicle (ATV) or boat and can even be hand carried into an incident area. Tier-3 solutions require minimal power input, only seconds or minutes to activate and demand only basic computer skills to initiate a communications session. Strike team solutions support executive-only level connectivity in a disaster recovery use environment or can be tactically used by a single agency with a single task such as damage assessment, urban search and rescue (USAR), shelter operations, etc. A properly architected and equipped emergency vehicle is fast becoming the starting point for front line Tier-3 deployable communications systems. Advanced life-support rigs, police cruisers and fire engines are fast becoming personal command and control centers. Streaming live video, field data collection and a variety of communications backhaul options are enabling onboard systems to do more than ever before. Additionally, modern Tier-3 solutions are characterized by the briefcase and backpack-sized office-in-a-box technology.

Tier-2 or unified command-level solutions are defined as systems capable of supporting a great number of individual voice, data and video connections from disparate organizations or agencies. Unified command systems possess the capacity to connect fire, emergency, medical and law enforcement within an incident or disaster theatre as well as interconnecting the hundreds of simultaneous connections and hold the same requirement as Tier-3 with respect to ease and schedule of deployment. Tier-2 systems are most often kitted in rugged cases, built permanently into vehicles or introduced to the scene via trailers.

Tier-1 or secure command solutions differ only slightly from Tier-2 options. The communications technologies that comprise either remain similar in form and capacity. Tier-1 systems require only the addition of physical functionality in the form of ergonomics and physical security. The tried and true mobile command vehicle (MCV) in use today by public safety agencies serves as the quintessential secure command environment. The often windowless four walls of the modern MCV inherently limit access, keeping prying eyes away from decision-makers and incorporate heating, ventilating and cooling comforts. Investments solely in MCV-based technologies

Ohio Department of Public Safety

Ohio's Department of Public Safety, working with the state's Multi-Agency Radio Communications System (MARCS) Steering Committee, put together a deployable communications system several years ago after realizing that its current system simply wasn't interoperable enough to be responsive in the case of severe emergency. The Department's Emergency Management Agency and Steering Committee wanted a reliable system that could quickly supplement lost communications or communicate with first responders who enter an area to help in the case of crisis.

The Department started with a transportable 800MHz-based Transportable Communications System (TCS), which can be used to replace a non-working site, supplement a site for added capacity or link via satellite to more stable locations.

Added to the five-channel trunk site are additional radio systems that allow first responders to link into whatever technology is being used across the state, explains Mark Patchen, director of Technical Support Division. For backhaul communications, the state relies on satellite technology. Equipment is installed in 12 interoperable vehicles located at sheriff's offices throughout the state. These vehicles provide rapid deployment for local incidents.

represent a limitation in the ability to deploy with respect to geography and resources as often specific technical expertise is required to transport and operate the complex on board systems. Not all secure command investments come in the way of motorized vehicles.

Many organizations are utilizing tactical operations center (TOC) environments to provide security and ergonomic function to existing Tier-2 or unified command communications investments. These trailer-based TOC generally include a heated and cooled tent environment in a variety of sizes. The tent then becomes the operating environment consistent with the MCV or as an additional space capability in conjunction with an MCV. By simply combining a Tier-2-level deployable communications solution with the TOC, an organization now has Tier-1 ergonomics and security capability scalable up from a Tier-2 communications system deployment. The TOC adds incident command post (ICP) functionality by including erectable video display areas or video walls. For continuity of operations purposes, include rugged cases loaded with switches, servers and data storage to reconstitute downed facilities.

Deployable Communications Systems Components

No matter the mission, size or tier of any given deployable communications system, successful solutions all have common ingredients with respect to basic structure. It is feature sets and add-ons that provide the specific mission/task-based functionality that differentiates a fire-based solution from a mass care-based solution from a law enforcement system. The following individual component areas form a baseline structure for system development. While goals and objectives drive the need and investment level in each component area, all should be addressed when developing any new deployable communications technology capability.

BACKHAUL/REACH BACK — Basically backhaul technologies link remote operations to the rest of the world. Supporting development of the common operating picture, increased situation awareness and virtual incident command, backhaul technologies give strategic decision-makers nearly the same view of a response scene as possessed by the responding operations personnel. The ability to create a phone conversation, stream live video, forward necessary data near instantaneously to the back-end is essential to efficient use of resources. To accomplish this, the modern backhaul system must somehow intersect broadband services and the Internet. The most common methods of connecting voice, data and video information from a local scene to a remote far-end include satellite, cellular modem, Wi-Fi and terrestrial-based services. When considering which backhaul solution one should implement, the answer is simple. All of them. Satellite is generally the most

expensive but is also relatively impervious to regional catastrophic disaster. Cellular data connectivity serves as the most common backhaul method selected but is highly vulnerable as cellular infrastructures are often lost or degraded following a disaster. Wireless bridging to existing infrastructures is a viable option provided those infrastructures exist in the response area. Microwave systems can reach back for several miles but are often difficult and time consuming to erect. Data radio is an option with limited capacity and fiber optic and Ethernet connectivity should always be included.

LOCAL AREA CONNECTIVITY — While backhaul technologies are essential in development of a common operating picture and makes possible virtual incident command by linking the scene to ECC (Emergency Communication Center) and EOC (Emergency Operations Center) facilities; it is local area connectivity that enables operations and supports responders on scene. The ability to establish an infrastructure communicating voice, data and video information throughout the critical incident site and across level and functional lines is at the core of the interoperability issue.

Local area connectivity often begins with the ubiquitous 800MHz, 700MHz and VHF/UHF radio transmission. Everyone arriving at an emergency scene generally possesses the ability to talk via radio. The new target capability, however, is the ability to extend that radio coverage over a greater area with more available spectrum. In the 21st century threat environment, push-to-talk radio is no

Deployable Communications by the numbers

6: The number of U.S. cities DHS considers fully prepared to communicate during a disaster (Washington; San Diego; Minneapolis-St. Paul; Columbus, Ohio; Sioux Falls, S.D.; and Laramie County, Wyo.)

56: All 56 U.S. states and territories have developed Statewide Communication Interoperability Plans (SCIP) that identify near- and long-term initiatives for improving communications interoperability.

58%: The number of urban and metropolitan areas that have not developed strategic plans for interoperable communications, according to DHS.

75: The number of cities DHS says have policies in place for helping emergency workers communicate.

\$2 BILLION: The amount distributed by DHS to state and local governments through its Interoperable Communications Technical Assistance Program (ICTAP).

4,200: The number of U.S. communities (out of 6,800 communities surveyed) DHS believes are capable of talking to each other.

\$48.575 MILLION: The amount FEMA has available for planning, training, exercise and personnel activities related to emergency communications.

SOURCE: Department of Homeland Security

The Basic Differences in Tiered Solutions Available in the Market Today

Feature	Tier-1 Secure Command	Tier-2 Unified Command	Tier-3 Strike Team
Stand Up/Stand Down Interval	Hours	Minutes/Hours	Seconds/Minutes
Supported Organizations	Multiple	Multiple	Single
Supported Tasks	Multiple	Multiple	Single
HVAC	Yes	No	No
Physical Security	Yes	No	No
Includes Own Power Source	Yes	Maybe	No
Operates on Limited Power Source	No	Maybe	Yes
Users Supported	1-100	1-100	1-10
Hand Deliverable	No	No	Yes
Airlift Deliverable	No	Yes	Yes
Vehicle Based — SUV, etc.	Yes	Yes	Yes
Towable	Yes	Yes	No
Investment Range	250K +	50K-250K	3K-50K

longer enough. The need exists to also communicate intra-site via data and video information as well. This has given rise to the creation of ad-hoc networks supporting voice, data and video. Ad-hoc networks are essentially wireless networks supporting convergence and operating over a variety of frequency ranges. 802.11a/b/g, 4.9GHz, 900MHz, 3.5GHz and Wi-Fi Max are just some of the frequency ranges commonly deployed to support critical communications intra-site.

The introduction of the various LMR (Land Mobile Radio) spectrums as well as the cellular service spectrums repeated and boosted on scene form integral parts of the local connected area as well. These new wireless-based ad-hoc networks replace wired to switched Ethernet networks only available previously in close proximity to satellite or other backhaul solutions.

ROUTING CAPABILITY — Radio interoperability, or the ability for a wide variety of radio spectrums to find electronic common ground is largely achieved by converting the radio traffic to IP. Telephone communications is converting to Voice over IP, and digital megapixel cameras are replacing analog CCTV cameras at an alarming rate. It is IP that is at the heart of everything being discussed in deployable communications. Therefore it stands to reason that some mechanism for routing IP traffic is essential for any deployable solution set hoping to deliver voice, data and video. For IP-based services, routing capacity is required to connect local area connectivity with backhaul services as well as bridges and gateways.

Properly designed and configured routing capacity will keep local traffic local and only allow what needs to be transmitted to the generally capacity-limited backhaul. It will not require two individuals at the same local scene to utilize the limited backhaul capacity to talk to one another locally. Deployable routing capabilities take one of two forms: traditional hardware-based routers and software-based routers. Linux OS software-

based routers have become increasingly popular over the last several years. The ability to place software onto a variety of already ruggedized devices has a lot of appeal. Typically, off-the-shelf hardware-based routers do not possess the capacity to operate in environments of extreme heat and weather while software that can run on desktops, appliances and servers can economically be placed into operation on ruggedized devices.

BRIDGES AND GATEWAYS — Bridges and gateways connect existing local area connectivity to other local area connectivity systems, as well as connecting disparate technologies like 800Mhz radio to IP. There are three points at which bridges and gateways need to be considered in a deployable communications systems environment. The first point for which to examine bridge/gateway requirements is in the way of interconnecting disparate technologies. Examples of these types of bridges include radio interoperability bridges. Radio interoperability bridges take radio communications channels in 800MHz, 700MHz, VHF/UHF and project 25 spectrums and connect them onto an IP highway. This provides the capability for VoIP phones, handhelds and notebooks to communicate with legacy radio systems. Additionally, now that we connect disparate

Dedicated Spectrum for Emergencies

In 2008, the Federal Communications Commission (FCC) moved toward the idea of a nationwide, interoperable public safety broadband network dedicated solely to emergency communications efforts across the country.

The biggest part of the puzzle was cordoning off the 700MHz block of spectrum specifically for this network. To solve this problem, they created a public/private partnership framework for the 700MHz band, via an auction with competitive bidding.

The auction results determined the specific air interface technology that is being deployed across the country when building the interoperable broadband networks.

radio frequencies onto a common communications technology — IP — we can achieve radio interoperability. Conversion of analog radio signals to digital IP traffic makes it significantly less difficult to deliver radio traffic to a distant back-end. Via this type of bridge, it is now possible to listen to public safety radio traffic from one town from almost any location.

A second type of bridge/gateway to consider is one that interconnects disparate organizations. No amount of deployable communications gear in the world will replace the ubiquitous “runner” in an emergency response if proper attention to interconnecting bridges is not taken into account. Wi-Fi communications serves as the most promising method of interconnecting deployable communication systems from two or more disparate responding agencies. Most standards-based bridging Wi-Fi access points can communicate with other wireless access points of a differing manufacturer.

The third bridge/gateway requirement would be to connect local area connectivity to local area connectivity and to backhaul connectivity. This can be accomplished utilizing the same technologies used to bridge disparate agencies. Wi-Fi as well as millimeter and microwave technology can solve this dilemma in most cases. Intelligent access points can provide Wi-Fi, Wi-Fi Max or 4.9GHz bridging capability to connect either disparate agencies or geographically separated local area connections. The dual radio intelligent access points provide omni-directional client device connectivity and bridging capability all in one device.

CLIENT DEVICES — Client devices can include radios, notebooks, handheld computers, printers, scanners, video cameras, facsimile machines, VoIP phones, cell phones and data collection devices that will use the deployable communication infrastructure. While it is generally not necessary to provide client devices as part of a given deployable communication solution, it is advisable to take into consideration all of the client device types that might be called upon in a response. How does the solution receive an incoming fax? How will it handle print sharing? How will we serve, store and record streaming video and make image files available to the remote back-end? Asking these questions and more will aid in development of the core deployable infrastructure. Deployable video surveillance kits, for instance provide add-on situational awareness to any deployable communications solution. Streaming, recording and making video available to back-end and local area users becomes a special challenge though as video bandwidth requirements often exceed reasonable capabilities.

POWER AND TRANSPORT — It is not enough just to be able to connect to a variety of power sources. Deployable communications solutions must also operate over a variety of power conditions. Vehicle power, generated power and existing building AC are just some of the options one may be confronted with when standing up communications infrastructure following a disaster. Deployable solutions must be capable of operating over a wide range of voltage/amp variations. Electronic devices must also be protected from voltage overages just as they would when operating in a normal office environment.

Deployable communications solutions must also be transported in such a manner as to ensure long life and protection from the elements. Whether built into a vehicle, trailer mounted or installed in hardened cases, protection from the elements, protection from vibration and shock, and protection from the ingress of dirt, grime, dust and moisture must be accounted for.

Interoperability Standards

Despite major advances, interoperability continues to be an issue for many states and municipalities.

To further the cause, the Association of Public-Safety Communications Officials (APCO) has developed Project 25, a joint effort of U.S. federal, state and local governments with support from the U.S. Telecommunications Industry Association. The goal, says APCO president Chris Fischer, is to create a series of technical specifications for digital land mobile radio communications systems, resulting in greater interoperability.

“Standards are critical for interoperability,” explains Jeff Webster, a Homeland Security, Justice & Public Safety analyst with Input. “If all equipment adheres to the same set of standards, you can be sure that it will be able to communicate with other equipment in other jurisdictions. That’s where everything is headed.”

This type of progress, along with increasingly sophisticated, intelligent deployable communications technologies, will go a long way toward creating truly interoperable emergency communications systems in every U.S. jurisdiction.

Success Stories

HILLSBOROUGH COUNTY SHERIFF'S OFFICE — TAMPA, FLA.

HURRICANE CHARLEY RESPONSE: AUGUST 2004

The Hillsborough County Sheriff's Office (HCSO) needed to establish an ad-hoc mobile and portable communications network to provide basic communications and communications interoperability amongst a variety of responding agencies. Radio communications had become compromised and rendered unreliable because of interference and the sheer volume of requests for help. The agency needed a reliable, transportable communications solution that would allow its officers to communicate in the absence of power and electricity, and be easily moved as recovery efforts progressed to new parts of the region.

HCSO deployed the F4W Tactical Wireless Emergency Broadband Network (TWEB) system along a 16-mile stretch of U.S. Highway 17 and Florida State Road 62 that provided secure wireless Internet connectivity to multiple mobile command centers and patrol vehicles along the covered route. The network allowed interoperability among the fire, rescue and law enforcement agencies that assisted Hardee County and the municipalities of Wauchula and Zolfo Springs during the recovery period. The secure and reliable satellite broadband solution provided for Internet connectivity — users had access to their proprietary applications and the remainder of the command center network functions. The recovery teams could now communicate around the region, state and nation. Command was able to track deputies patrolling unfamiliar territories and provide critical information and data in real time. F4W also deployed a Command Plus 4 Surveillance System to provide wireless surveillance video of key intersections, staging areas and food distribution centers. The Florida Department of Law Enforcement (FDLE) and emergency response teams in Tallahassee and around the state gained access to the surveillance cameras. The network was originally deployed in Wauchula in less than four hours. When power was restored to part of the

covered area, a portion of the network was redeployed at a new location five miles south on U.S. 17 in less than three hours.

HURRICANE KATRINA RESPONSE: AUGUST/SEPTEMBER 2005

At the request of the Federal Emergency Management Agency (FEMA), CDW-G and Hewlett Packard established a Tier-1 secure command communications facility in Gulf Port, Miss., shortly after Hurricane Katrina. The facility provided data communications connectivity to a newly constituted multi-jurisdictional task force assigned to missing persons cases in the Gulf of Mexico region affected by Katrina. Law enforcement officers from local, state and federal agencies utilized the converted mobile home facility to gain access to various databases required to research, locate and clear cases associated with those reported missing. The facility included desktop computers and a local area network connected to satellite backhaul communications. The task force successfully cleared 693 of the 781 missing persons cases assigned to it thanks in large part to the secure command communications solution.

TENNESSEE TORNADO RESPONSE: FEBRUARY 2008

CDW-G and F4W combined to stand up a disaster recovery center in a central Tennessee municipality hard hit by the tornadoes of February 2008. City officials decided to locate the disaster recovery center close to those most affected by the tornadoes and consequently far away from the city's technology infrastructure. Utilizing the F4W Personal Systems Interconnect (PSI), a Tier-3 strike team solution, the response team was able to establish voice and data connectivity supporting five telephones and Internet connections within minutes. Utilizing satellite backhaul connectivity, the team was able to have an entire local phone company primary rate interface forwarded to the satellite communications link. Local inbound and outbound telephone calling capability was created where none existed before within hours of project conception. The F4W PSI additionally provided inbound call distribution capability as well as voicemail. Disaster recovery center personnel utilized wireless Voice over IP phones enabling them to work beyond the confines of their desks. ■

About the Author



Houston Thomas serves as the Public Safety Business Development Manager for CDW Government, Inc. (CDW-G). Mr. Thomas has nearly three decades of experience delivering communications and information technology solutions to government and private sector organizations. Ten years of that time was dedicated to Disaster Mitigation and Recovery Planning. Mr. Thomas has spent the last seven years focused primarily on the state and local public safety arena and first responders. In addition to his technology expertise, Mr. Thomas is an experienced Disaster Response leader in the area of Mass Care Logistics and has been actively involved in a number of domestic response operations, including the response to the hurricane seasons of 2004 and 2005, including Hurricane Katrina.

For more on CDW-G's public safety products and services, see the21stcenturycommunity.com.