

SPECIAL REPORT

Homeland Defense

JOURNAL

MorganFranklin Guide

Interoperability Versus Assured Communications Critical Factors for Emergency Managers



Five Critical Considerations for Assured Communications in a Crisis



1. Communication is the key to effective disaster preparation and recovery. Redundancy is essential for the flow of communication. Don't get caught without options.

When your system takes a hit, when the power goes down, are you 100 percent sure your systems will support your disaster response?



2. An emergency off-site center should be considered in a continuity of operations plan. A reliable and tested plan B allows an organization to rebound and restore essential operations in the event of an emergency.

If your physical location is compromised, do you have the built-in resiliency necessary to keep core operations running smoothly?



3. Recognize organizational interdependencies. Have a plan to keep every relevant agency, department and organization in the loop with accurate information to effectively coordinate crisis response.

Do you have reliable and accurate data systems that provide ready access to essential information necessary to contain catastrophic situations?



4. Establish a plan to ensure that the right people are put in the right places during an emergency. This includes the ability to manage resources from the disaster site itself.

Do you have dispatch capabilities that conserve time and help mitigate incident loss?



5. High assurance telephony, IP network and radio connectivity are vital to voice, video and data connectivity in the event of an emergency.

Are you fully leveraging existing technology investments? Do you have 100 percent confidence in the technology solutions that support your interoperable communications plans?

Every organization and municipality faces a unique set of risks, circumstances and environmental factors. MorganFranklin is a leader in developing fully extensible and affordable assured communications solutions.

Mobile Command Vehicles, Back-up PSAPs, Interoperable Solutions, Distributed CAD and other high-stakes communications challenges.

Contact MorganFranklin at inresponse@morganfranklin.com or 703-564-7525 ext. 350.

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

By Paul Serluco, Managing Editor, Homeland Defense Journal

This guide is a companion document to MorganFranklin's guide: "Understanding the New GSA Disaster Recovery Procurement Program for State and Local Government."

"All 50 states should aim to have interoperable systems for public safety by the end of 2008,"

U.S. Department of Homeland Security Secretary Michael Chertoff said during a keynote speech at the National Grants and Training Conference in Washington, D.C., 2006.

Part One: The Problem Communications Interoperability and Beyond

Communications interoperability among agencies and jurisdictions has been a long-term problem in the public safety community. Since the Department of Homeland Security was established in 2002, it has been working to improve interoperable communications. From FY 2003 through FY 2007, more than \$3 billion in grant assistance was provided to state and local agencies for equipment and other projects to improve communications interoperability. Programs such as the Interoperable Communications Technical Assistance Program (ICTAP) and SAFECOM have also been formed to develop tools, expedite technology standards development, and standardize testing and evaluation to assist public safety agencies in the planning and implementation of communications systems. However, as DHS Secretary Michael Chertoff stated in his speech in May of 2007 to the Tactical Interoperable Communications Planning Conference, immediate communications interoperability requirements have yet to be fully met. Those requirements must be identified and met rapidly to ensure public safety.

The Current Situation

Barriers to interoperable communications are both technical and operational. Each agency typically has its own unique legacy technologies, requirements, operating environments and processes. Therefore, achieving interoperability requires that, in addition to addressing technology and disparate communications systems, agencies must examine governance, procedures, training, exercises and usage. Urban and metropolitan areas have access to operational planning and exercise support to address these needs within the framework of multi-jurisdictional, multidiscipline incident responses. A scorecard has also been introduced to assess each area's progress in implementing interoperability. Secretary Chertoff argued that, "The scorecard is an important milestone in this ongoing process because it marks the culmination of two years of planning and exercising tactical interoperable communications capabilities."

DHS requires designated urban/metropolitan areas to focus on the creation and/or validation of regional SOPs that, in some cases, represented the first time local jurisdictions came together to align operational communications plans for incident response. DHS also emphasizes multi-jurisdictional and multidiscipline governance structures as demonstrated through the development of the *SAFECOM Statewide*

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

Communications Interoperability Planning Methodology and the Urban Area Working Group requirements. Some areas had long-standing governance bodies that provided multi-jurisdictional and multidiscipline leadership in developing longer-term communications goals and resource plans. Other areas used the TICP process as an opportunity to bring such leaders to the planning table.

Analysis of the scorecard results shows two common trends across all areas:

- Areas developing and/or using shared systems tended to demonstrate more mature governance structures, SOPs and usage.
- Areas that diversified their funding sources to address sustained interoperability tended to also have stronger governance structures in place.

Overall Scorecard Trends

- Policies for interoperable communications are now in place in all 75 designated urban/metropolitan areas.
- Regular testing and exercises are needed to effectively link disparate systems to allow communications between multi-jurisdictional responders (including state and federal) during crises.
- The DHS Tactical Interoperable Communications Initiative has played a fundamental role in advancing interoperability in designated urban/metropolitan areas.
- Cooperation among first responders in the field is strong, but formalized governance (leadership and planning) across regions has lagged. Governance is critical in planning for larger-scale, multi-jurisdictional responses and the implementation of next-generation technology.
- Areas that were part of the UASI Grant Program tended to demonstrate greater traction in strategic planning across the region.
- Areas with a history of multi-jurisdictional cooperation because of prior incidents demonstrated stronger SOPs and usage.
- Many of the exercises were more complicated in

terms of the number and type of participating agencies, which provided more insight into the breadth of the SOPs and the depth of usage. Areas with less complicated exercises and fewer participants scored higher in usage because the events required less coordination.

- Areas that were empowered to develop a TICP based on a “bottom-up” approach of a collaborative, regional nature scored higher in Governance than those areas in which a “top-down,” state-centric approach was employed.

Next Steps for 2008

DHS has stated that it will continue to align its programs and resources to best address the communications needs of first responders. Accomplishing this feat will require a coordinated DHS effort to provide increased resources and assistance to states and localities to empower greater communications interoperability across broader regions.

Prioritizing five efforts will support this goal:

- 1. FY 2008 Grant Programs:** The Homeland Security Grant Program (HSGP) and Infrastructure Protection Program will encourage interoperable communications as a program focus area.
- 2. Completed Communications Unit Leader (COML) Training:** DHS will complete and release the criteria for COML training to ensure that public safety agencies have clearer guidance on the role of COML in incident response.
- 3. Improvement Plans/Scorecard Recommendations:** DHS ICTAP is developing and will continue to deliver technical assistance to address the most prevalent gaps identified through the Tactical Interoperable Communications exercises.
- 4. Best Practices/Lessons Learned:** A compendium of all best practices and lessons learned from the TICP validation exercises will be provided to each designated urban/metropolitan area. Contacts for

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

each area will be provided to encourage a peer-to-peer “cross pollination” of practices.

5. Statewide Plans: Designated urban/metropolitan areas will be asked to continue an active role in the development of Statewide Interoperable Communications Plans as required by December 31, 2007.

Scorecard results show that urban/metropolitan areas have come a long way in developing their tactical interoperable communications capabilities. The technology exists to permit interoperable communications, but solutions are often not available regionally and in many areas are far from seamless. Continued training and the use of available technical solutions and their SOPs are critical to operational success. Work remains even in those areas that have demonstrated success at the tactical, command level of communications interoperability. Multi-agency communications have been addressed within many of these jurisdictions, but regionalizing the existing communications strategies to identify longer-term interoperability goals across multiple jurisdictions and levels of government must still take place.

Part Two: Solutions Assured Communications

There are many factors driving state and local emergency management officials’ desire for truly assured communications:

- Not relying 100 percent on public infrastructure to support a large-scale emergency or national crisis.
- Providing emergency responders access to enterprise applications and vital situational data from disparate systems at the scene.
- Collaborating (data and voice) with multi-state, federal and other important stakeholders at the scene.
- Minimizing the financial liability and negative implications that may stem from the perception of a slow response to an emergency or national crisis.
- Making the most out of tax dollars and grants by leveraging the best commercially available off-the-shelf technology rather than proprietary and custom-built communications solutions.

- Providing the public with increased confidence that state and local leaders are investing in a wide range of measures to protect community interests.

Achieving assured communications in the event of a disaster or emergency requires careful planning and expert advice.

Mention the word interoperability and many people immediately think of radio, but interoperability is much more. Proper preparation means more than the possession of interoperable radios. It encompasses backup and continuity of communications infrastructure and critical systems that operate even when public systems do not.

This involves backup circuits and sometimes mobile infrastructure to provide a truly resilient and flexible solution for ensuring critical communications. For example, the use of dedicated or shared SATCOM for continuity of critical applications like 911, 311 and other PSAP functions.

“People have to know what it is they need and not make assumptions that their unique environments require the same exact solutions used somewhere else,” Chris Herndon, chief technologist with MorganFranklin, said. A lot of technology has been purchased partially through a kind of peer-pressure. We see municipalities jump on a bandwagon for specific technology solutions quite often, Herndon said, “There are no silver bullet solutions for assured communications.

“At MorganFranklin we are vendor neutral. We truly look at projects from a requirements perspective as opposed to trying to fit a solution set that we have.” MorganFranklin provides consulting and engineering solutions to public and private sector emergency managers who require unimpeded access to essential information and critical systems.

“We believe that it’s critical to look at things with a broader lens. This means making sure your requirements consider existing or planned continuity goals, backup power supplies, existing project synergies, etc.,” said Herndon. “Too often failure to do so leads to the purchase of technology solutions that are not the right fit down the road.”

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

“As a company we insist on asking the hard questions and spending the time up front to make sure that our clients are looking at emergency communications with a view that is broader than, say, radio interoperability by itself. After all, if cell towers are down, will radios even work?”

Four Critical Considerations for Assured Communications

1. Redundant Connectivity

Traditional public communications infrastructure can be seriously disrupted in an emergency event, or an environment of severe weather with landlines out, cell towers down and power supplies damaged. To ensure emergency communications, redundancy is essential. This means looking beyond landlines and cellular phones for more reliable connectivity that includes third-party managed and dedicated satellite communications.

All the functions necessary to perform in an emergency and the communications systems needed to support them must be considered. Consideration of the wide range of people and organizations necessary to communicate with — emergency responders, emergency operations centers, outside response organizations, media, government agencies, employees and their families — is essential as well.

Considerations:

Critical considerations for redundancy are:

- Prioritize access to the key data and systems required to conduct essential functions.
- Avoid reliance on terrestrial communications alone. Take advantage of basic and advanced satellite solutions if that is what your risk profile warrants.
- Consider ‘multi-jurisdictional dedicated satellite networks’ — a new approach that takes advantage of the technical benefits of dedicated satellite communications without the high cost.
- Remember the importance of planning logistically for fuel when powering your own backup generators. Many outages result from failed backup power generation.

2. Continuity Planning for Emergency Operations Center and 911 Capabilities

If your primary dispatch location or command and control center is compromised, will you have the resiliency to maintain critical operations?

Government agencies at state and local levels across the country and many other organizations are establishing emergency off-site centers as part of their continuous operations planning (COOP). A rapidly deployable and well-designed off-site public dispatch and emergency coordination capacity — fixed or mobile — can dramatically reduce the risk of downtime and ineffective resource allocation and can dramatically increase an effective response.

The communication component of a COOP plan requires well-defined chains of communication that include alternate means of communicating should primary systems fail to function. Arrangements must also be made for emergency use of other equipment and the transportation of personnel, data and supplies to an alternate location.

Duplicate or master records and programming data should be maintained in a remote area from which the necessary information can be accessed and operations resumed.

Considerations:

Critical considerations for an off-site emergency communications center are:

- Maintain communications capabilities sufficient to support essential operations and to ensure public access to emergency resources. This **must** be the first priority.
- Consider entering into a mutual aid agreement with other organizations and agencies to use their facilities for command and control.
- Plan for adequate people space and all that this entails — equipment, food, beds, supplies, accommodations.
- Consider Mobile Emergency Response Operations Centers (MEROCs) and Mobile Emergency Communications Vehicles (MERVs). Mobile platforms are a viable option. Current technology

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

allows for the integration of much of traditional communications systems into mobile platforms. The benefit that comes from this is the ability to move public safety and emergency dispatch capacities to the safest possible location. The City of Chicago, for example, now has the ability to restore its 911 capabilities in a mobile platform should the facility ever become inoperable.

- Make certain your first responders and emergency personnel are able to access enterprise applications and vital situational data from disparate systems at the scene.

3. Recognize Organizational Interdependencies

In the event of a catastrophic incident, do you have instant access to all the essential data and information from your disparate systems? Connections with other organizations are essential. A lack of cross-department and interagency coordination will result in poor emergency response.

DHS ranked many of those cities with successful multi-region training exercises much higher on the SAFECOM scorecard. People are people, and in the face of an emergency people will rely on what is most familiar, comfortable and easiest to use. But the fact is that technology is really only part of the equation. Rankings reveal that highly effective emergency management organizations have good relationships within and across core stakeholder groups. These relationships are a fundamental success factor for building critical information links. Partnerships are crucial.

Considerations:

Critical considerations for managing organizational interdependencies are:

- Ensure the ability to collaborate and coordinate voice, data and video with multi-state, federal and other important stakeholders at the scene. Know who these stakeholders are and include them as part of your technology, process and controls planning.



- Map interdependent agencies, departments, systems, processes, data and controls in a COOP plan best practice.
- Meet regularly with all stakeholders — emergency management, fire, police, federal, state and local agencies, hospitals, utilities, contractors, emergency equipment suppliers, community organizations and more.
- Place emphasis on the importance of regularly testing the reliability, timeliness and accuracy of critical information and analysis flows.

4. Right People, Right Places

Your continuity plan must be clear and must ensure

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

that the right people are in the right places during an emergency. This requires having the ability to manage resources from the disaster site. Key personnel must know where they need to be in an emergency as well as their specific functions in a crisis. Although a designated person must oversee direction and control, in an emergency, key people may not have connections with the control center. Key personnel should have trained backup personnel just in case; individuals who can take action on their behalf when necessary.

Prudent emergency planning includes the selection of alternate emergency control locations, either static or mobile, if the primary location becomes nonfunctional. These alternate locations must have the ability to link into the emergency communications network and handle data and voice transmission and management.



Critical considerations for managing people and locations:

- Ensure that key personnel know what they have to do and where they need to be.
- Have suitably equipped alternate locations if the primary control center is out of commission. This must be part of your continuity planning for your Emergency Operations Communications and public access 911 infrastructures.
- Appoint and train backup replacements for all key personnel.
- Train, train and train again.

Take a Regional Approach

“To get almost anything accomplished right now from a grants perspective it is going to have to be state-wide or at a minimum, a regional activity,” said MorganFranklin’s Herndon. “It is very important not to look at things in a silo to avoid proliferating stove-pipe solutions. We urge people to cooperate and consider regional requirements and the Department of Homeland Security expects this.

“Cities have to get regional buy-in, and we can facilitate this and give them technical information to allow them to work the people side of the whole thing. But no project is going to be funded or get under way until they have established that regional approach. That is one of the biggest driving issues right now and that is certainly the focus for these grants,” he said.

“The Federal government has learned over the years that writing hundreds of pages of specifications for protocols or for pieces of equipment does nothing except lead to more stove-pipe systems and proprietary systems that yet again lock government into one or two vendors.

“We have gone full spectrum. The government’s latest position is that it is not going to write specifications, so now we have a bunch of new technology that still doesn’t interoperate any better than the stove-pipe systems do.

“What the DHS is wrestling with is the ‘make sense’ point between the two; some sort of basic evaluation criteria or interface specifications or interoperability standards without having the full blown military specifications of the past. That is why they are addressing this as a regional matter. They figure that if people and agencies have to deal with this as a state-wide or regional activity, it is much more likely they will achieve cooperation and interoperability.

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers



“Quite often much of our business is derived from organizations making the wrong decisions and then having to try and figure out how to make their major purchase do something useful for them. Obviously we like to be involved before they have gone out and bought a \$1 million command truck but, again, quite often we are looking at a major acquisition, say, a communications system or a network operations center that really only addresses a very small percentage of their core requirements. Then you have to work out how to fix it, retrofit, upgrade it so that it will actually work and do what they need it to do.

“This happens more often than not because the guys in agencies tasked with going out and finding the best solution usually have three or four full-time jobs already, manning their communications centers and everything else that they have to do on a daily basis. On top of all this they then have to weave their way through all the fodder of sales pitches and advertisements. Unfortunately, it is definitely not a one-size-fits-all market.

“We make a point of making sure we exhaust all

opportunities for commercially available off-the-shelf products (COTS) before we even consider going into something custom or proprietary. Too often people end up building custom solutions that are just a duplication of commercially available products. If I build my own custom solution, where is the logistical support behind it for software and hardware issues, for the upgrade? However, if I leverage COTS, I am going to have a warranty, technical and logistical support and all the other infrastructure support I may need.

“You have to consider the full life cycle of the product. If I can

address 85 or 95 percent of my requirements with COTS, am I really going to benefit from that additional 5 percent or 15 percent by going with something custom-built and very much more expensive? Quite often you will find there is no significant additional benefit. It is an education process and it is very true that an educated consumer is our best customer.

“COTS is a big deal because that is what really makes or breaks these systems two to five years down the road. We have engineered many communications systems for major clients and, so far, we have yet to build a custom system,” Herndon said.

The Assured Communications Solution

Recent disasters demonstrate that Emergency First Responders require a rapidly deployable, interoperable communications infrastructure that provides high assurance telephony, network and radio connectivity for their critical communication needs. Local infrastructures simply cannot be relied upon during a crisis.

Affordable and practical solutions to day-to-day communication challenges are what federal, state and municipal organizations seek. MorganFranklin experts understand that commercially available off-the-shelf

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

(COTS) hardware and software, IP and satellite communication are essential to build flexible and robust communication systems. The days of homegrown, proprietary systems are long gone, along with the need to go to the large integrator to achieve an organization's goals for communication. With its vendor-neutral approach, MorganFranklin delivers the best capabilities to address each customer's specific needs.

The first step a provider must take is to listen, determine and define those needs. To build a system, you need to understand your range of incidents and scenarios, existing assets and the end goal. Communications infrastructures do not have to be built from scratch.

Chances are your current system consists of equipment that required a significant investment of time and money. To make things even more complicated, perhaps during the purchasing process each of your departments did their own thing. MorganFranklin begins the design of a new system by taking the existing patchwork of components, bringing together their disparate capabilities, and creating a state-of-the-art, interoperable command and control network.

For more information about the MorganFranklin Corporation and their capabilities for assured communications, visit www.morganfranklin.com/inresponse.

Accessing Solution Providers

MorganFranklin is a participant in the cooperative agreement program with the GSA that allows state and local governments to purchase information technology services. The cooperative agreement allows state and local governments to leverage the U.S. government's significant buying power. MorganFranklin is also an authorized provider of disaster preparedness services and

solutions under the new GSA Disaster Recovery Procurement Program. This allows state and local buyers access to vendors of products and services from plywood to communications solutions. See the companion document to this report titled "Understanding the New GSA Disaster Recovery Procurement Program for State and Local Governments."



Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

Steps to Assured Communications Success

- **Know Your Requirements**
- **Don't Assume Technology is the Only Answer**
- **Work it out to get the Right Solution**
- **Squeeze the EXTRAordinary out of your COTS**

Case Study #1

Communications Interoperability on the Move: Chicago First Responders Prototype Vehicle for the City's Disaster Relief

Equipped with state-of-the-art technology to keep information flowing to and from City of Chicago leaders, first responders and Chicago citizens in the event of a crisis, this proven emergency command and control vehicle features radio, telephone, commercial video, internet and satellite connectivity.

A centralized data fusion facility on wheels, the system is designed to supplement local communication infrastructures as well as to function independently as a regional communication center when local systems collapse. It is virtually a 911 center on wheels.

With 115 telephone lines and 96 independent cellular lines, the vehicle ensures the continuity of communications during a crisis. In the works for two-and-a-half years, the mobile command vehicle is linked directly with the Chicago Office of Emergency Management and Communications (OEMC).

High praise for the comprehensive emergency response vehicle was immediately forthcoming. Chicago Chief Emergency Officer Cortez Trotter told the *Chicago Sun Times*, "This is superior to anything we've been able to find out there."

The interoperable emergency response system features internet and media plug-in capabilities and the system connects seamlessly with all major operational systems and office applications. Streaming

video via satellite with 30 interior and exterior video monitors provides both on-site and remote users up-to-the-minute awareness of emergency situations. Police, fire department and other emergency agencies can also be dispatched directly from the scene. Hyper-advanced technology ensures that it will not become obsolete, a concern the city had with an emergency response vehicle it previously intended to purchase from another company.

The multi-million dollar vehicle was officially deployed during the September 7th, 2006 Chicago Loop Disaster Evacuation Drill. The new system "makes disaster response more immediate and manageable," said Bob Morgan, MorganFranklin CEO. "Working with the Chicago Office of Emergency Management and Communications gave MorganFranklin the opportunity to make a real difference when disaster strikes."

Chicago Mayor Daley said, "No other city has this. In short, Chicago is far ahead of most cities when it comes to using state-of-the-art technology."

Making a Difference

The mission of the OEMC Command Vehicle project is to develop and deliver a system capable of extending the core Command, Control and Communications functions of the OEMC, via satellite, to any location within the Continental United States. All of the many technical subsystems rely on commodity, commercial standards to ensure the highest level of flexibility, portability, extensiveness and interoperability. Many of those subsystems are interconnected to provide more local

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

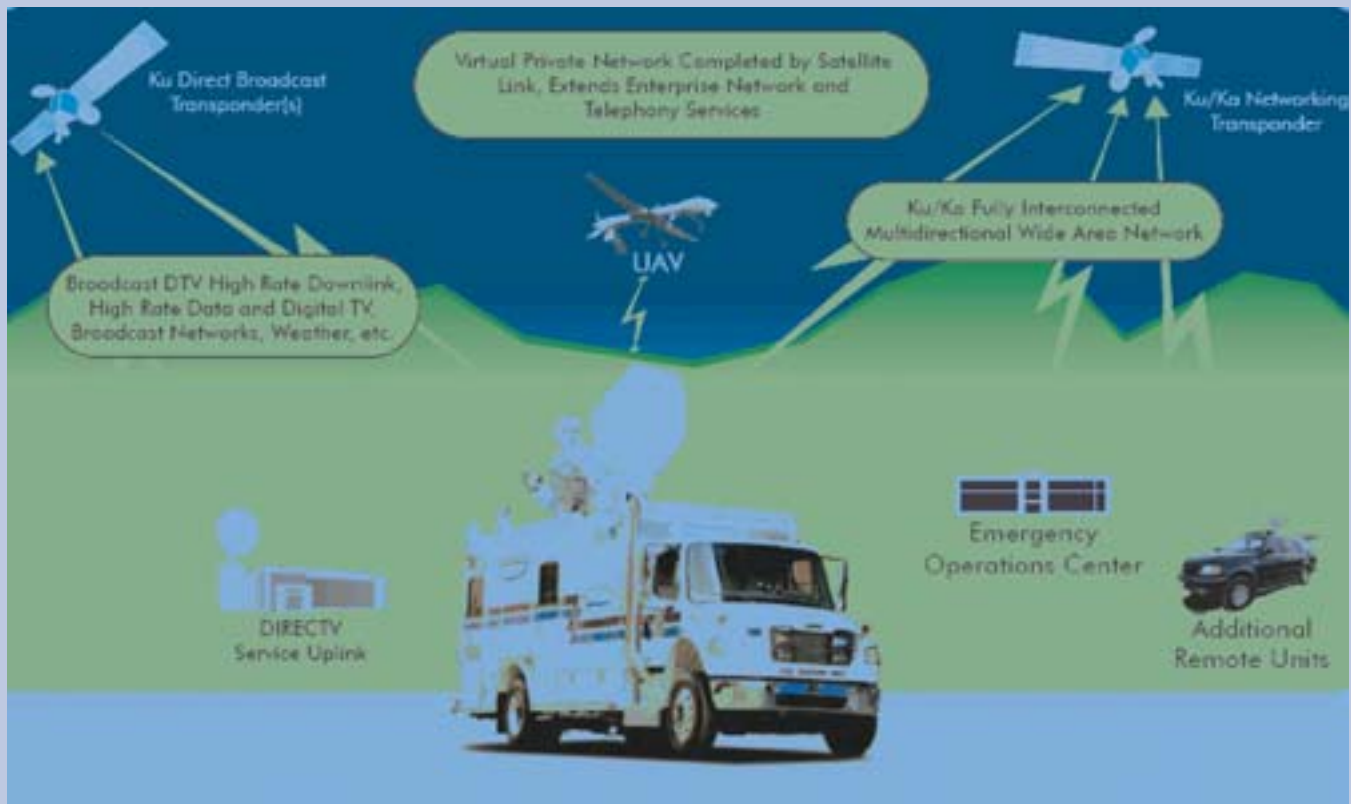
capability on the vehicle, and also to provide the maximum level of interoperability between the vehicle and existing emergency systems that support various agencies of the City of Chicago.

The system consists of four core components:

1. A large self-propelled vehicle (truck) containing all of the technology.
2. A large Ku-Band satellite hub terminal located in downtown Chicago.

3. A high-performance Ku-Band satellite link that connects the vehicle with the satellite hub.
4. A high-performance standards-based network, based entirely on the Internet Protocol (IP) that connects people and applications residing on the vehicle to people and applications in the OEMC and other locations as required.

Together, all of these components form the *Chicago Unified Command System*.



The core component of the system is a large truck capable of providing command, control, communications and logistics support for major incidents and events that affect the City of Chicago. The truck supports two fully-equipped dispatch positions — one for police and one for fire — and has three technical work stations. It is

equipped as an emergency vehicle, with lights, siren and in-cab compatible radio systems.

The truck can operate autonomously for up to two or three weeks with an onboard power generation capability that includes a high-capacity diesel generator. It can also draw shore power using a 50 Amp, 220 Volt receptacle and, in addition, can be

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

powered by a pigtail/lug connection from a light pole or a building. The truck is equipped with a high-performance fully-automated Ku-Band satellite antenna capable of supporting a high-capacity satellite link between the vehicle and a satellite hub facility. In case of a failure of the primary satellite link connecting the vehicle to the OEMC, the truck is equipped with a backup satellite link.

A high-performance IP network installed in the truck, at the satellite hub and at the OEMC, is dedicated to the Unified Command System and forms the core of the linkage between the vehicle and the OEMC. There are three core IP networks available to support the operations of the vehicle — Primary Satellite, Backup Satellite Link and Verizon EVDO Wireless, as well as Cingular HSDPA High-Speed Wireless Data.

The truck is able to receive commercial video broadcasts via satellite and can distribute video from various sources to any video monitor or broadcast element. Most of the 29 video displays on the vehicle are equipped with SDI inputs. The vehicle is also equipped with a full complement of Land Mobile Radios (LMRs) to support literally any frequency used by public safety agencies at the local, state and national level. One aircraft radio, one marine radio and one HF (Military) radio are all part of the package. And the vehicle is equipped with a JPS/Raytheon ACU-1000 radio interoperability system. This system allows the support of any new radio frequency (not already covered above) by simply plugging the radio directly into the ACU-1000 system.

One of the key functions of the Unified Command system is the extensive implementation of voice communications. This has been identified as an essential element that has been lacking in many recent national-scale disaster response scenarios. The Unified Command System provides the truck with 115 channels of dedicated voice. The onboard digital cellular switch will support three

primary means of communications — urban search and rescue, local/regional 911 capabilities, and dedicated cellular support for responders. All voice functions are carried over an all-IP network using a state-of-the-art, Cisco-based IP voice network infrastructure. Using this methodology all of the voice functions can be unified into the core IP network to provide maximum performance and flexibility.

Five patch panels both inside and outside of the vehicle feature a number of analog telephone jacks. These jacks can accommodate connections to fax machines, analog telephone handsets or classified STU/STE telephones.

The truck is equipped with a state-of-the-art ClearCom Digital Matrix Intercom system. Initially equipped with 64 ports, the intercom can be expanded to accommodate more than 200 ports if necessary. One intercom station is installed at each dispatch station and at each technical work station. An additional intercom station is installed at the patch panel in the truck's rear exterior. The digital intercom supports the establishment of ad hoc voice conferences, which allows any number of onboard radios to be connected seamlessly.

Two complete dispatch work stations are also featured equipment. These work stations are each outfitted with a full implementation of the OEMC's Computer-Aided Dispatch (CAD) application. This GIS-based application operates on a dedicated workstation for each position, with three dedicated 20-inch LCD monitors per dispatch station. In addition, each dispatch work station is equipped with a telephone handset, one each UHF and VHF land mobile radios, three small LCD video monitors, and an intercom station for the ClearCom Intercom.

The truck also features a 24" Plotter, a color laser printer, as well as a multi-function printer, fax and scanner. These three devices help to deliver the function and power of an office environment to the incident commanders. There is a

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers

large flat countertop work area in the center of the vehicle suitable for laying out large sheets of paper for mark-up or discussion. On the wall behind this work area is a 46" Clarity LCD moni-

tor, which is connected to VGA and KVM matrix switches. Ten additional LCD monitors and six computers in the truck are attached to the KVM and VGA matrix switches.

Case Study #2 – Hurricane Katrina

“Our operations were initially impeded by lack of adequate communications with our own units and other state, local and federal officials.”

Major General Harold A. Cross, The Adjutant General of Mississippi

Much controversy has been generated over communication system failures, particularly in the aftermath of Hurricane Katrina. Telephone lines and cell phones failed and because of unreliable and varying radio frequencies, emergency responders were unable to effectively coordinate rescue efforts.

In his testimony before the House Select Bipartisan Committee to Investigate the Preparation for and Response to Hurricane Katrina, Major General Harold A. Cross, the Adjutant General of Mississippi, indicated that initial response efforts in the storm and its after effects were seriously hampered by the military's inability to communicate internally with its own units, or externally with local and long-distance leaders.

As a result of Hurricane Katrina, the Federal Government continues funding emergency response as a high priority. In 2007, \$3.2 billion was provided in non-defense homeland security to support homeland security activities including establishing interoperability standards for first responders.

“This office will ensure that Homeland Security is exercising its leadership role to bring local, state, and federal efforts together in a partnership that is essential to national progress on interoperability,” said Michael Chertoff, DHS Secretary. “This is a national effort, not a federal effort, and I thank the first responder community for their initiative and collaboration.”

MorganFranklin's Chris Herndon said they were called in by New Orleans, a city with an interest in building in some redundancy and some additional capacities in their Public Safety Answering Point (PSAP) that supports the 911 emergency calling system.

“They heard about our communications vehicle in Chicago (see Case Study One) and then went to Chicago to look at it. They then called us and said they needed a vehicle to support their operations,” said Herndon. “We went to meet with them. We weren't in that first meeting more than a couple of hours before we said, ‘You need to take a big step backwards because it doesn't sound like a vehicle is what you need.’ This is a perfect example of how we look at a project from the requirements perspective.”

Special Report

MorganFranklin Guide: Interoperability Versus Assured Communications Critical Factors for Emergency Managers



MorganFranklin at a Glance **Delivering Solutions for High-Stakes Financial,** **Operational and IT Issues**

MorganFranklin delivers a combination of professional services and IT solutions for business and government leaders who face high-stakes financial, operational and IT objectives. Information is at the heart of the company's model, according to Robert Morgan, MorganFranklin's co-founder and chief executive. "We provide solutions that improve reliance upon, access to and competitive use of information across core operations and support functions for government and business.

We address our clients' high-stakes challenges by leveraging capabilities in a number of domains: finance and accounting, operations and management, technology and communications," he said.

MorganFranklin Delivers:

- Bullet-proof IT systems and communications net-

works to ensure secure and reliable access to data and intelligence.

- Accounting, financial reporting, risk management and audit support to help manage the complexity and scrutiny organizations face today.
- Process improvement, enterprise program management, IT strategy and business intelligence to help clients manage radical growth and change.

The company was founded in 1998 and is headquartered in McLean, Virginia. Today MorganFranklin serves national and international clients from expanding offices in Illinois, Maryland, Arizona, and the U.K. Facilities include corporate, integration labs, and engineering. The company brings technical and functional expertise from industry, consulting, accounting and audit, government and military backgrounds. Technical qualifications include CPA, CIA, CISA, CISSP, RCDD, MBA, Ph.D., PMP certifications, to name just a few.

MorganFranklin Corp.
1753 Pinnacle Dr., Suite 1200
McLean VA 22102
Phone 703-564-7525
Fax 703-564-7526

www.morganfranklin.com

Homeland Defense
JOURNAL

Homeland Defense Journal, Inc., Suite 1003,
4301 Wilson Boulevard, Arlington, Virginia 22203
Phone: 301-455-5633