

KEEPING CONNECTED DURING A CRISIS:
A CASE FOR THE INTER-GOVERNMENT CRISIS NETWORK



A Frost & Sullivan White Paper

TABLE OF CONTENTS

TABLE OF CONTENTS

Introduction	3
Figure 1- Emergency Response Communication Levels	3
Figure 2- Mississippi River Satellite Images, 1993 (Flood) and 2002 (Average)	5
Figure 3- Partial List of Hurricane Katrina First Responders	6
Current Situation	6
The Ideal Emergency Management Communication Network	9
Case Study-Hughes Network Systems	11
Conclusion	13

INTRODUCTION

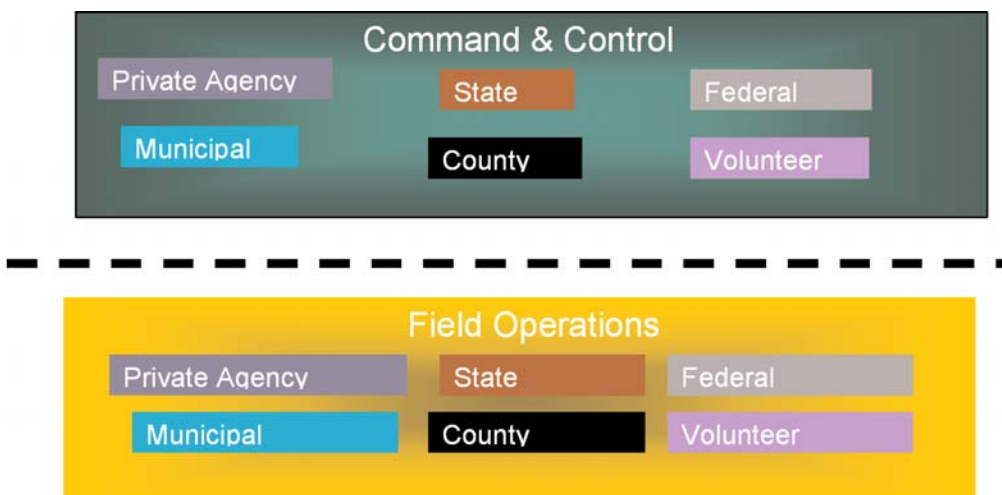
Communication is the lifeblood of the modern world. The ability to communicate with almost anyone, almost everywhere, and at almost any time is increasingly taken for granted at all levels. Individuals, organizations, and governments often plan for the future with the assumption that they will have the ability to communicate flawlessly. For those involved in emergency management, however, this is often not the case. When an incident occurs, whether caused by humans or an act of nature, successful emergency communications, particularly when involving multiple organizations, call for an in-place risk management strategy to ensure that a resilient communications network will be required.

Emergency communication occurs at two basic levels:

- field operations (tactical) and
- command & control (strategic)

Communication at the tactical level allows first responders and other “on site” personnel to communicate and coordinate their actions. An example of this would be the use of tactical radios by fire fighters in a major California brushfire. Such incidents often call for more fire fighters than California has on hand, requiring escalation. Frequently the National Guard takes part and fire crews are moved in from adjoining states. In extreme cases, personnel are brought in from all over the country. When these out-of-state contingents are combined with local personnel, state firefighters and National Guard contingents, they need seamless tactical communication to allow groups to interact and exchange information necessary to make the best possible decisions during the crisis.

Figure 1 – Emergency Response Communication Levels



Even in the same city there can be communications interoperability issues. In the 9-11 attack, for instance, it turned out that NYC Firefighters were unable to talk to the NYC Police Department. For the most part, these tactical issues are well on their way to being solved. Money has been allocated and equipment developed to allow better communication between different contingents of first responders, and progress continues to be made. Additionally, progress is being made on creating a common vocabulary for first responders to access unambiguous communications.

Although the needs of an individual emergency worker for communications are generally filled by voice and text messages (whether by radio, cell phone, or even satellite phone), the broader requirements for communications in an emergency situation are much greater. These requirements necessitate what might be called strategic level communications and are vital to effective emergency response even though they are often hidden or less-obvious. In fact, local command and control of first responders is the tip of the emergency communications iceberg. Like an iceberg, much of incident-related communication is below the surface and invisible to those who do not have to manage the response to a major incident.

The second basic level of emergency communications (strategic communications) is needed for applications such as streaming video, video conferences, transmitting large GIS files, VoIP, and other major uses of emergency communications bandwidth that are necessary for operational planning, damage assessment, and resource coordination. These do not directly improve the ability of an individual first responder to cope with, for example, a flood, but they are essential to enable risk-communications so decision makers can make informed choices on deploying first responders and assets. After a levy has been breached, there is relatively little that can be done. The time to deal with such an event is before it occurs by figuring out where a breach is likely and sending resources there to prevent it. Unfortunately, by the time such decisions can be made, it is possible that routine communications channels will already be degraded or destroyed, slowing both decision making and the implementation of the intended response. This is where current networks are weakest: not in the ability to coordinate efforts in the field (which have been greatly improved following the events surrounding Hurricane Katrina) but in the ability to move the large quantities of data necessary to coordinate the responses that put personnel in the field.

Once removed from the actual site of an incident there are a number of important decisions that must be made. The first of these is simply what level of response is appropriate. Just as all of the fire engines in a city are not sent to a house fire, the response to an event must be scaled to the event. This is true for a number of reasons, first, resources are always limited, and not only personnel and equipment but funding must be conserved. With this in mind, the first question a disaster manager must ask is “How bad is this event?” Comparisons of pre and post incident GIS data can help identify areas where a major response is warranted. Likewise a video feed from the field may justify an immediate rather than a delayed response.

Just as all of the fire engines in a city are not sent to a house fire, the response to an event must be scaled to the event. This is true for a number of reasons: first, resources are always limited, and second, funding must be conserved in addition to personnel and equipment. With this in mind, the first question a disaster manager must ask is, “How bad is this event?” Comparisons of pre- and post-incident GIS data can help identify areas where a major response is warranted. Likewise a video feed from the field may justify an immediate rather than a delayed response.

Another question might be, “How bad is this event, really?” A video conference between those on the scene and their EOC, or the EOC and other involved organizations, can clarify the path forward. As military commanders know, the reports from the field must be interpreted, and not accepted at face value. A report of a “major enemy attack” from one subordinate may require a vastly different response than for a substantially similar report from another subordinate. The need to assess the quality of reports was one point made by response managers in the research supporting this whitepaper. Video from the scene and video conferences offer a way to evaluate the true magnitude of an event.

Finally, it is not enough to be able to pass large files up and down a single chain of command. In most cases a major disaster will call for the coordination of efforts by various organizations, often from different states. In the 1993 Mississippi river floods, an area 745 miles in length and 435 miles in width, totaling about 320,000 square miles, was affected. Nine states -- Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin -- were involved over the course of the flooding (see Figure 1.1). Were such an event to occur today, with the current arsenal of communications tools, these states would all need to be able to exchange large GIS files at the very least. No adequate response would be possible without a broadly shared understanding of the facts on the ground. It is not clear, however, that current networks would be up to the task of maintaining the required connectivity. They would be providing not just tactical coordination but also capability for strategic coordination on the broader allocation of resources and personnel to deal with the entire situation.

Figure 2 - Mississippi River Satellite Images, 1993 (Flood) and 2002 (Average)



Source: NASA

In the recent, much less damaging, 2008 Mississippi flooding, FEMA’s Region V planning cell included representatives of the Department of Health and Human Services, Environmental Protection Agency, American Red Cross, U.S. Army Corps of Engineers, the Defense Coordinating Element and the U.S. Coast Guard. Other agencies involved included The Centers for Disease Control, The Department of Housing and Urban Development (HUD), The General Services Administration (GSA), The Bureau of Alcohol, Tobacco, Firearms and Explosives, The National Guard, and The Environmental Protection Agency (EPA). These agencies were largely engaged in the state of Illinois, not the nine states involved in the 1993 flooding. Had there been nine states involved, coordination would

“No one, including OSHA, was responsible for collecting information on the total number of response and recovery workers deployed to the Gulf Coast in response to Hurricane Katrina, and no one collected it, but ten federal agencies provided estimates showing that, on October 1, 2005, the agencies had about 49,000 federal workers in the Gulf Coast area. In addition, six of these agencies estimated that their contractors had about 5,100 workers in the area on December 1, 2005, but the other four either did not track the number of workers employed by their contractors or did not employ contractors.”

- Government Accountability Office (GAO) Report to Congressional Requesters, Department of Homeland Security, Progress Report on Implementation of Mission and Management Functions; Aug. 2007 - <http://www.gao.gov/new.items/do7454.pdf>

have been vastly more difficult. These difficulties are illustrated by the fact that no one knows how many first responders were involved in Katrina recovery efforts.

If it is impossible to determine the number of first responders with the benefit of hindsight, it should be clear how chaotic events were in real-time. Figure 3 shows a partial list of first responders and associated assets; this list ignores state and local personnel as well as non-Red Cross NGO personnel. Even this limited list illustrates the magnitude of the task of coordinating all of the assets in the confusion of a major incident.

Figure 3 - Partial List of Hurricane Katrina First Responders

Organization	Personnel	Assets
U.S. Coast Guard	4,000	29 Coast Guard cutters and 52 aircraft
National Guard	22,000	Assorted
FEMA	5,000	All 28 Urban Search & Rescue Task Forces. 39 Disaster Medical Assistance Teams (DMAT) 10 Disaster Mortuary Operational Response Teams (DMORT); 2 Veterinary Medical Assistance Teams (VMAT) 2 Mental Health Team Other assets (not called out)
Red Cross	74,000	Volunteers
Out of state local firefighters	1,000	Volunteers (paid by their localities)

Current Situation

A common theme that emerged in Frost & Sullivan’s interviews supporting this whitepaper was that agencies and organizations felt that they had communications issues under control. However, in spite of broad requirements for strategic coordination, not just tactical communication, the majority of planning to date seemed to have gone into tactical voice communications. More effort spent in planning the type of robust networks that would allow effective higher-level decision making during an incident would be highly valuable, and often seems to have been underemphasized in current planning.

Even in cases in which such networks have been established, many share a common weakness. It is common for broad incident response networks to lack truly redundant communications paths, making them subject to the same incidents they are supposed to ride out. It is not enough to use different telecom suppliers, one providing a backup for the other. The paths themselves, not just the providers, must be diverse or the same failure mode may occur with both. In the interviews conducted for this whitepaper, a broad array of network backup plans was revealed. Various organizations had degrees of redundancy, but by no means were all truly robust.

Two southern states provide an example of the contrasts discovered. In one state redundancy was provided by the use of different technologies; in the other it came from different providers. In the first state, routine communications were conducted over a fiber ring connecting a series of nodes. The nodes were also equipped with radio

backups, which were supported with deployable antennas held in reserve. The radio systems were powered by generators and were independent of the surrounding infrastructure. Even this layered approach was deemed potentially insufficient, however, as it could not provide the large bandwidths needed to support strategic decision making if the fiber links failed. As a result, these capabilities were augmented with a further backup of mobile, satellite-equipped communication trucks. These trucks were also frequently used to provide ad hoc communications for special events and other non-disaster oriented events in which terrestrial communications need to be supplemented.

This layered approach, using fiber, wireless, and satellite links, has proven quite robust in practice. And, the frequent use of the satellite trucks maintains operator proficiency for the ultimate backup. The key to its resilience is that it does not rely on any single communications technology. Indeed, it allows a series of fallbacks that, as conditions grow worse, damaging growing portions of the state's communications infrastructure, allow the network to continue operation.

In contrast, a neighboring southern state has an entirely fiber-based network. Redundancy is considered by this state to be the use of two different telecom providers. Individual state agencies may make provisions for satellite communications backups, but only if they make their own arrangements. The state's network, as a whole, does not have a communications backup plan beyond that of using multiple providers and being prepared to relocate personnel to backup network nodes. Such a network is not nearly robust enough to guarantee availability after a major incident.

Specialized state organizations are even less likely to have a broad portfolio of communications solutions. In another example of the differing approaches used in assuring communications, one Midwestern state health agency uses satellite phones as its emergency communications backup. The agency has a weekly status meeting in which all of its locations call in by satellite phone to discuss their status. This fills the double purpose of testing the satellite phones and assuring that everyone knows how to use them in the event of an emergency. As an internal "network," this is a well-thought out plan, but it is limited in its ability to contact anyone who does not retain access to a telephone or have a satellite phone in an emergency. While this does constitute a genuinely redundant communications path, it is not a particularly flexible one. It is limited in its available bandwidth, making it difficult to exchange the sorts of datasets that can be necessary for an intelligent, broad-scale response to a disaster. It could also prove to be difficult to make unplanned links when necessary.

Currently, then, each state has a different communications plan, using different technologies and or vendors, and make decisions based on varying assumptions. In part this reflects differences in geography, history and budget. The above referenced state that added satellite trucks as a final networking layer did not consider the incremental cost - a major issue to ensure a resilient back-up network. As a result, the satellite trucks are used for non-disaster purposes on a regular basis. A western state communications official

saw the price of satellite as prohibitive and stated that they had no satellite capacity as part of their communications plan. It should also be noted that the western state was not subject to the sort of widespread disasters (including hurricanes) that regularly occur in the southern state, in part because of their lower population density. In this case, budget constraints may be the result of priorities (based on history) not just population or tax base.

Historically, the majority of emergency response infrastructure and planning has been intended for natural, not human-caused, hazards. This is no longer the case, however. Since 9/11, in particular, there has been a fundamental shift in planners' concerns, with human-caused incidents now a major concern. Emergency preparedness since 9/11, has come to include a much broader range of potential threats. These new threats mean that old calculations, based on historical weather patterns or the likelihood of other natural events, are no longer sufficient. The western state that could choose not to deploy satellite systems because the probable events did not require it, must now consider a whole new menu of potential hazards. For instance, the destruction of a nuclear power plant upwind of this western state would require a response on a scale as large as, or larger than, that required in the case of the 1993 Mississippi flood or Hurricane Katrina. When considering human-caused, not natural incidents, history is not necessarily a reliable indicator of future needs.

The chance of major human-caused events similar to 9/11 is at an all time high. However, in addition to incidents such as terrorist bombings, in which a physical attack is made on physical infrastructure, there is an increasing danger of cyber attacks. These attacks may occur in coordination with physical attacks or may occur independently. In either case, it is increasingly important that networks used to support incident response functions be secure. The danger of cyber attack is yet another reason to ensure that incident response plans do not count on the public Internet for connectivity. The Internet can be jammed by legitimate traffic in the best of times but cyber attacks can result in a crippled, not just overused Internet. In such a situation, it will be vital that incident response does not depend on Internet availability.

For a number of reasons the federal government is better prepared in term of emergency communication than state agencies. A much larger budget, stronger technology base and substantial experience in large scale incidents all help maintain federal capabilities. In spite of these superior capabilities, in Frost & Sullivan's research, federal agencies still tend to focus on tactical level communications for their personnel. Federal top level administrators were described as having excellent communication capabilities, but respondents tended to feel that cross federal communications were less important than communication with the field.

Responses from federal officials did not reveal a strong concern with the need for the ability to form new networks to face unforeseen situations. However, this is clearly at the heart of the federal role. It is not enough for federal agencies to be able to maintain

According to former Senator Bob Graham, the chairman of the congressionally appointed Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, "Ours remains a world at risk and our margin of safety is shrinking, not growing," Further, "The commission believes that unless the world community acts decisively and with great urgency, it is likely that a weapon of mass destruction will be used in a terrorist attack somewhere in the world by the end of 2013."

old institutional relationships; they must be prepared to deal with the ever increasing possibilities of the modern world. This means that they must be able to coordinate with any state or local agency to address an event, natural or human-caused, that may arise.

Unfortunately, the Governmental Accounting Office (GAO) has reported that the major federal agency responsible for emergency response and communications, the Department of Homeland Security (DHS), has “faced difficulties coordinating with homeland security partners” and that “information sharing remains a challenge for DHS.” In other words the federal government is not yet prepared to provide the sort of coordination needed to respond to disasters that exceed the scope of state preparations.

It is critical to understand that the confusion noted by the GAO is generated by the inability of multiple agencies to coordinate response efforts at the decision maker level during life threatening situations. Even though first responders can communicate with each other in the field, they neither understand nor trust the orders passed down the chain of command in the various agencies on site. A viable solution, therefore, would focus on coordination and interoperability at the decision-maker level and not just on field personnel.

The GAO’s comments also highlight the importance of information security. In order for necessary cooperation to occur, all stakeholders must be confident that their proprietary or mission critical information must be protected. Again, although an aid worker providing medical services to disaster victims may not be concerned about communications security, it is crucial that decision makers be able to conduct their business in a secure fashion.

The Ideal Emergency Management Communications Network

Based on its discussions with various state and federal agencies that are involved in disaster response, Frost & Sullivan has determined the following five attributes as the ideal network to support emergency response decision makers.

I. The ideal emergency management communications network must be path diverse and robust.

Such a network must be able to function under considerable stress without degrading. It must withstand flooding, wind, fire, and the general destruction to the physical communications infrastructure and it must, therefore be path diverse. Only Satellite networks fully meet this criterion. Because the majority of a satellite network’s hardware is in orbit and the remainder small enough to protect, satellite-based communications are the most robust current communicate technology. They are particularly well-suited to serve as a backup to other network architectures, allowing a seamless overlay without regard to the technology of the individual network or network element being backed up. For maximum efficiency, both pre-positioning satellite terminals on key sites and buildings,

“DHS implemented a system to share homeland security information. States and localities are also creating their own information "fusion" centers, some with DHS support. DHS has further implemented a program to protect sensitive information the private sector provides it on security at critical infrastructure assets, such as nuclear and chemical facilities. However, the DHS IG found that users of the information system were confused with it and as a result did not regularly use it; and DHS had not secured of the private sector's trust that the agency could adequately protect and effectively use the information that sector provided. These challenges will require longer-term actions to resolve. “

- From GAO-07-454: Department Of Homeland Security: Progress Report on Implementation of Mission and Management Functions: Homeland Security Progress

as well as an arsenal of transportable satellite equipment (that can be brought in after the event) are necessary. This layered backup approach gives the primary networks a physically diverse transmission path, making them fully redundant. In addition, as transport into an affected area can be a major concern, the ability to preposition satellite backups has additional logistical value.

2. The ideal emergency management communications network must be broadband and MPLS like.

The requirement for data, such as large GIS files, by decision makers means that they must be connected by a broadband network. Often a fiber ring or the public internet is sufficient, but these are not mobile and may be disrupted by the same event that they are to be used to manage. The addition of a satellite system ensures that the capability to move much larger files will not be lost. It also allows field teams to teleconference with, and send video to, decision makers ensuring that they maintain full situational awareness while remaining far enough away from the event to function efficiently. In addition, satellite links are private (unlike the Internet) and allow mesh networks, and IP multimedia. This MPLS-like functionality allows them to merge into the terrestrial network where it is still operational. At the same time, they effectively replace it where it is not functioning.

3. The ideal emergency management communications network must not be expensive.

Cost is always a concern, particularly for state and local entities. Although dedicated satellite bandwidth may cost more than terrestrial bandwidth (depending on a number of factors) it is always available when needed. The latest systems allow bandwidth on demand solutions that change the fundamental economics of satellite networks in a way favorable to their episodic use, making them even more applicable to an emergency role. With a satellite network as a backup, any significant additional cost will occur when an incident occurs.

4. The ideal emergency management communications network must allow communications between supporting organizations.

This is the greatest challenge for any emergency communications network. Interoperability is the subject of ongoing funding and technology efforts, but remains an issue as seen in the GAO's Progress Report. Even in events such as Hurricane Katrina, in which the nature of the event was fairly clear, coordination was poor. In a more confused situation like that of 9/11, coordination will be even more difficult.

In particular, it is difficult to establish relationships before an incident when events are unforeseen. In an incident caused by human action, such as 9/11, it will be almost impossible to preplan a response. The ability to quickly form coordinated networks is

increasingly important. This is particularly true in large-scale incidents such as Katrina and the Mississippi river floods where, as we have discussed, large numbers of first responders from differing organizations and levels of government all need to have their efforts coordinated.

5. The ideal emergency management communications network must be secure against cyber-attack.

Although security is often relatively unimportant in tactical disaster operations (where communication is more important than secrecy), this is not the case with higher level, “strategic” communication. In extreme conditions, social order can break down (as occurred in Katrina) and it may be necessary to protect information about the location or disposition of vital resources. In the case of a human-caused event like 9/11 it is entirely possible the response will need to be kept under operational security. It is probable that future disasters will have national security aspects that will require both data and operational security as they may involve a response to an active opponent, not just post-event physical condition.

Case Study – Hughes Network Systems

Having examined the current state of and requirements for emergency communications, Frost & Sullivan now turns to Hughes Network Systems (HNS) proposed Inter-Governmental Crisis Network (IGCN). The IGCN is a novel approach to providing a satellite overlay on existing networks. At its core, it leverages the unique attributes of HUGHES Spaceway 3 satellite. Spaceway 3 carries onboard IP processing capabilities not seen previously in satellites. In fact, DOD is using Spaceway 3 as a prototype for its TSAT project which will culminate in flying its own IP-Switch. These packet processing capabilities allow HNS to set up pre-defined and ad hoc networks by using Spaceway 3’s onboard intelligence. With proper coordination and pre-planning among government agencies, HNS can establish an emergency network of networks of Spaceway 3-enabled customers, or logical “user groups” based on government policies. Also, in a matter of hours an entirely new network structure can be created, connecting Spaceway 3 users who were previously not connected. Thus, once a broad user base is established, IGCN can be used to form established user groups and ad hoc additions to these groups in near real-time. In addition, Spaceway 3 uses transponders transmitting in the Ka-band, offering significantly more bandwidth than previous C and Ku-band satellites. IGCN also allows high levels of security in its communications as well as the ability to tailor security to control personnel, who are able to gain access according to the needs during a particular incident.

1. The ideal emergency management communications management communications network must be path diverse and robust.

The strength of a satellite solution in this role has already been discussed but the

Spaceway 3 satellite has additional capabilities including the ability to mitigate rain fade by increasing transmission power over areas affected by severe weather. Since bad weather is strongly linked with a number of classes of emergencies, this is a valuable addition to the Spaceway portfolio. Other unique attributes are the ability to form mesh networks connectivity and NOC-less operations (no network operations center to fail and no terrestrial backhaul necessary in other satellite systems) allowing closer emulation of the fail safe nature of the MPLS and fiber networks that Spaceway 3 is backing up.

2. The ideal emergency management communications network must be broadband and MPLS like.

IGCN's use of Ka-band frequencies gives it superior bandwidth capabilities. It has the ability to offer uplinks of up to 2 Mbps and downlinks of up to 8 Mbps with the ability to handle and prioritize concurrent video, VoIP and data traffic concurrently from multiple locations.

3. The ideal emergency management communications network must not be expensive.

Current estimates put IGCN hardware costs at \$3,000 per terminal, with service packages technically and economically designed for COOP and Emergency Preparedness. IGCN leverages already existing Hughes infrastructure to provide a number of different service plans tailored for different budget and bandwidth needs. IGCN can also justify itself with the cost savings achieved when an expensive terrestrial backup network is replaced by an on-demand satellite network (IGCN). In effect, IGCN's disaster communications functions, user groups, backup connectivity, and all of a satellite solution's flexibility can be paid for by the savings gained by reducing the number of terrestrial networks that must be supported.

4. The ideal emergency management communications network must allow communications between supporting organizations.

This is the requirement in which no other system can come close to IGCN. The ability of Spaceway 3's onboard intelligence to create networks on the fly means that "pick-up teams" can be assembled in a matter of hours, however unlikely the necessary combination might be in terms of pre-event planning. Because IGCN can form user groups out of the total user base, it avoids the need to rush dedication network equipment into a disaster zone. Instead, existing IGCN users are given network access over preexisting equipment.

5. The ideal emergency management communications network must be secure against cyber-attack.

IGCN and Spaceway 3 are capable of the highest levels of security, beginning with the fact that it is a private network that goes directly to the customer's data center. Being separate from the Internet in and of itself allows for better security. In addition, it avoids the issues of a clogged Internet that could accompany an emergency characteristic of a cyber attack. In addition IGCN includes onboard AES encryption and is capable of transporting traffic that has been encrypted with Type 1 secure devices.

Hughes Network Systems, LLC (HUGHES) is the global leader in providing broadband satellite networks and services for enterprises, governments, small businesses, and consumers.

Conclusion

Hughes Network Systems' Inter-Governmental Crisis Network offers federal, state, and local governments an opportunity to fulfill their responsibilities to their constituents and prevent disasters such as those that followed Hurricane Katrina. The technical advantages of the Spaceway 3 based ICGN network, coupled with the potential organizational advantages of a broadly available network with costs mitigated by the scale of a commercially sold product and service plans designed around COOP usage patterns, make ICGN a truly superior answer for those who need to coordinate emergency response over a broad geographical and organizational range. With the increasing danger of human-caused incidents and the danger that climatic change will increase the number and ferocity of weather events, it is vital that the United States be prepared to deal with any incident that may occur. It is necessary that authorities be able to deal with any possible incident, anticipated or otherwise. ICGN would greatly increase the ability of the United States to deal with major incidents both human and natural, and enable government to fulfill its duty to its constituents in any situation.

CONTACT US

Beijing
Bengaluru
Bogotá
Buenos Aires
Cape Town
Chennai
Delhi
Dubai
Frankfurt
Kolkata
Kuala Lumpur
London
Melbourne
Mexico City
Milan
Mumbai
New York
Oxford
Paris
San Antonio
São Paulo
Seoul
Shanghai
Silicon Valley
Singapore
Sydney
Tel Aviv
Tokyo
Toronto
Warsaw

Silicon Valley
331 E. Evelyn Ave.
Suite 100 Mountain View, CA 94041
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SW1W 0DH, UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
<http://www.frost.com>

ABOUT FROST & SULLIVAN

Frost & Sullivan, the Growth Partnership Company, partners with clients to accelerate their growth. The company's TEAM Research, Growth Consulting, and Growth Team Membership™ empower clients to create a growth-focused culture that generates, evaluates, and implements effective growth strategies. Frost & Sullivan employs over 45 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from more than 30 offices on six continents. For more information about Frost & Sullivan's Growth Partnership Services, visit <http://www.frost.com>.