Custom supplement to Government Computer News and Washington Technology

Emergency Preparedness & Response

Inside:

Juniper NETWORKS

Since adding Juniper's remote access solution to his network, Frank is prepared for the occasional bad day.

>> **Get Ready:** Floods, snowstorms, pandemic scares, terrorist attacks, transportation strikes. If no one could get to work, is your office prepared?

Get Better: A Juniper Networks SSL VPN, with industry-leading security and functionality, keeps your employees working from anywhere. Juniper is the market share leader, offering superior Secure Access ICE (In Case of Emergency) licensing options and providing immediate Continuity of Operations (COOP) plans, ensuring remote access to critical resources and seamlessly keeping government and law enforcement agencies, public utilities, all businesses — including your business — running.

Get Juniper: For our free ICE Flash Presentation — a compelling walkthrough of continuity planning — plus webcasts, white papers, demos and more, visit www.juniper.net/getready or call 1.866.298.6428.

Juniper your Net™

1.866.298.6428

We Can Work It Out

NSPD-51 and HSPD-20 are paving the way. Technology is providing solutions. But people working together are still paramount when preparing and responding to emergencies.

"Try to see it my way
Do I have to keep on talking till I can't go on?
Why do you see it your way?
There's a chance that we might fall apart before too long.
We can work it out. We can work it out."

We Can Work It Out, The Beatles

The common denominators to make Emergency Preparedness & Response (EP&R) efforts truly work are culture and communication.

Talking, listening and working with one another trump technology in importance. Technology is important, but the technology is available for fully interoperable communications, geospatial applications and the inventory/logistics management and control needed for EP&R efforts.

What isn't there yet is a culture of open communications. But that doesn't mean people aren't working on it.

EP&R Leaders Speak Out

"The technology for interoperability has been solved," says Steve Cooper, American Red Cross CIO. "But the people protocol has not. We need people to have training to increase the level of preparation and response for everyone when they show up at a disaster scene."

"We've got to introduce ourselves to other responders prior to an emergency," adds Cooper. "Don't try to do it in the middle of a disaster."

"If you are in the government sector, then reach out and find out what your agency is doing and get involved with federal interagency working groups. If you are in the private sector, ask yourself, 'what are you doing to help government, non-governmental organizations and non-profits with their efforts?'"

The Department of Homeland Security agrees.

"The federal government needs to lead by example," says Dr. David Boyd, director of the DHS SAFECOM program. "We need to do our homework to make sure we have it right; that we have a roadmap in place and taken the time to not just to hear from, but ask for participation from those not in federal agencies that have to be involved."

"The technology is there and the capabilities are there, provided the cultural adjustments have been made," Dr. Boyd adds. "People must be willing to share. IT is a key component and it exists in virtually every jurisdiction. Listen to the people who own, operate and use most of the nation's infrastructure and ask 'how do we meet their needs?'"

"If you are in IT, take the time to participate in conferences. Talk to police, fire and other emergency response personnel. It's not enough to stay locked up in your EA and SLAs. You have to get down to where the rubber meets the road."

The Department of Health and Human Services concurs.

Dr. Steven Phillips is leading the National Library of Medicine (NLM) effort to develop the Disaster Health Information Management Research Center. The DHIMRC (website to be launched in 2008) is part of the federal effort to prevent, respond to, and reduce the adverse health effects of disasters in partnership with federal agencies, local communities and their public health workers.

"That means actively partnering with FEMA, DOD, DOT, and the EPA, public health institutions, and international organizations to provide access to health and scientific information that support programs related to Disaster Preparedness and Response," explains Dr. Phillips.

The White House and Congress Weigh In

As reported in GCN, President Bush signed NSPD-51 and HSPD-20 outlining the strategy for preparing the federal government to continue running during a national emergency such as a terrorist attack or a natural disaster.

The new directive requires that continuity plans be part of daily operations of all federal agencies. Emphasis is being placed on geographic distribution of agency leadership and infrastructure to keep key government services operating during an emergency. All agencies will appoint a senior-level official to serve as their continuity coordinator.

Recently Congress surveyed agencies on their Telework policies, deemed critical to COOP efforts. New "Telework friendly" legislation is in the offing. They are trying to identify "Telework roadblocks" and come up with solutions to overcome resistance.

Read more about how the Red Cross, SAFECOM, the DHIMRC and Telework can help all of us say "we can work it out". •

Technology Transfusion

The Red Cross is counting on innovative uses of technology to deliver services during a disaster.

"We've got 35,000 dedicated Red Cross permanent staff and almost 1 million volunteers whose single mission is to assist people they don't even know," says CIO Steve Cooper proudly.

"Anything we can do to leverage technology to enable all these individuals to help other human beings is what we are all about."

Leveraging technology is critical to Red Cross preparedness and disaster response efforts. When you respond to more than 70,000 disasters a year (mostly fires) technology is an essential tool. And especially when history tells Red Cross officials that even during a "normal hurricane" (though Cooper says there is nothing "normal" about a hurricane), 10,000-20,000 families will need some type of assistance.

2004 and 2005 were far from "normal" hurricane seasons. In 2004, there were four hurricanes back-to-back in Florida. According to Cooper, that aggregation represented the largest natural disaster the Red Cross had responded to in its 125 year history.

"We assisted 75,000 families, which in Florida translates into 150,000 people," Cooper noted.

2004: Technology To The Rescue

Prior to 2004, the Red Cross's historical model for service delivery in disaster response has been through a face-to-face meeting. A trained case worker (either a staffer or volunteer) sits down with those affected by the disaster.

"We call them clients," explains Cooper. "They meet and ask questions such as: What damage has occurred? How many family members? Does anyone need special health services – mental or medical? Do you need clothing or shelter?"

After the discussion a decision would be made detailing all the services the Red Cross can provide. Assistance would be from time the disaster strikes to when they can go back into their home; or when other providers, such as insurance companies or federal, state or local governments can step in to provide assistance on a longer

Continued on page 6

Listen and Learn

Using a "bottom-up" approach, the SAFECOM program got input and feedback from emergency response practitioners to develop Statewide Planning Resources to address communications interoperability.

"Mundane, but important," declares Dr. David Boyd, director, Command, Control and Interoperability, Science and Technology Directorate at DHS.

That's how Dr. Boyd, who heads up DHS's SAFECOM program, describes the recently published set of criteria for statewide interoperability plans.

"Using a 'bottom-up' approach, we listened to emergency responders whose forte is responding to emergencies, not writing policies and procedures," explains Dr. Boyd. "The result is a template on how to write governance agreements and a template on how to put together SOPs and MOUs between agencies."

Developed as part of the Recommended Federal Grant Guidance for Emergency Response Communications and Interoperability Grants for Fiscal Year 2007, it provides "the most relevant guidance and tools available to assist in developing statewide interoperability plans".

DHS has defined interoperability as "the ability of emergency response agencies to talk to one another via radio communication systems and to exchange voice and/or data with one another on demand, in real time, when needed and when authorized".

DHS describes SAFECOM as "a communications program that provides research, development, testing and evaluation, guidance, tools, and templates on communications-related issues to local, tribal, state, and federal emergency response agencies working to improve emergency response through more effective and efficient interoperable wireless communications".

Bottom-Up Benefits

According to Dr. Boyd, the Statewide Planning Resources, which are available for download at www.dhs.gov/safecom, include:

Statewide Interoperability Planning Guidebook, which provides an explanation of the statewide plan criteria, a step-by-step guide for developing an interoperability plan, and a recommended layout for the statewide plans. Detailed explanations include common questions to consider, helpful

Continued on page 8

For Telework To Work Takes Work

COOP requirements along with proposed new legislation call for agencies to prepare for "alternative work environments".

Attention federal managers! Are you ready?

With HSPD-20 now in place, how are you planning to maintain operations if your agency is snowed out for a day (almost a yearly occurrence)? Or your building is flooded (like the IRS was for six months)? Or longer if something worse happened?

When the public calls Uncle Sam for help, who is going to attend to America?

Your agency's COOP should contain the answers. One of those answers to keeping the workforce working is Telework, which technologically is very much like delivering applications to that mobile worker who is using a laptop or PDA while attending a conference or on out-of-the-office work-related business.

Telework EXCHANGE
Eliminating Gridlock

A Sticky Topic

Although Telework has been around for a long time, only since 9/11 has it begun to pick up wide-spread support. Add to that the traffic woes that plague most metropolitan areas and Telework may just be ready to explode.

Just ask Cindy Auten of the Telework Exchange. The Telework Exchange is one organization dedicated to promoting the productivity and preparedness aspects of Telework. (www.teleworkexchange.com)

"People are really stepping up and looking at the business continuity issue and incorporating Telework into their plans," Auten explains.

"We are seeing a lot of instances where natural disaster preparedness is very critical. Telework fits into that. It is a part of a contingency plan, it is not the solution. But it's very important to maintaining operations."

That fact has not been lost on GSA, which issued new telework guidelines that clarifies security requirements for Teleworkers and reduced agencies' equipment burdens for off-site workers.

Now, not all Teleworkers will require access to their agency's centralized information systems; some can work effectively having

Continued on page 10

Continued from page 4

Technology Transfusion

basis if needed.

In 2004, "we introduced laptops in the hands of those caseworkers and for the first time our emergency response and case work was actually being done in real time," says Cooper. "We had 15-20 case workers who fed the information wirelessly to a nearby emergency vehicle where the server was set up."

Case workers used a Red Cross developed application called Client Assisted Services (CAS) to gather the information. Further, "we also attached to that application the capability to load and issue debit cards," states Cooper.

"Literally on the spot we would load a debit card the user could take to merchants to buy food and other necessities. It was the first time we rolled out the technology and it worked."

2005: The Katrina Challenge

During Katrina the Red Cross was faced with assisting 1.4 million families which translates to 4.1 million individuals.

"We had designed that CAS to scale," says Cooper. "But we never imagined scaling 20 fold and our application couldn't accommodate data as rapidly as needed. And there was no way to provide face-to-face casework to assist 1 million families, especially with people being relocated all over the U.S."

That reality meant a change of plans. "We made a decision 3-4 days after levees breached, when we realized the worst was happening," explains Cooper. "We had to change the mechanism by which we provided case work and emergency financial assistance."

The change was to use technology and stand up a Call Center from scratch; something the Red Cross had never used for the delivery of casework. From scratch it was operational in six weeks.

But the reality was, while the Red Cross could handle the volume technically, there were simply not enough case workers despite adding satellite offices and working 24/7. Still the effort was a technological success according to Cooper.

"We used technology to stand up a Call Center, gave trained agents laptops and they adjudicated cases by phone," explains Cooper. "We distributed emergency financial assistance through a partnership with Western Union, who, with the proper authorization number, distributed the money the case worker had agreed to provide to victims. That was the first time that was ever done."

"Leveraging technology is critical to Red Cross preparedness and disaster response efforts. When you respond to more than 70,000 disasters a year (mostly fires) technology is an essential tool."

–Steve Cooper, American Red Cross

2007: Ready to Serve

Fast forward to now, when the Red Cross has completed a very successful pilot program using the Louisville, Kentucky chapter. "We are now moving to a steady state Contact Center to deliver all of our assisted services during the tornado season," Cooper says. "We're now working with a couple of providers and although it's not in place yet, we will be prepared to use a Call Center to adjudicate cases along with face-to-face meetings to provide disaster services and where necessary to provide emergency financial assistance."

The Red Cross is preparing to scale up to serve 80,000 to 100,000 families if necessary through current models. If the number rises above 100,000 for a single event then it becomes catastrophic.

"We put together an agreement with FEMA where they have agreed to take the lead in a catastrophic event," says Cooper. The Red Cross plays a support role and will handle 10% of what FEMA does.

"We are now restructuring our Contact Center to handle 10,000 to 20,000 on a "normal" basis, but be able to scale to 100,000 in a reasonable period of time – 10 days. We have adapted the use of a Contact Center to process mechanisms, tools and methodologies that we have historically used for delivery of disaster services," says Cooper.

Future View

Currently the Red Cross is seeking input in two key areas of technology from industry.

The first is wireless. "We need to leverage more wireless capabilities," says Cooper. "We want to sit down with industry and tell them the challenges we face and ask them for ideas on how we could use wireless to connect shelters, to actually put real time capability on the ground around damage assessment and help us improve our technical capabilities."

The second is geospatial. "I want computer maps that can be accessed on cell phones so responders can find instantly information such as where is the nearest hospital, police station or fire house," adds Cooper. "And with GPS I can track where my own workers are."

Cooper has words for those in government as well. "If you are in the government sector, then reach out and find out what your agency is doing and how it is involved in preparedness and response. Then take action." •

06.017.07

A change in conditions requires a change in approach

In today's world, emergency managers face a complex and ever-changing array of challenges—from assessing and mitigating risks and assuring interoperability to developing strategic training exercises and managing the grants process. Each aspect is critical for not only saving lives and protecting property, but for achieving the highest levels of preparedness and response.

Booz Allen Hamilton, a global strategy and technology consulting firm, has proven expertise in helping emergency managers address these challenges and meet their goals through an integrated, collaborative approach. We work side-by-side with clients, sharing our experience and knowledge and developing effective, integrated solutions for today's emergency managers. Booz Allen is committed to delivering results that endure.

Booz | Allen | Hamilton

delivering results that endure

www.boozallen.com

Continued from page 4

Listen and Learn

hints in completing each section, and a list of the criteria each section addresses.

Formatted Statewide Plan Template, which was developed to assist statewide communications interoperability planners. Once content has been identified, it may be loaded into this template.

Statewide Communications Interoperability Planning (SCIP) Version 2.0, which provides a step-by-step guide for developing a locally-driven statewide strategic plan. The approach detailed in the SCIP Methodology Version 2.0 captures lessons learned from Kentucky's and Nevada's statewide planning processes, and may be modified and applied at all levels (local, tribal, state, and federal) nationwide to develop a practitioner-driven strategic plan.

Frequently Asked Questions for Statewide Plan Criteria which provides a comprehensive list of FAQs that address statewide plan criteria.

Promising Research Results

6,816 agencies responded to the 2006 National Interoperability Baseline Survey. The poll was the first interoperability assessment that used a comprehensive definition for interoperability. It was designed in partnership with the emergency response community and assessed stages of development in five areas: governance; standard operating procedures; technology; training and exercises; and usage. Respondents were evenly split among law enforcement, fire response and EMS.

"2/3 of the respondents said they engage in interoperability for scheduled events such as a Thanksgiving Day parade," Dr. Boyd reports. "That's good news because it means that the technical means for interoperability are present in most agencies throughout the U.S."

While that's good news technically, Dr Boyd notes that interoperability is not ever-present. "They haven't institutionalized the non-technology components required to achieve interoperability," explains Dr. Boyd. "There is no governance process, no SOPs, no training and exercises. Interoperability only occurs around those specific events even though the technical ability is really there."

Even though this shows there is much to do, Dr. Boyd is buoyed by the findings. "It tells us to continue to stress those non-technology components of interoperability and it is possible to achieve emergency levels pretty quickly. We know they can do it."

Hence the Statewide Planning Resources.

"The second thing we found was that interoperability tended to be effective in adjacent jurisdictions or within the jurisdictions," says Dr. Boyd.

"We have a series of rapid communications capabilities in cities that we didn't have before: Boston, Chicago, Houston, Jersey City, Los Angeles, Miami, the National Capital Region, New York, Philadelphia, and San Francisco," declares Boyd. "The localities drove it and we just tried to facilitate things and they were able, using what they had on board, to establish a command level of interoperability."

"But the most important observation to make is consistently the most successful projects are those that are driven from the local level that make sure that they meet their needs," says Boyd. "They are the guys who are pointing the stick and are going to do things, and then build them up to larger state-wide types of plans."

And what are the least successful according to Boyd? "The least successful are those that are driven hard from the top down and don't adequately involve localities from the very beginning. And that's not surprising. After all it's the local guys who own, operate and maintain some 90% of the nation's public safety wireless infrastructure."

The Culture Challenge

"The biggest of all the challenges has to do with cultural change. It has to do with how you think about governance, how you think about making systems work together," adds Dr. Boyd.

Adding to the challenge is how you create joint standard operating procedures so that everyone can work together says Boyd. "Probably the stickiest of all the problems is how are you going to pay for all of this? We need the political leadership commitment beyond anything that we had since the Eisenhower Interstate program."

"To make interoperability work, listen to the folks who own and operate most of our critical infrastructure and the people who use it and respond to emergencies. Develop a customer focus and ask how do we meet their needs?"

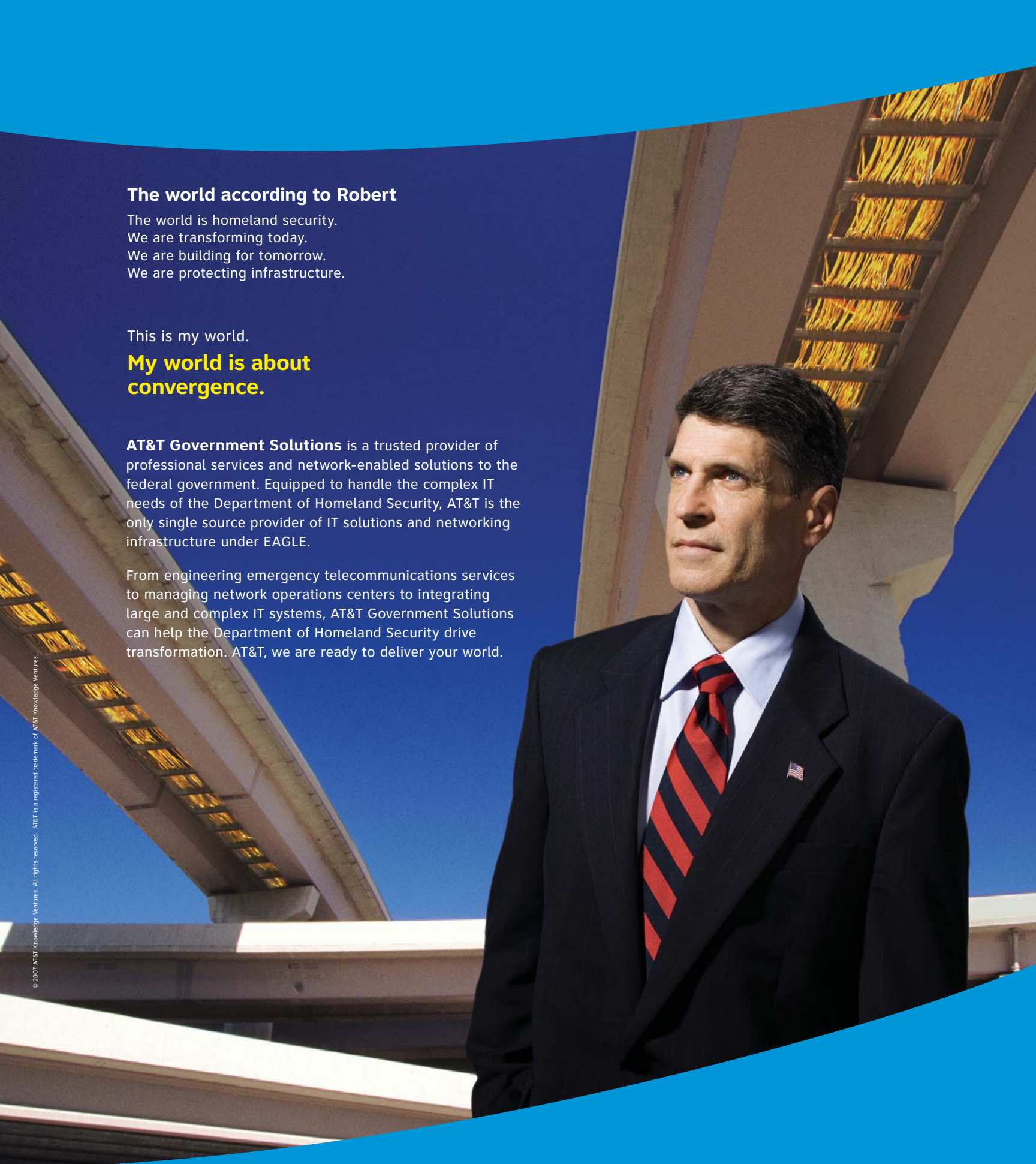
–Dr. David Boyd, DHS

The technical capabilities exist according to Boyd. "But unless you do the non-technical pieces – the planning, training, governance and SOPs – interoperability will not reach full fruition."

That's why over the next few months, Dr. Boyd will be working with states on planning and why over the next 1-3 years he will be leading R&D on ways to make interoperability simpler and cheaper.

"We have funded workshops for instructors through the National Governors Association and the National Association of Counties to continue our work with the states," says Dr. Boyd.

"We will continue to solicit the ideas from a broad array of industry providers, federal/state/local agencies and first responders on how to best address interoperability over time from both a technology and non-technology perspective." •



The world according to Robert

The world is homeland security.
We are transforming today.
We are building for tomorrow.
We are protecting infrastructure.

This is my world.

My world is about convergence.

AT&T Government Solutions is a trusted provider of professional services and network-enabled solutions to the federal government. Equipped to handle the complex IT needs of the Department of Homeland Security, AT&T is the only single source provider of IT solutions and networking infrastructure under EAGLE.

From engineering emergency telecommunications services to managing network operations centers to integrating large and complex IT systems, AT&T Government Solutions can help the Department of Homeland Security drive transformation. AT&T, we are ready to deliver your world.

att.com/gov/EAGLE

The new at&t
Your world. Delivered.

Continued from page 5

For Telework To Work Takes Work

only e-mail and telephone contact with HQ.

According to the guidelines, "A user who Teleworks one or two days per week, and whose job consists largely of writing and document preparation, may never need to login to agency systems from an alternative worksite".

However, Teleworkers who must be connected to their IT systems must use a VPN to make certain their off-site computer is as secure as office computers. GSA's new guidelines also recommend agencies update their Help Desk support for Teleworkers, including knowing how to run diagnostics for troubleshooting.

Congress has also begun to see the wisdom in Telework. "New proposed legislation clarifies a lot about eligibility," says Auten.

New Telework Legislation

The Telework Enhancement Act of 2007, proposed on March 27, 2007 includes a requirement for each agency to create a new position, the Telework Managing Officer (TMO), who is responsible for their respective agency's telework programs.

"We stress to agencies it's important to establish a Telework policy and a program for COOP. Then test it out, train for it. Have your Teleworking employees actually Telework and they will be technologically ready and culturally ready in case of an emergency as well."

–Cindy Auten, The Telework Exchange

Specifically, the bill clarifies the definition of Telework by defining it as a work arrangement in which an employee regularly performs official duties at home or other worksites at least two business days per week on a recurring basis.

"It says all people are eligible unless otherwise stated," Auten explains. "This completely flips the eligibility requirements from before. Now everybody will be eligible. A manager who previously said none of my employees are eligible, now is going to have to provide background as to why they are not."

It Takes Work

For Telework to work takes work says Auten.

"Telework has to be incorporated into your standard operating procedures. I think that you can't just turn around and say you are teleworking tomorrow, there has to be training involved, it has to almost become natural," notes Auten.

"We stress to agencies that's why it's important to establish a Telework policy and a program for COOP. Then test it out, train for it. Have your Teleworking employees actually Telework and they will be technologically ready and they will be culturally ready in case of an emergency as well."

There is also the security issue to deal with. "You have to have the infrastructure and policies set in place on how to handle sensitive and classified information with your employees," adds Auten.

When Telework Works

Auten says successful Telework programs such as the one at PTO and DISA happen when there is a dedicated Telework Coordinator who is responsible for enhancing Teleworking and marketing Telework within each agency.

"Interestingly in this new legislation one of the requirements is actually to bring on board a Telework Managing Officer. It is a full time senior level Telework coordinator," says Auten.

Right now, according to Auten the major challenge is management resistance. "How do you get management on board to Telework? I think that you can't ignore technology, but the technology is there. But the major area is cultural, learning how get work done in a distributive environment. There is management resistance because may like to be able to talk to my employees face to face; I want them in the office next door."

Success stories come from building base programs, training your employees on dealing with cultural and technology issues and incorporating other agencies best practices. "There are some amazing programs out there and they have some great advice they are very willing to share with other agencies on how to build a program," Auten says.

Whether staff is mobile or Teleworking, the bottom line for success will be maintaining and growing productivity.

For Auten, productivity is very important. "A lot of people talk about the issue of productivity and a performance management system. By establishing a performance management system to focus on their work output Teleworking can almost become transparent."

Auten sees a bright future for Telework. "I think Telework is going to be 'going green'. There are a lot of perfect storm issues pushing Telework forward and we are going to see a lot less cars on the roadways and we are going to see a better work/life balance and we are going to have productivity increase."

"We are going to see agencies that are equipped to handle disaster preparedness and they are actually saving a lot of money. The ROI in Telework and recruitment is going to be huge in the next 5 years and I think that's where the government needs to really focus too." •

Smart Solutions

Application Delivery is the Key to COOP

Under the ongoing threat of a terrorist attack, pandemic, or any other natural or manmade disaster, the federal government is working to sharpen disaster recovery response plans. Extensive continuity of operations planning (COOP) initiatives are under way, involving network security enhancements, offsite recovery locations and tactics to speed recovery. At the same time, agencies must navigate the federal regulatory COOP requirements as directed in Presidential Decision Directive 67 and Executive Orders 12656 and 13286. Not only must continuity preparations mesh seamlessly with current agency IT plans, they must also be flexible enough to function in nearly any scenario. In a pandemic or highly contagious influenza outbreak, for example, federal workers would very likely be ordered to stay at home. Demand for telework would soar, and federal emergency managers now worry how they will ever be able to support the explosion of traffic on current agency networks.

The Gartner Group[1] recommends all organizations have IT response plans that, at a minimum, will:

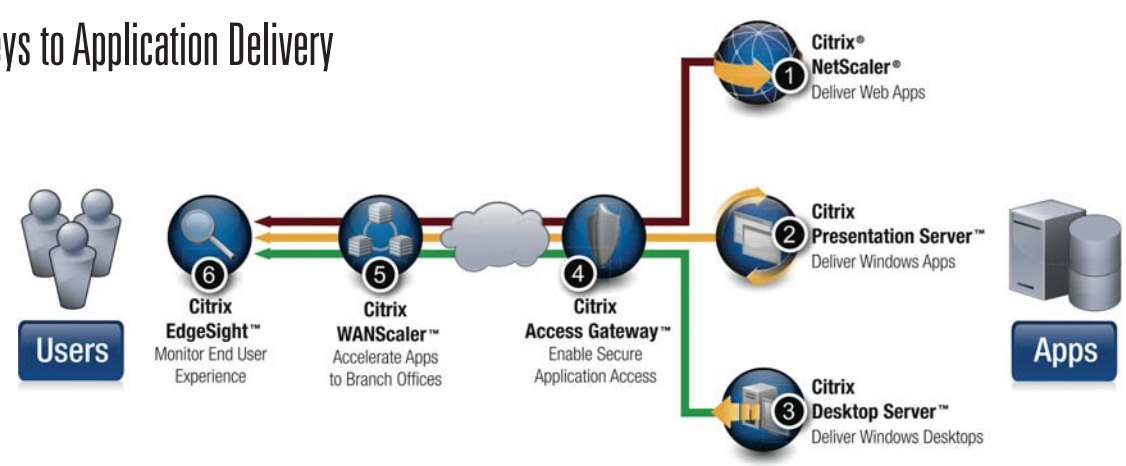
- Enable large numbers of employees to work from home for extended periods;
- Provide the means for workers to collaborate remotely;
- Maintain consistent communication with partners, constituents and other stakeholders.

To ensure continuity in times of crisis, federal agencies are turning to Citrix's Application Delivery Infrastructure. In the aftermath of an emergency, employees can use any computing device to securely access mission-critical applications and information, from anywhere, over any connection – wireless to Web. If the data center is affected, the Citrix application virtualization platform enables IT managers to redeploy critical applications at a backup location quickly – and with complete transparency to users – reducing or eliminating the need to rebuild networks and desktops. One component of this solution is the Citrix Access Gateway, a universal SSL VPN appliance that provides secure, always on access to applications, while protecting information, even when users must connect over public networks during an interruption. Citrix's SSL VPN appliance is ranked in the Gartner Group's Magic Quadrant and rated as competitive by Forrester Research.

Citrix is a trusted provider of secure application delivery solutions to the federal government, military services, the intelligence community, systems integrators, as well as state and local governments. As a vital component of any government COOP initiative, Citrix plays a central role in helping agencies and departments to connect remote workers,

[1] *"Use Good Business Continuity Management to Prepare for a Disaster," Gartner, Inc. 2005.*

Six Keys to Application Delivery



CITRIX **For more information, and to read the 2007 Gartner Magic Quadrant Report on Application Delivery Products, please visit www.citrixfederal.com/COOP.**

Just In Time, Just What I Need

The Disaster Health Information Management Research Center (DHIMRC) is being developed by the National Library of Medicine (NLM) to be the U.S. Government portal to provide tools, information & research to assist with disaster preparedness & response.

"It was very unusual," says NLM's Dr. Steven Phillips. "After Katrina, people noticed many of the displaced were going to libraries. The public just took it upon themselves and basically that's how the whole thing got started."

What seemed unusual was that Katrina victims and government responder agencies alike were using libraries. Why? Because libraries often had Internet access and wireless connectivity. Victims used them for information on federal recovery programs and to register so they could find their relatives and their relatives could find them.

What the public got started has resulted in HHS/NIH/NLM efforts to develop the DHIMRC.

Dr. Phillips is heading up the NLM effort. He is a heart surgeon who spent the majority of his career practicing in Des Moines, Iowa. In 1993, he became an NLM Board of Regent member, chaired the Board in 1997 and from 1999-2002 served as NLM deputy director of research. Then he left government, did some consulting and basically retired.

He came back earlier this year to head NLM's DHIMRC efforts at the behest of NLM director Dr. Donald Lindberg. "I said sure but 'why me, I don't know a lot about disasters?' He said 'well you are a heart surgeon; you have dealt with a lot of disasters'." That may have been said "tongue in cheek", but Dr. Lindberg knew Dr. Phillips also has the organizational skills and the institutional knowledge to "do the heavy lifting" needed to meet NLM's DHIMRC basic mission, which is to collect, organize and distribute information.

"The DHIMRC challenge is how to deliver the right information in the right format to the right person at the right time."

–Dr. Steven Phillips, National Library of Medicine

The NLM Long Range Plan

In 2006, the responsibility for the medical component of Disaster Management moved from DHS to Health and Human Services.

The 2006-2016 NLM Long Range Plan recommends NLM ensure continuous access to health information and effective use of libraries and librarians when disasters occur. A further goal is to establish the DHIMRC "to support NLM's strong commitment to disaster remediation and to provide a platform for demonstrating how libraries and librarians can be part of the solution to this national problem".

This will ensure effective recognition and the use of libraries as a major and largely untapped resource in the nation's disaster efforts.

According to the plan the goals of the DHIMRC are:

To maintain information access and research best practices for sustained access to health information during and after disasters. The research will support the Common Operational Picture and COOP concepts to ensure timely, continuous access to crucial "just in time" and "just what is needed" information by federal agency health professionals, first responders, public health workers, patients and families.

To partner the National Network of Libraries of Medicine's (NNLM) eight regional libraries and nearly 6,000 member libraries and public library colleagues with their local and regional emergency responders to enhance the network's key role in providing disaster information and training at the local level. The NLM with the NNLM will be the information triage hubs of health information for disaster preparedness and response.

To identify health topics and resources essential for all-hazards preparedness, disaster response, and recovery through the NLM Literature Selection Technical Review Committee (LSTRC).

To develop new tools that focus on online and off line management during a disaster, such as the Wireless Information System for Emergency Responders (WISER) and Radiation Event Medical Management (REMM).

To research options and programs for "real time" syndromic and other surveillance technologies to alert officials to anomalous clusters of biological and related events.

These and other tools will provide access to: information about acute injuries and outbreaks; effective management of chronic illnesses under stressful disaster conditions; clinical consultations and expertise; and patient information and communication technologies.

Planned 2008 Debut

Access to the information – when the portal is up and running most likely in 2008 – will be free to the public. One of Dr. Phillips objectives is to get Congress to put wording in a bill specifically about the DHIMRC. "Get authorization and it's easier to get appropriations," Dr. Phillips says.

At the same time, Dr. Phillips has been researching. "I started going to grass roots, continuity of operations meetings with mostly disaster responders, fire chiefs, police chiefs, community planners, in places like south Florida and Georgia," explains Dr. Phillips.

"The meetings had maybe 50 to 100 people, but these are the ones who are really doing the work. I went to find out what they need and to let them know that we were starting this information center, because there was no central government center for information."

"My objective is to just gather information related to any form of disaster with the concept of reducing the adverse health effects related to disasters. So we are not really concentrating on dirty bomb information or on hurricane or on any specific type of event. We just want to see what people need and try and gather and prioritize the information related to what is needed." •

trusted advisers.
focused on you.

Federal agencies have a communications partner with the experience, the know-how and the ability to deliver advanced Networx solutions. For nearly 10 years, agencies have relied on our world-class team to deliver highly reliable, secure communications under FTS2001, WITS and other major federal programs. Now we will deliver on Networx.

The experience and management capability that Verizon Business brings to Networx Universal and Enterprise helps ensure that all of your needs are recognized, analyzed, and prioritized during the transition process. This enables the Verizon Business team to focus on one successful outcome -- yours.

verizonbusiness.com/federal

verizonbusiness

Custom supplement to Government Computer News and Washington Technology

Interoperability It's in the Network!

There really are very few technological reasons for interoperability issues to hinder emergency responders.

Commentary By Jim Flyzik, The Flyzik Group

We have been discussing incompatible, aging communications technology as a major barrier to effective disaster response for several decades. Reports abound with stories of public safety and law enforcement agencies failing to communicate during crisis situations. A report earlier this year from the DHS indicated most of the cities the Department examined lacked the infrastructure needed to communicate promptly and coordinate action in the event of a major disaster.

There really are very few technological reasons for interoperability issues to hinder emergency responders. The problem is the discussion has focused almost exclusively on the devices being used to communicate such as land-based mobile radios, cell phones, and PDAs. While devices such as the radio certainly play a critical tactical role, the danger is that such a narrow focus limits the potential effectiveness of emergency responders. Let's examine "who" needs to communicate.

- Federal law enforcement personnel need to communicate with one another and with state and local counterparts.
- Emergency response personnel need to communicate with one another and with federal, state and local government officials.
- Non-Governmental Organizations, such as the American Red Cross need the ability to communicate with government officials and first responders.
- DoD personnel and the National Guard may be required to communicate with various stakeholders.

And of course, a variety of private sector entities may be called upon to assist in any response situation.

It is just not feasible to ever expect all these entities to communicate using one type of communication media such as a land-mobile radio.

Moving to a converged network doesn't have to involve an expensive replacement of existing systems. When emergency communications technologies are layered upon an existing, field-proven infrastructure, there is nothing to throw away.

Alternatives Must Exist.

The real gaps in interoperability are caused by underlying communication networks that are unable to connect to every possible device – from radios and desktop phones to cell phones and PDAs. A truly effective emergency response involves coordinating people and information across diverse systems, devices and locations – including disaster sites, offices and staging locations – and doing so with the fewest "handoffs" possible.

Open, standards-based converged networks, which combine disparate voice and data infrastructures into an integrated whole, enable the interoperability needed to eliminate fragmented communications. With converged technologies, a single platform manages both voice and data information and enables responders to communicate with each other from wherever they are, using any method of communication.

There is no need to replace the familiar and effective radios used by first responders. Rather, converged technologies will allow these familiar tools to be part of a broader spectrum of devices that not only talk to each other, but interact with applications as part of a larger, fully interoperable environment. The network itself overcomes any incompatibilities among radio systems or other devices.

Use The Most Familiar Device

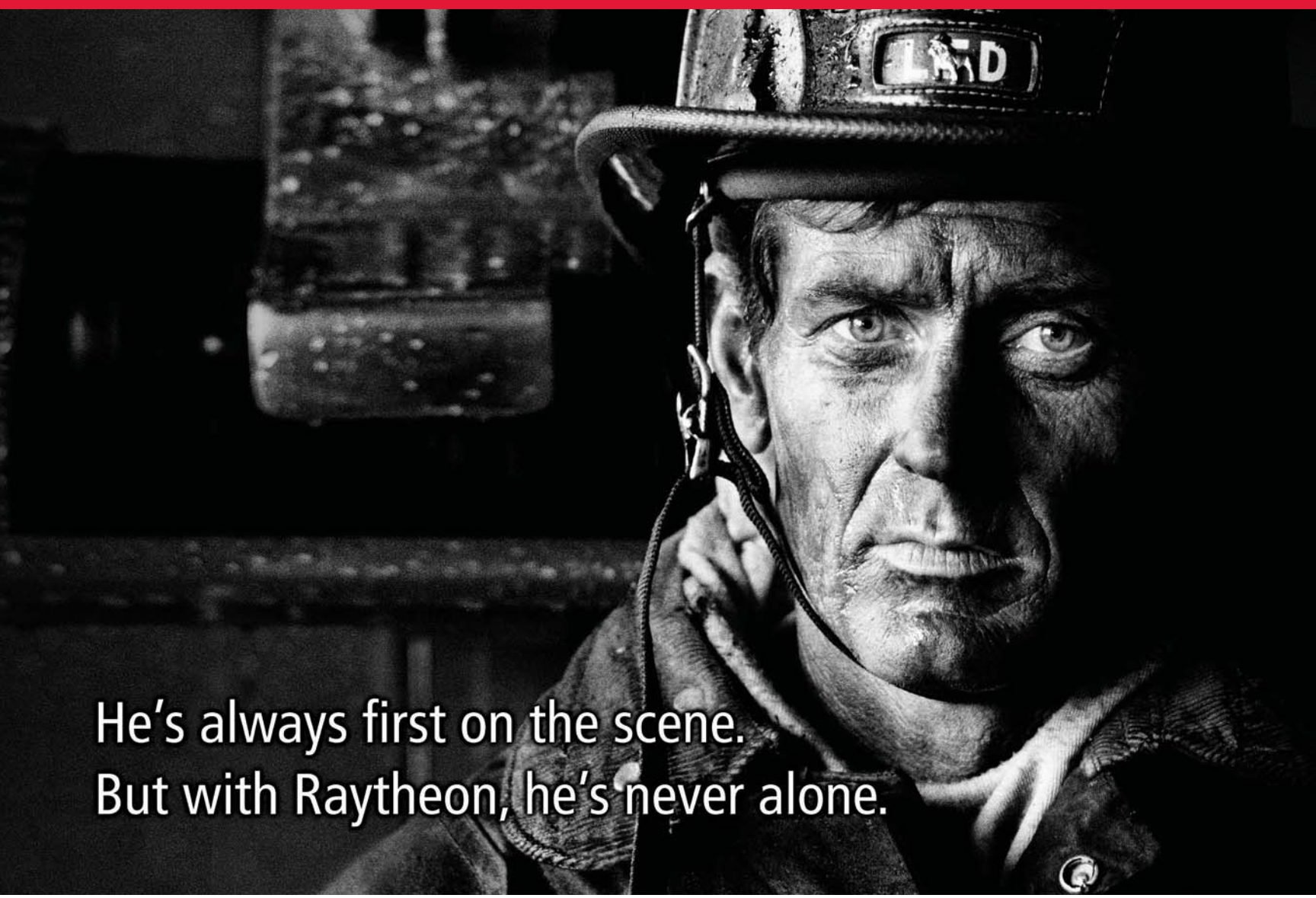
When the land-based mobile radio works, use it. When it is necessary to bring in more diverse assets and organizations, turn them on. Each individual should use the device most familiar to them. The network should enable the devices to talk to one another. Clearly, as we migrate to Internet Protocol Version 6 (IPv6), this interoperability requirement will be addressed.

Moving to a converged network doesn't have to involve an expensive replacement of existing systems. When emergency communications technologies are layered upon an existing, field-proven infrastructure, there is nothing to throw away. That means agencies don't have to choose how to allocate limited funds between emergency or operational imperatives. With converged communications, all needs can be met at the same time, with the same resources, and often without replacing major systems.

Moving forward should entail separating the interoperability discussion from the issue of modernizing land mobile radio and other handheld assets. Law Enforcement and Public Safety Officials need the best radio assets as part of their tactical toolset. The upgrading and modernization of radio assets to digital narrowband should continue as a major priority to get the best technologies into the hands of those that need it. But we should not confuse this issue with achieving interoperability. Let competitive technologies resolve the issue of the devices (radios, PDAs, cell phones, notebook computers, etc.). Focus the discussion of interoperability on the IPv6 converged network infrastructure. •

Jim Flyzik, The Flyzik Group
Mr. Flyzik is former CIO, Treasury and Special Advisor to DHS Secretary Tom Ridge.

Homeland Security



We're proud to support the brave men and women who are America's first responders. Our preparedness and response technology and services are based on decades of experience developing and deploying solutions that perform even under challenging and harsh conditions — the kind that first responders face head-on. We are determined to provide the best support available. So whatever situation you're facing, you'll have Raytheon by your side.

www.raytheon.com

Raytheon

Customer Success Is Our Mission

Serving those who serve.

At Lockheed Martin, we have a long and proud history of working in partnership with those whose sole purpose is the protection of our nation and its people. Lockheed Martin stands ready to support our partners as they move toward a more secure America. With our unique expertise in network-enabled solutions, systems integration, information technology, and many other technologies, Lockheed Martin has the demonstrated capability to provide critical solutions to this most critical of needs.

www.lockheedmartin.com

LOCKHEED MARTIN

We never forget who we're working for®