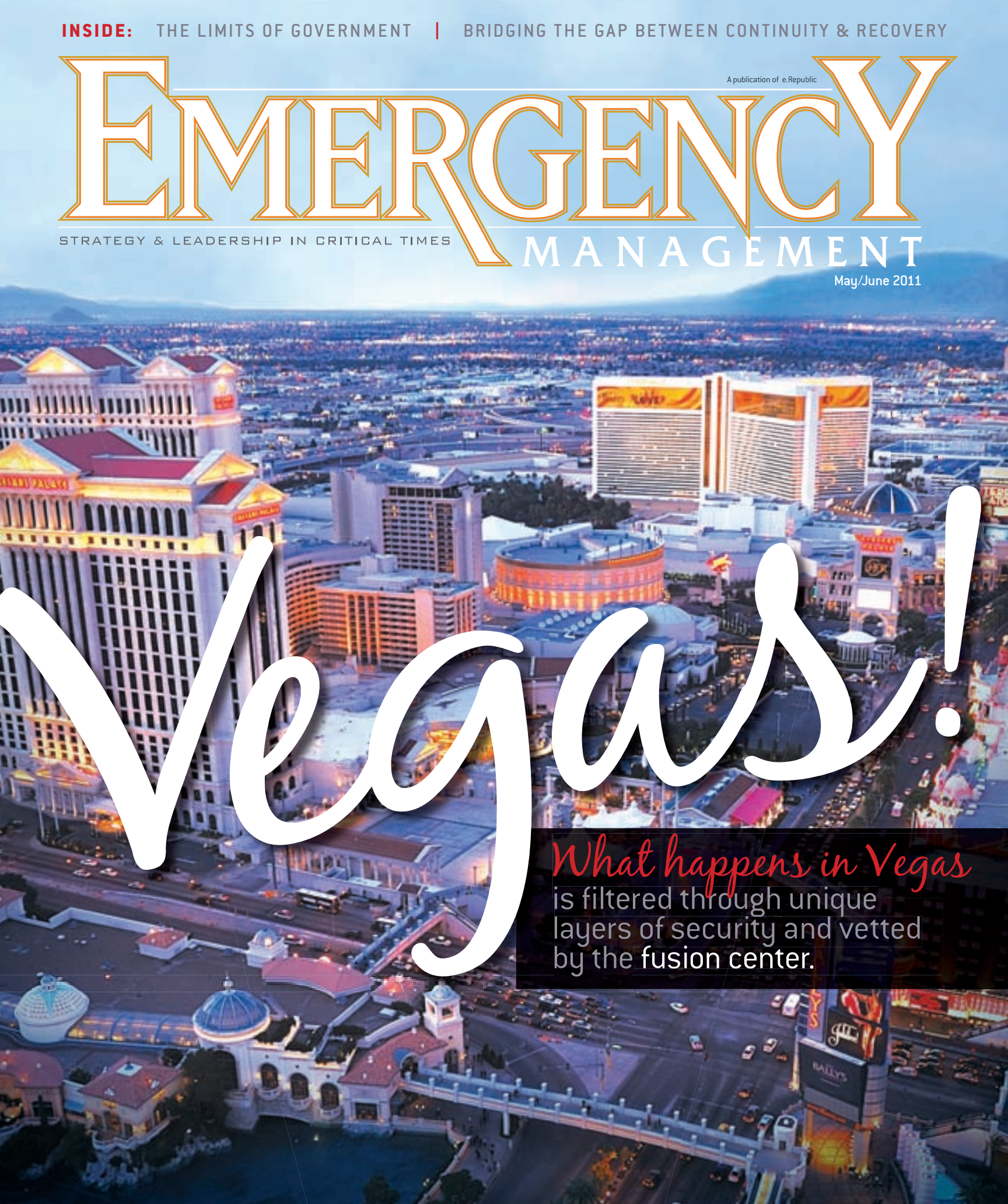
A publication of e.Republic

EMERGENCY MANAGEMENT

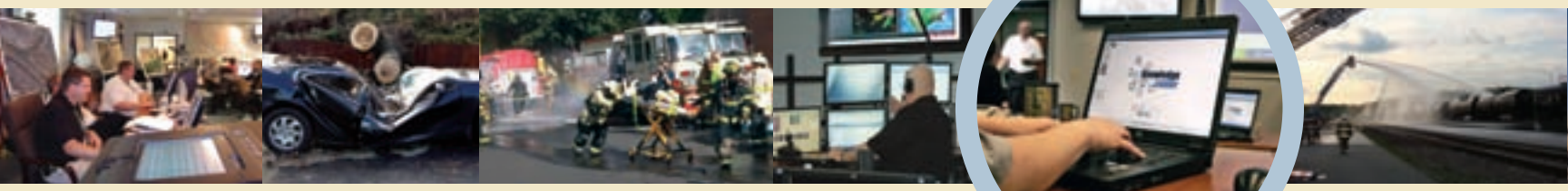
STRATEGY & LEADERSHIP IN CRITICAL TIMES

May/June 2011



Vegas!

What happens in Vegas is filtered through unique layers of security and vetted by the fusion center.



Knowledge is Power.
Knowledge Center™ is Fusion.

Use **Knowledge Center™** to promote a ***virtual collaborative environment*** to facilitate cooperation and provide instant access to information—**anytime, anywhere.**

Common Operating Picture (COP)

Interoperability

Fusion Center

Situational Awareness

Incident Management Software Solutions

Fully-functional, out-of-the-box, no training required.

Incident Management System

Incident Command System (ICS)
Critical Infrastructure/Key Resources (CI/KR)
Situation Reporting (SITREP)
Geographic Information Systems (GIS)

Hospital Incident Management System

Hospital Incident Command System (HICS)
Hazard Vulnerability Assessment (HVA)
Patient/Triage tracking
Hospital Available Beds (HAvBED)

Fusion System

Optimized intelligence sharing
Secure, tiered access control
Dynamic, configurable reporting
Interoperable with CADs

Learn More about Knowledge Center!

Be a part of our virtual EOC at the 2011 UASI Conference!

June 20–23 in San Francisco, CA

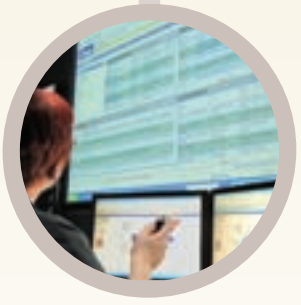
*"The Knowledge Center's '**common operating picture**' is something that every response organization should strive for."*

— Commander Timme, US Coast Guard

Knowledge center™

*"I think this type of information sharing is **an example of how it should be**."*

— Lieutenant Zupanc, Ohio Fusion Center



Don't just report. Communicate.

Call us: **412.635.3322**

www.**knowledge-center**.com

Incident Management Software Solutions

*Contents

SHUTTERSTOCK.COM/MARKO POPLASEN

The budget is tight and the need is critical. Scary. But we've helped public safety organizations large and small make it work, and we can help you from needs assessment to implementation. And by partnering with industry leaders like Panasonic, General Dynamics Itronix and Lenovo, we can help make sure your first responders have the technology they need when they need it.

See how we do it at the21stcenturycommunity.com

Panasonic TOUGHBOOK® GENERAL DYNAMICS Itronix lenovo + CDW·G® PEOPLE WHO GET IT™

*Contents

PHOTO COURTESY OF WWW.ISATSB.COM

DEPARTMENTS CONTINUED

REST OF THE BOOK

Group Publisher:	Don Pearson dpearson@govtech.com
Founding Publisher:	Tim Karney tkarney@govtech.com
VP Emergency Management/ Homeland Security:	Martin Pastula mpastula@govtech.com (916) 932-1497
Publisher:	Scott Fackert sfackert@govtech.com (916) 765-1875
Executive Editor:	Steve Towns stowns@govtech.com

EDITORIAL

Editor:	Jim McKay jmckay@govtech.com
Associate Editor:	Elaine Pittman epittman@govtech.com
Managing Editor:	Karen Stewartson kstewartson@govtech.com
Assistant Editor:	Lauren Katims lkatims@govtech.com
Features Editor:	Andy Opsahl aopsahl@govtech.com
Chief Copy Editor:	Miriam Jones mjones@govtech.com
Staff Writers:	Hilton Collins hcollins@govtech.com
	Corey McKenna cmckenna@govtech.com

DESIGN

Creative Director:	Kelly Martinelli kmartinelli@govtech.com
Art Director:	Michelle Hamm mhamm@govtech.com
Senior Designer:	Crystal Hopson chopson@govtech.com
Illustrator:	Tom McKeith tmckeith@govtech.com
Production Director:	Stephan Widmaier swidm@govtech.com
Production Manager:	Joei Heart jheart@govtech.com

PUBLISHING

VP of Strategic Accounts:	Jon Fyffe jfyffe@govtech.com
VP Bus. Development:	Tim Karney tkarney@govtech.com
East	
Regional Sales Directors:	
East	Leslie Hunter lhunter@govtech.com
West, Central	Shelley Ballard sballard@govtech.com
Account Managers:	
East	Melissa Sellers msellers@govtech.com
West, Central	Erin Gross egross@govtech.com
Business Development Director:	Glenn Swenson gswenson@govtech.com
Bus. Dev. Managers:	Lisa Doughty ldoughty@govtech.com
	John Enright jenright@govtech.com
	Pat Hoertling phoertling@govtech.com
	Kevin May kmay@govtech.com
Regional Sales Administrators:	Sabrina Shewmake sshewmake@govtech.com
	Christine Childs cchilds@govtech.com
National Sales Administrator:	Jennifer Valdez jvaldez@govtech.com
Director of Marketing:	Andrea Kleinbardt akleinbardt@govtech.com
Sr. Dir. of Custom Events:	Whitney Sweet wsweet@govtech.com
Dir. of Custom Events:	Lana Herrera lherrera@govtech.com
Custom Events Managers:	Tanya Noujaim tnoujaim@govtech.com
	Katey Lamke klamke@govtech.com
	Gina Fabrocini gfabrocini@govtech.com
Custom Events Coordinator:	Megan Turco mturco@govtech.com
Custom Events Admin.:	Sharon Remeiro sremeiro@govtech.com
Dir. of Custom Media:	Stacey Toles stoles@govtech.com
Custom Media Editor:	Emily Montandon emontandon@govtech.com
Sr. Custom Media Writer:	Jim Meyers jmeyers@govtech.com
Custom Media Writer:	Noelle Knell nknell@govtech.com
Custom Media Proj. Asst.:	Courtney Hardy chardy@govtech.com
Dir. of Web Products and Svcs.:	Vikki Palazzari vpalazzari@govtech.com
Web Services Manager:	Peter Simek psimek@govtech.com
Custom Web Products Manager:	Michelle Mrotek mmrotek@govtech.com
Web Advertising Manager:	Julie Dedeaux jdedeaux@govtech.com
Web Services/Project Manager:	Adam Fowler afowler@govtech.com
Subscription Coordinator:	Eenie Yang subscriptions@govtech.com

CORPORATE

CEO:	Dennis McKenna dmckenna@govtech.com
Executive VP:	Don Pearson dpearson@govtech.com
Executive VP:	Cathilea Robinett crobinet@centerdigitalgov.com
CAO:	Lisa Bernard lbernard@govtech.com
CFO:	Paul Harney pharney@govtech.com
VP of Events:	Alan Cox acox@govtech.com
Chief Marketing Officer:	Margaret Mohr mmohr@govtech.com
Chief Content Officer:	Paul W. Taylor ptaylor@govtech.com

Government Technology's Emergency Management (ISSN 2156-2490) is published by e.Republic Inc.

Article submissions should be sent to the attention of the Managing Editor. Reprints of all articles in this issue and past issues are available (500 minimum). Please direct inquiries for reprints and licensing to Wright's Media: (877) 652-5295, sales@wrightsmedia.com.

Subscription Information: Requests for subscriptions may be directed to subscription coordinator by phone or fax to the numbers below. You can also subscribe online at www.emergencymgmt.com.

100 Blue Ravine Road, Folsom, CA 95630
Phone: (916)932-1300 Fax: (916)932-1470
www.emergencymgmt.com

A publication of e.Republic Incorporated

The inside pages of this publication are printed on 80 percent de-inked recycled fiber.

Respond to emergencies at the speed of 4G. *Improve response times with a wireless connection that's fast and flexible. The Sprint 3G/4G USB U600 is the perfect tool for public safety. Download map data, access GIS information and monitor surveillance remotely in real time at fast 4G speed with unlimited 4G data. Only on the Now Network.™*

sprint.com/4G 1-800-SPRINT-1 (1-800-777-4681)

Sprint

The Now Network™

Sprint 3G/4G USB U600

"Sprint showed the biggest improvement in customer experience across 14 industries."
–Forrester Research Report: Customer Experience Index 2010

Reader Feedback

Value-Added Education

In the March/April issue, we published reader comments in response to *Degree of Expectation* in the November/December 2010 issue. The topic continues to receive attention from *Emergency Management's* readers.

"I am in complete agreement with the readers' assessments of higher education opportunities in [emergency management]. While I have lower degrees in parallel disciplines, choosing the 'value added' higher education degree is difficult. As these programs cost money, pursuit of these degrees has to be on target so as to obtain a position or further movement within a current position. With that, which ones are considered to be 'premium value?'

Thank you for your time, and [I] look forward to more discussion and solutions in creating a 'score card' for higher educational institutions that offer degrees in emergency management."

Best Regards, Jeff Pollard
Specialist, Incident Coordination and Support
Non-Radiological Emergency Management
Operating Support and Fleet Governance
Tennessee Valley Authority

National EAS Test

Rick Wimberly discussed the first-ever national test of the Emergency Alert System (EAS) in *A National Test* from the March/April issue. Online readers expressed their support for the test, which will take place later this year.

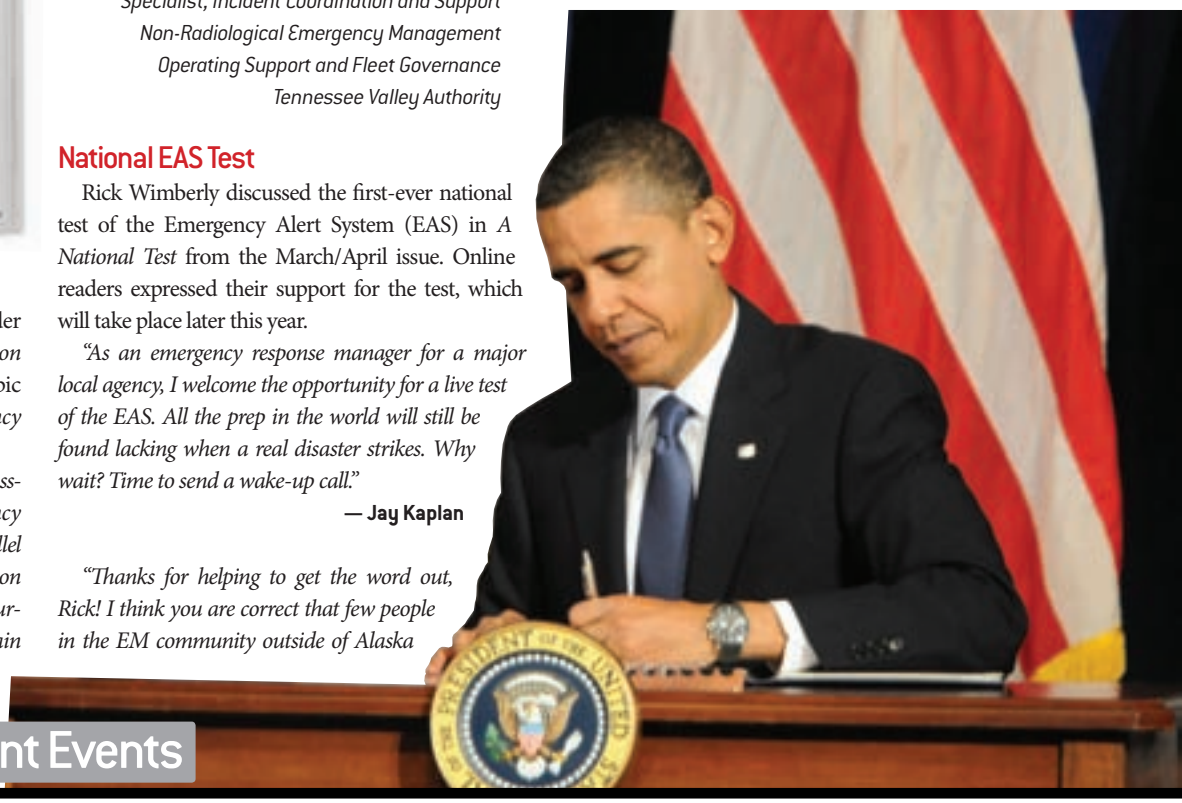
"As an emergency response manager for a major local agency, I welcome the opportunity for a live test of the EAS. All the prep in the world will still be found lacking when a real disaster strikes. Why wait? Time to send a wake-up call."

— Jay Kaplan

"Thanks for helping to get the word out, Rick! I think you are correct that few people in the EM community outside of Alaska are aware of this first-ever live code EAS test for presidential warnings."

— Richard

Your opinions matter to us. Send letters to the editor at **editorial@govtech.com**. Publication is solely at the discretion of the editors. *Emergency Management* reserves the right to edit submissions for length.



Emergency Management Events

9 June

ALL-HAZARDS/ALL-STAKEHOLDERS SUMMIT
Philadelphia

The All-Hazards/All-Stakeholders Summit will address man-made and natural hazards — fires, floods, earthquakes, terror events — facing the Philadelphia area and address best practices in preparing for and mitigating these crises.

Contact: Liese Brunner at 800/940-6039 ext. 1355 for registration information, and Scott Fackert at 916/932-1416 for sponsorship information.

9-11 June

INTERNATIONAL ASSOCIATION OF EMERGENCY MANAGERS MID-YEAR MEETING
Emmitsburg, Md.

The meeting is for IAEM members, emergency management professionals, congressional staffers and federal officials with a role in homeland security and emergency management. Sessions will include briefings from U.S. Department of Homeland Security officials.

www.iaem.com

12 June

NATIONAL FIRE PROTECTION ASSOCIATION CONFERENCE & EXPO
Boston

The conference will feature the latest in fire, security and life-safety products and technologies. There will be more than 130 sessions to attend and an association technical meeting to discuss NFPA codes and standards that need to be considered.

www.nfpa.org/conference

19-22 June

WORLD CONFERENCE ON DISASTER MANAGEMENT
Toronto

The conference gathers Canadian and international speakers, representing all areas of disaster management, to provide solutions on how government, communities and businesses can prepare for emergencies and adapt to global and local threats and catastrophic events.

www.wcdm.org

20-22 June

NATIONAL URBAN AREA SECURITY INITIATIVE CONFERENCE
San Francisco

The conference's theme is creating capabilities through regional collaboration. The conference will provide an opportunity for stakeholders from all areas of homeland security and emergency preparedness to exchange information to make the U.S. safer.

www.urbanareas.org

7 July

ALL-HAZARDS/ALL-STAKEHOLDERS SUMMIT
San Diego

The All-Hazards/All-Stakeholders Summit will address man-made and natural hazards — fires, floods, earthquakes, terror events — facing the San Diego area and address best practices in preparing for and mitigating these crises.

www.emergencymgmt.com/events

Who can handle a security challenge this complex?

With leading-edge technology, Siemens combines knowledge and experience to deliver tailored security solutions.

To be your long-term partner, today's integrator has to provide more than technology; they have to know your business and risk profile, understand the regulatory environment, compliance issues and how to customize an intelligent, layered security solution. The Integrated Security Solutions (ISS) team at Siemens Security boasts a combined average of 27 years in the security industry. Siemens has the highest level of expertise, access to leading-edge products and the talented resources to execute complex solutions. Our team has all of these in-house and ready to deploy. We have the answers to your toughest questions. **usa.siemens.com/integratedsecuritysolutions**

Answers for infrastructure.

SIEMENS

Black Swan Events

By Eric Holdeman

The world has been experiencing a series of extreme events — political, technological and natural. In the realm of disasters, in a little more than a year, we have experienced significant earthquakes in Haiti, Chile, New Zealand and Japan. The Gulf of Mexico oil spill is yet another reminder of how devastating and widespread a technological disaster can become.

Japan was hit by a triple whammy: an earthquake, followed by a tsunami and then a partial meltdown of nuclear reactors. This natural disaster led to cascading events, including the deaths of tens of thousands, the evacuation of hundreds of thousands and electrical power shortages that will continue for months. While Haiti's damages were difficult to watch, they were expected given its status as a poor country with few resources. Because of Japan's history of disaster preparedness, however, the images that filled our TV screens seemed improbable for an industrialized, modern country.

"Black swan events" are those that are possible, but are totally unexpected. The definition by author Nassim Nicholas Taleb includes: "First, it is an outlier, as it lies outside the realm of regular expectations, because nothing in the past can convincingly point to its possibility. Second, it carries an extreme impact. Third, in spite of its outlier status, human nature makes us concoct explanations for its occurrence after the fact, making it explainable and predictable."

While science may point to the potential for future cataclysmic events, human nature is to discount those as not occurring in our lifetimes. Given recent events, however, it's easy to predict more black swan events that will range from natural to technological disasters and terrorist events.

Emergency managers and their partner organizations must expand their thinking, planning and response capabilities to encompass the "maximum of maximums." As we plan for the future, we need to envision catastrophes so large that the response and recovery will go far beyond what we have experienced.

In May, FEMA conducted such an event. The National Level Exercise commemorated the 200th anniversary of a New Madrid fault zone earthquake that impacted a multistate region. Superimpose the existing population and the "as built" infrastructure of today over this geographic area and you can imagine how such an earthquake could change the course of rivers and conceivably the history of the impacted region.

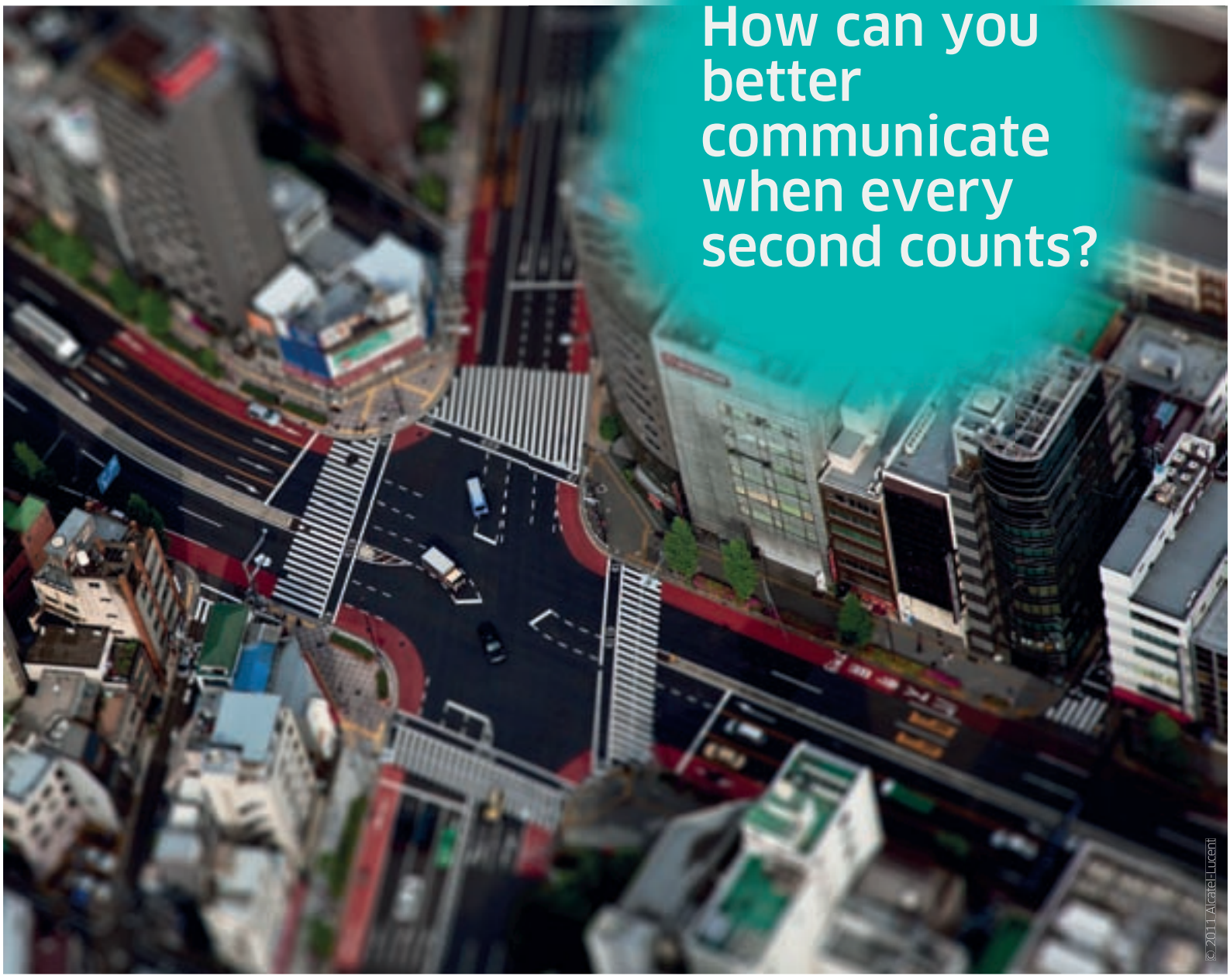
As we look for lessons learned from recent disasters, it is critical that we communicate the risks as forcefully as possible to the people who are in positions to make wise decisions on the allocation of resources toward building resiliency in communities. If there's one thing that we should learn from black swan events, it's that they are hard to prevent. Their size and scope may overwhelm our feeble attempts to respond. In the long term, it will only be the resiliency of the people, organizations and systems that will change the course of history and the disaster's impact. Most of the time we can't change what happens to us, but we do control how we respond and recover.

The editors and staff at *Emergency Management* magazine pledge our best effort at bringing information to you that can help make a difference when disaster strikes. Visit us online and at our new Facebook page, www.facebook.com/emergencymgmt, and tell us what you are doing. Help us help you by sharing your best practices and lessons learned. We'll do the rest.

Eric Holdeman is the former director of the King County, Wash., Office of Emergency Management.

Questions or comments? Please give us your input by contacting our editorial department at editorial@govtech.com, or visit our website at **www.emergencymgmt.com**.

BY EQUIPPING PUBLIC SAFETY AGENCIES WITH BETTER COMMUNICATIONS AND RICHER INFORMATION EVERYWHERE, WE CAN IMPROVE EFFICIENCY AND SAFETY FOR EVERYONE.



alcatel-lucent.com

AT THE SPEED OF IDEAS™

Alcatel·Lucent

* IN THE NEWS

The tsunami and magnitude 9.0 earthquake that struck Japan in March, causing a nuclear crisis as radiation leaked from the damaged Fukushima nuclear plant, triggered the U.S. to take note of its nuclear preparedness. Nuclear power provided 14 percent of the world's electricity in 2009, and that number is expected to grow as nations continue building nuclear power plants — 62 were under construction as of March, according to the World Nuclear Association. Here's a look at some of the countries that utilize nuclear power, as well as at-risk nuclear power sites in the United States.

WORLD

Billion kilowatt hours in 2009: **2,560**

Percentage of total electricity in 2009: **14%**

Nuclear power reactors in operation: **443**

Nuclear power reactors under construction: **62**

CANADA

Billion kilowatt hours in 2009: **85.3**

Percentage of total electricity in 2009: **14.8%**

Nuclear power reactors in operation: **18**

Nuclear power reactors under construction: **2**

UNITED STATES

Billion kilowatt hours in 2009: **798.7**

Percentage of total electricity in 2009: **20.2%**

Nuclear power reactors in operation: **104**

Nuclear power reactors under construction: **1**

MEXICO

Billion kilowatt hours in 2009: **10.1**

Percentage of total electricity in 2009: **4.8%**

Nuclear power reactors in operation: **2**

Nuclear power reactors under construction: **0**

The top 10 nuclear power sites in the United States with the highest risk of suffering core damage from an earthquake (based on 2008 geological data).

U.S. MAP SOURCE: U.S. NUCLEAR REGULATORY COMMISSION, WORLD MAP SOURCE: WORLD NUCLEAR ASSOCIATION

BY THE NUMBERS

31 states have nuclear power plants

3 states reported adequate resources to conduct population-based exposure monitoring

42% of the state health departments reported minimal or no planning to detect radiation contamination in first responders

20 states reported having a finalized radiation-specific written response plan

16 of the 20 states with a written plan reported having conducted a drill or an exercise of the radiation plan

28 states reported providing training to local jurisdictions on any aspect of radiation emergency preparedness and response

SOURCE: DISASTER MEDICINE AND PUBLIC HEALTH PREPAREDNESS JOURNAL'S SURVEY OF 38 STATE HEALTH DEPARTMENTS

PHOTO COURTESY OF AARON SKOLNIK/FEMA

Employee Locator System

A NEW EMPLOYEE LOCATOR could aid Miami-Dade County, Fla., officials in coordinating responses to future disasters. The application plots where county employees live and work on a map that's searchable by an employee's identification number, name, address or ZIP code. In addition to plotting locations on a map, the application provides information on employees' job titles, what languages they speak and any special skills they may have.

Employees update this information through the county's BlueBook system, which houses employees' profiles and contact information. The BlueBook information can be used by the Department of Emergency Management to assign roles for disaster response. All employees who are not designated as essential to department operations or the Emergency Operations Center are required to assist in the county's disaster response.

High-Tech Warning System Aided Tsunami Response

THE 20-FOOT-HIGH TSUNAMI that slammed ashore in northern Japan on March 11 has taken an untold number of lives and caused incalculable damage.

The water displaced by the magnitude 9.0 temblor, the fifth-most powerful earthquake in the world since 1900, propagated outward across the Pacific. The surge arrived hours later and caused localized damage on the shorelines of Hawaii, Washington, Oregon and California.

The worldwide event evoked memories of the 2004 Indian Ocean tsunami, which killed 250,000 near the coastline as the monstrous waves hit. The disaster highlighted the need for better tsunami data and an early warning system for coastal areas. The U.S. National Oceanic and Atmospheric Administration took the lead and by 2008 had placed 32 sensor buoys in the Pacific.

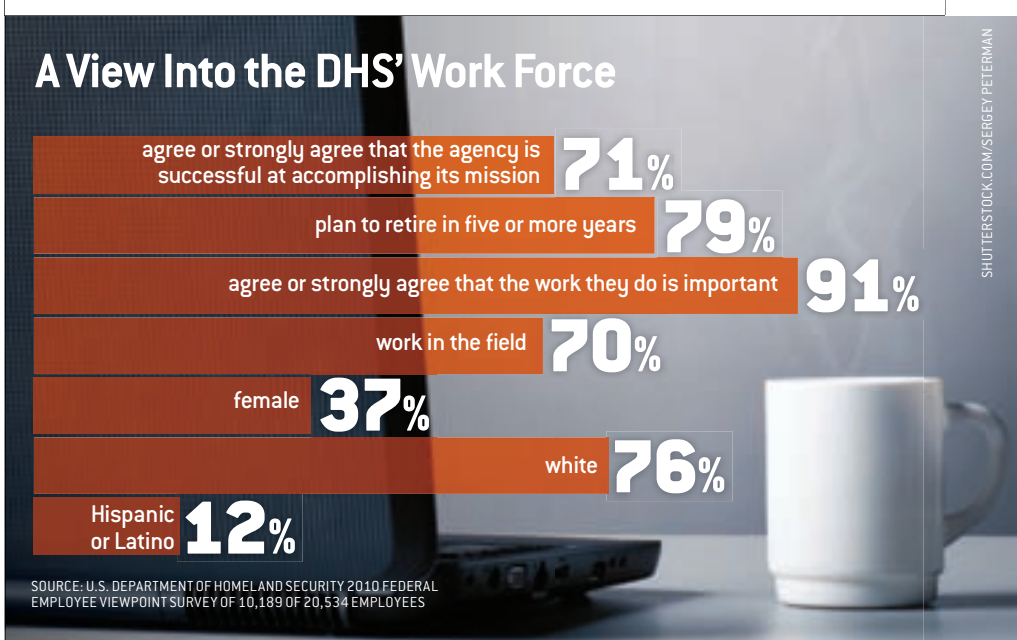
The so-called "DART" buoys include a tsunometer on the ocean floor that measures wave height and water pressure at 15-second intervals and then predicts what the wave height will be in the next interval. The wealth of data allowed scientists to estimate the intensity, wave height and projected time of landfall for the tsunami that struck Japan. This lead time gave local authorities around the world the ability to close beaches along the Pacific Rim and evacuate low-lying areas in advance.

IPhone App Engages Citizens in CPR Emergencies

WHEN SOMEONE SUFFERS A HEART ATTACK, little time is available to save the person's life. To increase the chances of saving victims of cardiac arrest, the San Ramon Valley, Calif., Fire Protection District launched a feature on its free iPhone app, called Fire Department, [http://firedepartment.mobi] that notifies citizens in the area when someone requires CPR.

Citizens who opt in to the CPR feature indicate that they are trained in the life-saving method. If an emergency is called in to 911 that requires CPR, citizens can start the procedure if they arrive at the scene first. The app also notifies citizen rescuers where to find the closest publicly accessible defibrillator.

A View Into the DHS' Work Force



SOURCE: U.S. DEPARTMENT OF HOMELAND SECURITY 2010 FEDERAL EMPLOYEE VIEWPOINT SURVEY OF 10,189 OF 20,534 EMPLOYEES

SHUTTERSTOCK.COM/SERGEY PETERMAN

SHUTTERSTOCK.COM/ANDYZ.

IT'S Vegas Baby!

And what happens in Vegas is filtered through unique layers of security that revolve around the fusion center.

JIM McKAY, EDITOR, AND
ELAINE PITTMAN, ASSOCIATE EDITOR

Each year more than 30 million people are drawn to Nevada by Las Vegas' luster. The self-proclaimed "Entertainment Capital of the World" is home to 18 of the world's 25 largest hotels, and more than 19,000 conventions were held in the city in 2009. Las Vegas is without question a terrorist target. Beyond the cop on the street, there's an effective, underlying layer of security that may be unprecedented, and it starts with the fusion center, the Southern Nevada Counter-Terrorism Center (SNCTC), an all-hazards, 24/7 model for public-private collaboration.

PHOTO BY ELAINE PITTMAN

In an unassuming building near McCarran International Airport in Las Vegas, 14 different agencies from federal, state and local government work together toward one goal: to keep residents and tourists safe. One of three fusion centers in the state, the SNCTC stands out because it's an all-hours operation that focuses not only on terrorism, but also on all crimes and hazards.

Conceived after the 9/11 attacks, the U.S. Department of Homeland Security (DHS) recognizes 72 fusion centers across the nation that analyze and gather threat-related information from all levels of government. "It's a multiagency group of folks who are sending information to their agencies and gathering it from their agencies," said Lt. Dennis Domansky of the Las Vegas Metropolitan Police Department. "It's information sharing and looking to identify trends."

The SNCTC opened in July 2007 and seeks to connect the dots between crimes that may look unrelated but could be precursors to a bigger event, while working with the community and tourism industry to collect information about suspicious activities. "It's recognizing the type of trend that you might not recognize if everybody is working independently," Domansky said.

No two fusion centers are identical — and there's good reason to avoid a cookie-cutter approach. Although there is a baseline of what every fusion center should be able to do (e.g., receive, analyze and disseminate information while collaborating with other agencies), they can differ greatly. "Since every area is different, you have to be able to move things around and do different things," said Sgt. Brian Hibbetts. "Our process wouldn't work in Boise, Idaho."

Because Sin City and its famous Strip attract more than 36 million visitors per year, a terrorist attack or large-scale disaster could cripple its tourism industry. The SNCTC works closely with the private sector, including hotels and casinos, to share information and collect reports about suspicious activity. Security and preparedness falls onto every organization in the Las Vegas Valley to ensure that people and critical infrastructure are kept safe.

MINING INFORMATION

The SNCTC is divided into two sections — intelligence collections and crime analysis — that together try to determine if suspicious reports or criminal activity are linked to something larger like preparation for a terrorist attack.

The intelligence collections section has overt and covert squads, according to Hibbetts, who leads the section. Officers are charged with following up on suspicious activity reports, collecting information in the field, conducting surveillance and source development.

SHUTTERSTOCK.COM/MARKO POPLASEN

Progressive Posture

A Florida county thinks ahead as it rolls out a next-generation 911 network.

BREVARD COUNTY, FLA., is taking a leading position in the move to next-generation (NG) 911 services, which will allow citizens to send text messages, images and videos to emergency call takers when industry standards are in place. The county is replacing its aging 911 public safety communications network with an Emergency Services IP network (ESInet) from AT&T, an Internet protocol (IP)-based network for routing and delivery of 911 calls. It will be more reliable and redundant than the existing network, with no single point of failure. And because it's IP-based, the system will be able to handle data files, such as text and images, as well as traditional voice communications — capabilities that don't exist today for 911 services.

To ensure that the system is ready for the future, the county chose to make the network compatible with i3 standards, even before those standards are finalized. The i3 standards, defined by the National Emergency Number Association, dictate the basis for NG 911 and will ensure that 911 systems across the country will be able to accept text messages, photos, video and more. Incorporating i3 standards now will allow the network to evolve faster as standards are ratified.

"The technology is growing and changing so quickly," said Deborah Sands, 911 Coordinator for Brevard County. "As the technology develops and the ability to do things like texting 911 occurs, we will be ready to accept it and handle it properly."

The new network will support the county's eleven 911 call centers, also known as public safety answering points (PSAPs), which serve about 540,000 residents on the eastern coast of Florida. The system will be hosted across three sites, managed by AT&T and the county's emergency operations center, to ensure both geographic redundancy and operational security. If one host goes down, all 11 PSAPs can be supported on the other two sites. This cloud approach keeps the system ready for any disaster, in terms of continuity of operations.

"We have a lot of water," Sands said. "We have four PSAPs on the beach. If they get wiped out, we have to be able to move our equipment somewhere else, be it another 911 cen-

"As the technology develops and the ability to do things like texting 911 occurs, we will be ready to accept it and handle it properly."

— **Deborah Sands, 911 Coordinator, Brevard County, Fla.**

ter, or out of the county if we have to. We had to prepare for the worst-case scenario."

Sitting on the edge of the Atlantic Ocean, the county has to be prepared for hurricanes, other severe weather and water-related incidents. It also must contend with wildfires that consume a lot of acreage each year. And the county is home to the Kennedy Space Center, where there is potential for a release of toxic chemicals if a launch goes awry.

Flexible Solution

The new system will go online in stages — one PSAP at a time — with the entire system scheduled to be up and running before the end of 2011. The county decided to replace the entire network due to its age, rather than just upgrading components, Sands said. "It's overdue for an overhaul. And we don't want to piecemeal it," she said. "We want to do it right."

The state-of-the-art network has the ability to expand or contract due to either a rise in the county's population or decreased need based on potential PSAP consolidation. With all these variables, network flexibility is very important.

"It was a must," said Sands. "Because of the Space Center shuttle program and how things are going out there. And the unknowns with budget cuts. We had to know that if we were going to be consolidating, that we would not have to continue to pay the price. That was a very big thing that we looked into."

AT&T was able to supply the flexibility the county needed. There are other advantages too. "It allowed us to look at all our linkages between our PSAPs," said Bob Lay, Director of the county's Office of Emergency Management. "And all PSAPs are not equal, because they all work for different people. But we had them all brought up to a certain standard. So with this new system, all of our 11 PSAPs will be operating from the same standard space in terms of electronics and connectivity."

Better Service

Citizens and visitors alike will one day be able to send text messages, photos or video to 911 centers. "Big benefits for the citizens will be the new network's redundancy and reliability,"

Lay said. "But the most important part is that it will bring in other operational uses, other ways of communicating to 911 centers."

Because the new network is based on IP technology, the county gets a system that's simpler and will require less maintenance than the previous one. And with the built-in redundancy, if there's an interruption in service, it can often be fixed without citizens even knowing there was a problem.

With AT&T as the single vendor for the new network, the county is receiving assistance on installation, project management and training from one company. AT&T will also monitor the system 24 hours a day. "We've had a really good relationship with AT&T," Sands said. "They've been working very hard with us to make sure everything is in place before we go live."

Lay said the new network creates opportunities for the future. "Somewhere down the road of next-generation 911, I think there will be a lot of bridges built that will allow information sharing in terms of 911 systems that we haven't even thought of today," he said. "I think this is a very exciting time for everybody — both government and our residents."

For Brevard County 911, it always comes back to the public's safety. "I think it's important that the citizens of Brevard County know that this won't change the way 911 is currently operating," said Sands. "It's only going to make it better."

The Southern Nevada Counter-Terrorism Center's watch desk is staffed 24/7 and tracks the area's law enforcement information.

Staying in Touch on New Year's Eve

When Tom Lozich patrolled the Las Vegas streets on New Year's Eve as a uniformed officer, he felt there was a discrepancy between what happened on the streets and what happened in the resort hotels. And he thought that disconnect was dangerous.

Now as executive director of corporate security for MGM Resorts International, he and his resort hotel industry partners have averted potential disaster by developing the Unified Intelligence Operation Center, an assemblage of personnel from the various resorts who gather and monitor goings-on inside and outside the resorts.

"When I was on the street with [the Las Vegas Metropolitan Police Department] it was almost as if there was a barrier put up, and what was going on in the hotels wasn't being relayed or communicated back to the street and vice versa," Lozich said. "How could an incident at a resort affect the revelers on the street? It could be catastrophic."

This past New Year's Eve, the group assembled at the Bellagio casino, each representative armed with a radio and e-mail access to and from the Southern Nevada Counter-Terrorism Center, command centers throughout the city and between resorts.

That communication keeps everyone abreast of where the resources are needed, keeping the public at the various resources safer. The information is analyzed and shared where appropriate. For example, this year a ticket scalper oversold a nightclub venue, causing a near riot. But law enforcement was quickly brought in to quell the situation before it got out of hand.

"It's based on the Incident Command System model, which is underutilized by the private sector," Lozich said. "Again, it illustrates the partnership that we have and how we work very closely with the fusion center."

The crime analysis group looks at all types of crime occurring in the valley, from robberies to rapes and murders, to analyze trends. The valley is home to about 2 million people and includes the Henderson Police Department, North Las Vegas Police Department, Boulder City Police Department and the Las Vegas Metropolitan Police Department, as well as the state police and federal agencies. A police officer who handles a robbery in one jurisdiction may be unaware that a similar type of robbery is happening in another area. This is where the crime analysis group steps in to fill the information gap.

"We do a lot of data mining for the criminal precursors to terrorism," said Patrick Baldwin, manager of the crime analysis group. "Most terrorist acts have some type of crime component, either pre-observational surveillance, which could be trespassing or stealing certain chemicals."

A recent example of the partnership between the two sections highlights how they work together. The crime analysis group saw a 700 percent increase in thefts of 20-pound propane tanks from 2007 to 2009, but wasn't sure if the thefts were crime or terrorism related (the tanks could be used to make bombs). While the crime analysis group worked with terrorism analysts, the collections intelligence section interviewed people who were caught stealing propane tanks. "We were able to determine that it wasn't terrorism related," Hibbetts said. The thefts were attributed to the recession — people were selling them to recycling yards and using them to heat homes. However, without fusion center staff looking at police reports to identify trends or activities that could be related, the thefts could have not been connected — and officials wouldn't learn until afterward that it was the precursor to a devastating event like a terrorist attack.

"That incident made me realize that we need to do a better job at mining our own data to find these things as they're occurring and determining the relationships as we go along," Baldwin said.

The SNCTC's personnel are tasked with looking into and tracking everything that happens in the valley. Something that sounds like a standard occurrence to the average person, like a natural gas leak, can cause analysts' internal alarms to sound. "Maybe a natural gas leak isn't just a faulty pipe, or it's someone planning something," Domansky said. "It is looking at all those things and doing that analytical work trying to identify the worst-case scenario."

ENLISTING THE PUBLIC

Collecting and following up on suspicious activity reports are another way the SNCTC seeks to prevent crimes and terrorism. The fusion center is one of 15 sites that have implemented the Nationwide Suspicious Activity Reporting Initiative, which seeks to "implement common processes and policies for gathering, documenting, processing, analyzing and sharing information about terrorism-related suspicious activities," according to the federal government. Signs and billboards around Las Vegas encourage tourists and residents to "see something, say something," and report suspicious activity at the Southern Nevada County Terrorism Trusted Information Exchange website, www.snctc.org, or through a homeland security hotline.

The SNCTC receives at least one suspicious activity report every day, and multiple reports during big events. Hibbetts said it's difficult to distinguish between suspicious and regular activity. "We will get reports that this guy was taking pictures and he was facing a completely different direction than every other tourist," he said. "They will say, 'It looks like he was taking a picture of where the ceiling and the wall come together.'"

Officers will go to the location to follow up. "Ninety-nine percent of the time, we are able to contact the person and they weren't taking a picture of what we thought they were — or there was actually a legitimate reason for it," Hibbetts said. "It's that 1 percent of the time that makes us nervous."

And since it's such a small number of reports that aren't linked back to legitimate activity, it's tempting for officers to become complacent.

SHUTTERSTOCK.COM/SONGQUAN DENG

Domansky said regular updates keep officers on their toes. During an average day he receives two to three updates about situations that are being responded to or suspicious activity that has been reported. And a weekly update summarizes local, regional, national and worldwide terrorist events or suspicious activities.

Another way officers stay engaged is by having detectives go through rotations at the DHS National Operations Center in Washington, D.C. The SNCTC representative spends one to six months working with the federal department and learning about national and international events. "Then we can bring that back to our bosses and show them what is happening overseas and what we need to be looking for," Hibbetts said.

The rotations not only benefit fusion center staff, they also help build relationships with DHS officials in the nation's capital. When Hibbetts was working in Washington, D.C., in 2010, there was a school bus crash in Las Vegas, and DHS officials wanted to brief Secretary Janet Napolitano on the accident. Hibbetts learned from the SNCTC that it was a minor fender bender and no students were on board, so DHS representatives were able to tell Napolitano not to worry.

A TRUE 24/7 OPERATION

When six people were killed and Rep. Gabrielle Giffords, D-Ariz, was shot during a Congress on Your Corner meeting in January in Tuscson, Ariz., phone calls to the area's fusion center were forwarded to a 911 call center, said Baldwin. "A lot of [fusion centers] say that they are 24/7, but for a lot of them, their phone rings and it goes to a dispatching center," he said. "But here you have a fusion center employee answering the phone all the time."

The SNCTC's watch desk is staffed around the clock and is located in the same area as the crime analysts, a large room filled with TV screens that show dispatch information, active law enforcement calls by area and national and local news. The watch desk representative also monitors patrol radio traffic and answers the counterterrorism hotline.

According to the DHS, most fusion centers have expanded beyond terrorism to focus on all crimes, while some, like the SNCTC, have taken their operations a step further with the all-hazards approach, including a built-in approach to monitoring natural disasters. While the center's representatives track what's happening in the Las Vegas area, they also follow weather updates and information about natural disasters through local and national news, as well as the National Weather Service. During severe weather, the center's staff supplies emergency management officials and incident commanders with up-to-date information to help monitor the situation.

PHOTO BY ELAINE PITTMAN

"Say there is a big storm coming and there is potential flooding in the Moapa Valley, which is 60 miles north," Domansky said. "The police department, Clark County and the city will put together their incident management team to start developing a plan or even activate the [Emergency Operations Center] locally to monitor it, and that's when the fusion center will start feeding information that way."

The SNCTC also takes the all-crimes/all-hazards stance when it comes to protecting students and faculty in the Clark County School District, which is the fifth largest in the country. Hibbetts said that in 2008 there was a rash of violence in the valley and a high school student was shot and killed two blocks from his school. "We as an agency and as a fusion center said this has to stop and we have to come up with a better way to handle this," he said.

A school district dispatcher was embedded in the fusion center to provide a link between the schools and police. "You put a dispatcher in front of the computer and he or she will be able to look at it and know everything that's going on," Hibbetts said. "They know the people they need to call and the buttons to push to make it happen."

Now when a school official hears a rumor about an upcoming fight, the information is reported to the school district police and the SNCTC's watch desk. It's then pushed out to the local police departments. Hibbetts said since this process has been in place, there hasn't been a major incident at or near any of the schools.

The SNCTC also seeks to educate police officers to be force multipliers in the mission to mitigate and prevent terrorist activities through the terrorism liaison officers program. About 2,200 officers have completed the Web-based training that informs them what to look for and how to report the data. The fusion center doesn't turn only to law enforcement officers as force multipliers — the casino and hotel industry plays a large part in keeping the Las Vegas area safe.

Next-Generation Emergency Notifications

Safe Towns

Keep your community safe and connected

800-600-3911

INFO@AMERILERT.COM
WWW.AMERILERT.COM/SAFETOWNS

AMERILERT®

Amerilert Safe Towns™ is the most comprehensive suite of municipal safety communication services available. From one intuitive interface, it unites an award-winning emergency notification system, text-a-tip service, info hotline, crisis collaboration tool, and more. Get your free demo of this cloud-based, GIS-interfaced, CAP Compliant system today.

EMERGENCY MANAGEMENT - DISASTER RECOVERY - CONTINUITY OF OPERATIONS
CRIME PREVENTION - MASS NOTIFICATION - COMMUNITY RESPONSE

"We tried to look at the hundreds of positions we have in our company — which ones have the greatest opportunity to see as much as a security officer or a person in a surveillance room?"

Tom Lozich, executive director of corporate security, MGM Resorts International

A UNIQUE KINSHIP

Beyond the hired security personnel, there's a layer of security within the hospitality industry that's rather inconspicuous — and that's by design. Las Vegas is a party town and while the goal is to protect its main asset — people —from harm, it has to do so without alarming visitors. There can't be a uniformed cop on every street corner.

The layered security system is getting more and more elaborate, and there's a set of strong relationships comprising SNCTC staff, the hospitality industry and others, including the University of Nevada, Las Vegas (UNLV). The collaboration is unique partly because of the inherent need of the hospitality business to protect its assets, and because the industry understands that operating within a silo would limit the industry's ability to protect its critical assets.

The importance of this mission is evidenced by the Las Vegas Convention and Visitors Authority funding a full-time analyst at the fusion center. The analyst analyzes suspicious activity information that comes in from the federal and state levels as well as from the resorts, and maintains direct contact with personnel at the resorts.

"Having someone from the private sector funded by the private sector sitting at the fusion center having access to a great deal of information, then messaging back and making sure there's two-way flow of information — that has worked quite well," said Dawn Scalici, deputy undersecretary for analysis at the DHS. "I won't say it's totally unique, but it really does stand out quite a bit in terms of the kind of private-sector interaction they have."

The fusion center staff includes overt and covert personnel always on the lookout for something unusual. Add that to security personnel hired by individual hotels, along with the Las Vegas Metro Police, and you have several layers of security. But that's not enough.

"We know we can't do it alone," Hibbetts said. "It can't just be police."

It must be everyone, including maids, front desk clerks, valets, and recently, taxi cab drivers. They all receive training on what to look for and what to do with the information. It's a network of eyes and ears not limited to security personnel.

More than 36 million tourists visit Las Vegas each year and a terrorism event could cripple the tourism industry.

"We've created this platform of sharing information not only among ourselves, but also with the industry and the fusion center," said Tom Lozich, executive director of corporate security for MGM Resorts International. "When you look at this, security [personnel] is not the main component, nor should it be. Everybody has a role to play, and we've adapted a collaborative effort."

SEE SOMETHING, ACT

Whether it's inherent in the nature of the Las Vegas community or whether it was forged through hard work, this network of collaboration thrives. One reason is the outreach done by the fusion center staff, Hibbetts said. "You get a whole lot more mileage out of walking into somebody's office than you do picking up the phone."

And having the card or phone number of someone to call when something doesn't look right is crucial. "If we're not out there making contacts with people, then the people don't know who to call," Domansky said. "They have information that is useful, but they often don't know what to do with it."

The outreach and training of private-sector personnel is a requirement that's taken on a new dimension recently. The city has taken the See Something, Say Something campaign to heart, using a logo, created by a graphic designer at the MGM Grand, that has been adopted by the city.

And it goes beyond billboards. There's a real effort to get nearly everyone in the hospitality industry involved, and to give them the impetus to keep their eyes and ears open and the confidence to report something unusual.

Fusion center staff used to conduct instructor-led training of private-sector personnel, but the training has gone online with DVDs and Web pages. All employees at the MGM Grand go through Web-led training, including watching Nevada's Seven

EMERGENCY MANAGEMENT

AN URGENT NEED.
IMMEDIATE OPPORTUNITIES.

Government and private employers need thousands of managers who can prevent and respond to disasters, or prepare for acts of terrorism. Be ready with a degree from University of Maryland University College (UMUC). You can earn your BS in emergency management. Or choose from an MS in technology management or an MS in management—each with a specialization in emergency management.

- Learn to prepare and implement disaster preparedness and response plans
- Acquire the leadership skills you need for crisis management and disaster response
- Financial aid and an interest-free monthly payment plan available

UMUC
University of Maryland University College

Enroll now.

800-888-UMUC • umuc.edu/standup

Signs of Terrorism, which explains what behavior might be out of the norm and could be preparation for a terrorist act.

The training gets more specific and drills down into what various staff members might look for depending on their jobs. There are videos for parking valets, guest room attendants, porters, technicians, guest services representatives and most recently cab drivers.

Each video is tailored to the position held at the hotel. For instance, the bellhop might see something different than a maid would. "We tried to look at the hundreds of positions we have in our company," Lozich said. "Which ones have the greatest opportunity to see as much as a security officer or a person in a surveillance room?"

Lozich called it a focused approach in that the valet outside parking cars will see something different than the guestroom attendant on the 33rd floor and should be trained as such. The DVDs underscore what might be suspicious activity that warrants reporting and how to report it. The DVDs avoid profiling individuals, and SNCTC personnel stress watching for suspicious activities rather than suspicious people.

The videos were developed in a collaborative effort with the industry, the fusion center and the Institute for Security Studies at UNLV. During development, business practices and the constraints of the hotel industry were taken into consideration. The industry can't afford to put staff in a training room for hours at a time and provide a PowerPoint presentation. It can, however, provide looping video in a lunchroom or break room and train employees at opportune times.

Employees view the DVDs on preshifts, when one shift starts and another ends. And the point is driven home daily, from the billboards employees see as they drive to work to the looped "MeTV" on the video screens in the lunchrooms and elsewhere. "I call it media touch points," Lozich said. "We understand posters aren't the answer; it has to be a layered approach between our MeTV to the cards that we hand out to promote discussion between security and employees."

NEVER BITE THE HAND THAT FEEDS

Anyone can view the video, Nevada's Seven Signs of Terrorism, or fill out a Suspicious Activity Report at www.snctc.org. But employees of the MGM are coached to report any suspicious activity — an item out of place, a person acting strangely — to their supervisor or security personnel. If the supervisor or security officer believes it to be an urgent threat, he'll place a call directly to the fusion center. Or the information is entered into Trapwire, a citywide database linking surveillance systems of most resorts and the fusion center.

SHUTTERSTOCK.COM/RICHARD GOLDBERG

Lozich said it's critical that employees understand that there would never be negative repercussions from reporting something they deem suspicious. "We never bite the hand that feeds us. We never say, 'Don't call us again on this.' We treat every one as important. If it's important enough for an employee to report it to us, we're going to say it's important to us."

The private sector is sometimes accused of hiding information that may be detrimental to business. However, everyone agreed that the stakes are too high to bury information that could thwart a terrorist attack. "We know, unfortunately, that one bad day for one of us is a bad day for all of us," Lozich said. "That binds us together. Our view is we'd rather report something up front than have to suffer the consequences later. There's been a change in that regard."

Lozich said because the industry is the economic engine for the state, Las Vegas is actually like a small community. "We don't have a lot of diverse infrastructure, manufacturing and everything else. That really helps when we have a common goal. We're trying to make this the safest place possible."

Fusion center personnel are careful in releasing data to the industry that might hurt a certain resort or business. "The problem we run into is sharing information with the hotel casino gets into privacy issues," Hibbetts said. "Luckily we have a really good relationship with those entities, and they know that if they tell us something, we will not be telling their competitor."

> "A lot of [fusion centers] say that they are 24/7, but for a lot of them, their phone rings and it goes to a dispatching center. But here you have a fusion center employee answering the phone all the time."
>
> *Patrick Baldwin, manager, Southern Nevada Counter-Terrorism Center crime analysis group*

The information that goes online across the county via Trapwire usually includes general threats and doesn't single out a resort. If there is a threat to a specific hotel, law enforcement will contact that hotel and inform security of the threats.

So could this model work elsewhere? Certainly, especially in other areas with tourist-based economies like Florida and Hawaii, said David Shepherd, CEO of the Readiness Resource Group, which works with UNLV on private-sector security programs.

"What is your business? People. What is your No. 1 asset? People. The model here can be replicated? The fusion center can be replicated. Listen to the people, don't put them on a shelf and tell them you'll get back with them."

Everyone from maids to valets is taught to say something when they see something suspicious.

Population: 2.5 million, give or take
Museums: Span 57 acres
Waterways: Link to global shipping market
Mass Transit: 1.65 million riders per day
Highways: 7 major interstates
Stadium Capacity: 60,000 (more if the Packers are in town)

Sleep much?

Your team allegiance doesn't matter. As a member of a UASI area you know that emergency response and resource accountability are not a game. Federal mandates and NIMS-compliant safety standards must be followed. Mutual aid from surrounding counties and states needs to be validated and mobilized seamlessly within minutes. Incident data must be shared off-scene via the Web.

As the No. 1 provider of tracking solutions and field-based incident management tools in the United States, Salamander Technologies has set the standard with a network of 5,000 interoperable agencies. Are you one?

Scan to read how Salamander played a role in Super Bowl XLII.

Salamander™ TECHNOLOGIES

BlueStar *Your Solutions Distributor*

www.salamandertechnologies.com **877.430.5171**

SHUTTERSTOCK.COM/DMITRY NIKOLAEV

THE DOUBLE-EDGED SWORD

Transportation is the most serious of the Critical Infrastructure and Key Resources elements yet it's also a nexus for man-made or terrorist events.

"Nothing happens until something moves."

That's the motto of the United States Army Transportation Corps, but those words also have special meaning for emergency management. Within the four traditional phases of emergency management — mitigation, preparedness, response and recovery — transportation infrastructure is invariably a vital part, often the problem, and a critical operational element. In fact, in any given event, transportation/mobility and the transportation infrastructure become the operative issues, playing critical roles for initial response and short- and long-term recovery efforts. However, transportation can also be the nexus or cause for man-made or terrorist incidents.

BY BOB JAFFIN | CONTRIBUTING WRITER

Transportation infrastructure is a critical element in response and recovery.

PHOTO COURTESY OF DAVID FINE/FEMA

Although transportation is truly a double-edged sword, it might be the most critical of the Critical Infrastructure and Key Resources elements. Materials and people serve no purpose if we can't transport them to the right location to provide essential services.

Without adequate transportation information, busloads or carloads of critical volunteers and emergency responders can't be utilized. You can create ideally located warehouse facilities and execute indefinite delivery contracts, but unless your transportation network is up to the job, and unless there's coordination with adjoining regions, sometimes crossing state lines, nothing will move. However, with adequate capabilities it's possible to pinpoint the destination and route for up to 100 tractor-trailer loads of critical supplies, or deliver hundreds of thousands of gallons of water and millions of ready-made meals.

An examination of the events of the last five years in the United States demonstrates an inability of state, local and federal managers and executives to respond to transportation needs in an appropriate way. This underscores the need for more thorough understanding and integration of the transportation logistics disciplines. The moment someone says "evacuation," transportation efforts need to go into effect. In almost all cases, evacuation also entails multiple jurisdictions that technically are not contiguous to the affected area. Most evacuation plans end at the jurisdictional boundary of the senior player in the exercise, or are focused exclusively on the beginning of evacuation and not the entire end-to-end process.

Technology has improved our ability to collect and exchange information, vastly enhancing situational awareness. Many times, transportation infrastructure extends well beyond the local jurisdiction's road, rail, air and port capabilities. Large events over large geographic areas require cargo aircraft handling capability in or contiguous to the affected areas, as well as port capabilities, to provide cargo and handling capacity for the extremely large quantities of sustainability and recovery materials and heavy equipment.

Last year's earthquake in Haiti quickly demonstrated that both marine port and airport facilities, as well as surface transportation infrastructure, are critical to all phases of response and recovery. It was impossible to deliver goods and personnel at a rate that the international transportation system could accommodate. A lack of infrastructure or planning for augmentation or use of alternate facilities still prevents

Materials serve no purpose if they can't get to their location.

PHOTO COURTESY OF GREG HENSHALL/FEMA

The Cooperative Purchasing Network
TCPN
Official Contract Holder
Look for The Official Seal of Compliance

The Key to What You Need

TCPN helps you get the exact products and services you need from the vendors you want, all while meeting state procurement laws. Along with our contracts for office supplies and facilities TCPN has awarded vendors that offer solutions for energy, technology, and transportation.

So when you need something fast or want to choose your vendor, take a look at our list of TCPN Official Contract Holders...they're all competitively bid and bid law compliant. See what the purchasing power of governmental entities working together nationwide can do for you and your budget!

Key in www.TCPN.org today!

TCPN®
The Cooperative Purchasing Network
www.TCPN.org

An examination of the events of the last five years in the United States *demonstrates an inability of state, local and federal managers and executives to respond in an appropriate way.*

goods and personnel from flowing into and out of Haiti at the rate required. This winter there were multiple instances where neither snowplows nor sanding and salting trucks could stay on the slick highways. Couple this with the amount of utility infrastructure strewn across both roads and rail, and the flooding of both roads and rail, and you can see that transportation infrastructure is the most critical link in emergency response — beside communication and the first responders themselves. Some tragedies that gained nationwide attention as a result of the snowstorm in New York City also underline issues related to fully understanding the protection and use of transportation infrastructure.

There are many organizations and individuals, including transportation infrastructure owners and transportation providers, that emergency managers must engage with and include in their routine planning. The larger the jurisdictional unit, the more important it is to have awareness of and a grasp on the essentials of the areas of expertise of the following organizations:

- **American Association of State Highway and Transportation Officials:** Perhaps this organization, along with the Transportation Research Board, has the strongest and closest ties to emergency management. As the name indicates, it's a state-level organization, and the key component of this organization for emergency managers is the Special Committee on Transportation Security and Emergency Management.
- **Federal Motor Carrier Safety Administration:** If you want any exceptions made to the rules governing commercial trucking, these are the people you need to contact, especially during an emergency.
- **Pipeline and Hazardous Materials Safety Administration:** The administration has five regional offices staffed by hazardous materials specialists whose primary function is to provide outreach to the business and government sectors — they inform and educate, not enforce! It produces one of the most sought after publications in the world, the *Emergency Response Guidebook*.
- **Transportation Research Board:** Should also be of value to, and definitely in the libraries of, every emergency manager.
- **American Automobile Association:** If you expect people to use privately owned vehicles for any form of self-evacuation, you cannot afford to ignore this organization.
- **Federal Highway Administration**
- **Federal Transit Administration**
- **Maritime Administration**
- **Federal Aviation Administration**
- **American Association of Motor Vehicle Administrators**
- **Commercial Vehicle Safety Alliance**
- **American Ambulance Association**
- **Towing and Recovery Association of America**

Bob Jaffin sits on the editorial working group, and the training and education committee of the International Association of Emergency Managers. He spent nine years with the Navy Transportation Management School/Navy Supply Corps School acting as the Navy's senior HAZMAT transportation instructor.

PHOTO COURTESY OF MICHAEL RIEGER/FEMA

Esri Homeland Security GIS Summit

Now more than ever, it's important to know how to meet your mission and bridge the gap between limited resources and high expectations. Be part of the world's only geographic information system (GIS) conference for homeland security. Explore how the geographic approach helps you do more with less, providing a framework for intelligence-led, mission-critical decision making.

July 9–12, 2011
Hilton San Diego Bayfront
San Diego, California

esri.com/hssummit

esri®

PHOTO COURTESY OF MARVIN NAUMAN/FEMA

WHERE IS MILEPOST 243?

WHY EMERGENCY RESPONSE PLANS SHOULD INCLUDE THE RAILROADS.

Railroads shouldn't be mysterious entities in an emergency, yet local emergency response plans often don't cover them to a necessary extent. The railroad poses all the threats and liabilities of a major highway system, with one exception: A rail disaster is usually monumental and frequently becomes a multijurisdictional event.

Railroads are pioneering the transportation sector with intermodal, improved track conditions; computerization; fuel efficiency; employee optimization; and mergers. Yet railroads remain, next to domestic airlines, the safest form of transportation. Rail accidents for 2010 totaled 1,830, which included 261 highway grade crossing fatalities, 451 trespass fatalities, 20 rail employee fatalities and 4,272 nonfatal employee injuries, according to the Federal Railroad Administration (FRA) 2010 safety results.

Unlike other transportation systems, railroads are private and not dependent on the government. However, emergency pre-planning for a large-scale rail event is critical, especially as railroads become the most profitable and efficient form of U.S. freight transportation.

BY JOHN CEASE | CONTRIBUTING WRITER

Understanding how railroads operate is critical to the emergency manager.

PHOTO COURTESY OF MARVIN NAUMAN/FEMA

Increased fuel costs and initiatives to be more environmentally friendly have translated into more trains, increased speeds and additional freight and passenger traffic. Industry experts predict that volume will double by 2035. High-speed rail initiatives and increasing passenger loads will result in more railroad emergencies, which emphasizes the need for better local government emergency planning — increases in hazardous material (HAZMAT) transportation and passenger counts are not just homeland security concerns.

A comprehensive plan should address the following: Quickly determining the precise location, identifying the best access and staging areas, multijurisdictional coordination, potential for mass causalities and, if necessary, evacuation of rail passengers. Consideration must be given to a HAZMAT factor that may result in releases or spills. Emergency management should be prepared for the worst-case scenario. To ignore the railroad in your emergency plans would be like ignoring a major interstate highway or airport in your jurisdiction.

Understanding railroad basics can significantly enhance emergency responses. Here are specific questions emergency management needs to address when forming a rail emergency response plan:

- Does the plan identify each separate railroad in the response area?
- Does the plan include accurate emergency contact information for each railroad?
- Does the plan incorporate railroad milepost locations on response maps?
- Is the plan reviewed, verified and updated for continued changes?

In an emergency situation, quick decisions must be made regarding where, what and which types of public-sector resources are needed. One of the most important factors is understanding the railroad milepost address system that's used by all railroads to identify geographic locations. Like the street addresses in 911 computer-aided dispatch (CAD) or other map systems, the milepost address will be used by the railroad and needs to be integrated into local emergency planning because it's the only reference used by railroaders when noting a location on a rail line.

Failure to incorporate railroad mileposts into emergency plans could slow a meaningful response or cause an incident to expand exponentially.

Consider an emergency reporting scenario:

Railroad engineer to dispatcher: "This is W43. Our train went into emergency. We are on the ground at about Milepost 243. We have HAZMAT cars 10 in from the rear. Advise 911. I can see a plume of smoke from here."

Railroad dispatcher to 911 center: "I have a train derailment with a possible HAZMAT problem at Milepost 243. We probably need a fire and police response."

911 center to railroad: "Where is Milepost 243? Can you advise the nearest highway intersection? What county are they in? Can they move to the train to the nearest crossing?"

This is the beginning of a long and tense emergency management disconnect, in which failure to incorporate mileposts into the emergency plan slowed response time. In an emergency situation, quick decisions must be made on where, what and which types of public-sector resources are needed. As an emergency manager, you can ask a number of questions to enhance the public safety's response capability:

Where is Milepost 243 in relation to a highway map? Where can access be found to the right of way? Where can equipment be staged? What resources does the railroad have? How can you direct other jurisdictions to the milepost location?

Understanding how railroads are organized and operate is also critical to an emergency manager's portfolio of plans in order to interpret and act quickly on a railroad report to 911. This information is rarely integrated on any 911 maps.

Perhaps most critical to that plan is an understanding of how railroads are addressed and operated. Railroads have a mile marker system line address similar to that found on interstates and major highways. Railroads similarly call them the milepost.

The milepost (MP) addresses are set at approximately one-mile intervals along a designated

Get rid of the wires and the worry. *Government agencies connect securely and wirelessly outside of the office with Sprint Data Link.℠* ***Get in on the Now Network.™***

Sprint
The Now Network™

Your government work has moved outside the walls of a traditional office. With Sprint Data Link, your team can access intranets, shared files, department email and other critical applications outside of the office, all without compromising security. It's an easy and cost-effective way to provide a safe, seamless VPN connection between your enterprise network and the Sprint 3G and 4G networks. Just choose one of the following ready-to-go connectivity solutions.

1. Sprint 3G and 4G networks

> Give employees access to your agency network with Sprint-certified mobile broadband devices

> Help your on-the-go team communicate instantly with co-workers and other agencies

> Download important documents securely at lightning-fast speeds

> Enjoy greater flexibility with mobile broadband devices that can be plugged into laptops or embedded inside them

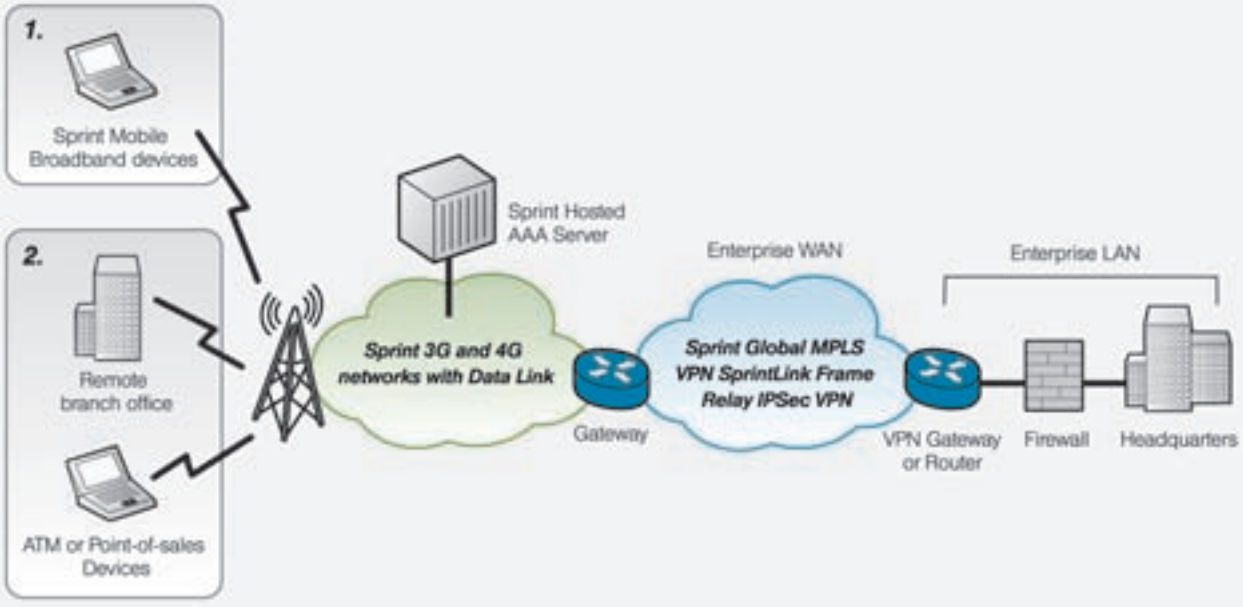
2. Sprint Wireless WAN

> Utilize Sprint-certified wireless modems or routers to create a WAN for your agency

> Use the WAN as a dependable wireline back-up or a low-bandwidth primary alternative

> Ensure redundancy for critical operations

> Add fixed sites or get mobile sites up and running more quickly and cost-effectively than with a wireline solution



Sprint Business Solutions Partner

FEENEY WIRELESS™

Feeney Wireless

(800) 683-4818

sales@feeneywireless.com

Railroads are pioneering the transportation sector with intermodal, improved track conditions and computerization.

PHOTO COURTESY OF MARVIN NAUMAN/FEMA

line with an MP 0 starting point. As the train moves away from MP 0, the milepost addresses increase sequentially. The distance between mileposts often varies because of rail line acquisitions or relocations, but this is not a problem because each milepost represents an unchanging specific geographic location on the line.

Switches, signals, sidings, bridges, tunnels, stations, highway grade crossings and other railroad infrastructure called "waypoints" between mileposts are assigned a milepost address. The milepost address is usually carried out to the hundredth of a mile. For example, a highway grade crossing may have a railroad MP address of 251.67. That indicates that the crossing is 251.67 miles from MP 0 on that specific line. Switches and/or signals that are remotely controlled from a control station are known as controlled points with names like CP MAX or CP 144.

Since railroads have multiple lines and branches, they usually have a "pre-line" alpha designator, ranging from one to three letters, such as A. For example, on the CSX Railroad, MP A 68.71 is a grade crossing in rural Skippers, Va., on the A line, 68.71 miles south of Richmond, Va. When a railroad reports an event to a 911 call center, it will refer to the MP address. It is precise to them but is rarely integrated on 911 maps.

To ignore the railroad in your emergency plans would be like ignoring a major interstate highway or airport in your jurisdiction.

Public grade crossings have a street name or highway number. In addition, every public and private "at-grade" crossing has a railroad milepost address and a unique U.S. Department of Transportation (DOT) six-digit number followed by an alpha qualifier. That identifier must be posted at every rail crossing and is monitored by the FRA's grade crossing inventory. Recent federal legislation requires the operating railroad to verify the inventory for accuracy every three years.

The highway grade crossing posting requires an emergency phone number, the operating railroad's name, the line's MP address and the DOT inventory identification number. There are approximately 211,000 such grade crossings in the United States, each with a unique DOT number. If accurate, this posting provides good rail addressing information. An emergency manager could establish a base MP map of a rail line in the jurisdiction.

Because of the number of rail consolidations, abandonments, mergers and failure to update crossing inventory postings as required by law, the grade crossing postings and inventory have a significant error rate. Like any business, there are constant changes on the railroad. It is important to remember that the person in charge of the local railroad's operation may be hundreds of miles away and never personally seen the line for which he is responsible. Verify and update your railroad file regularly.

If done correctly, GPS mapping of rail lines is viable and cost-effective for emergency management. Typically each rail owner's lines are GPS plotted and given an electronic footprint.

Integrating GPS mapped rail lines to include grade crossings, mileposts and other railroad infrastructure with existing maps promotes enhanced government emergency planning. Several years ago, a National Transportation Safety Board investigative report recommended that the National Emergency Number Association facilitate the inclusion of railroad milepost markers on all local emergency response maps across the country.

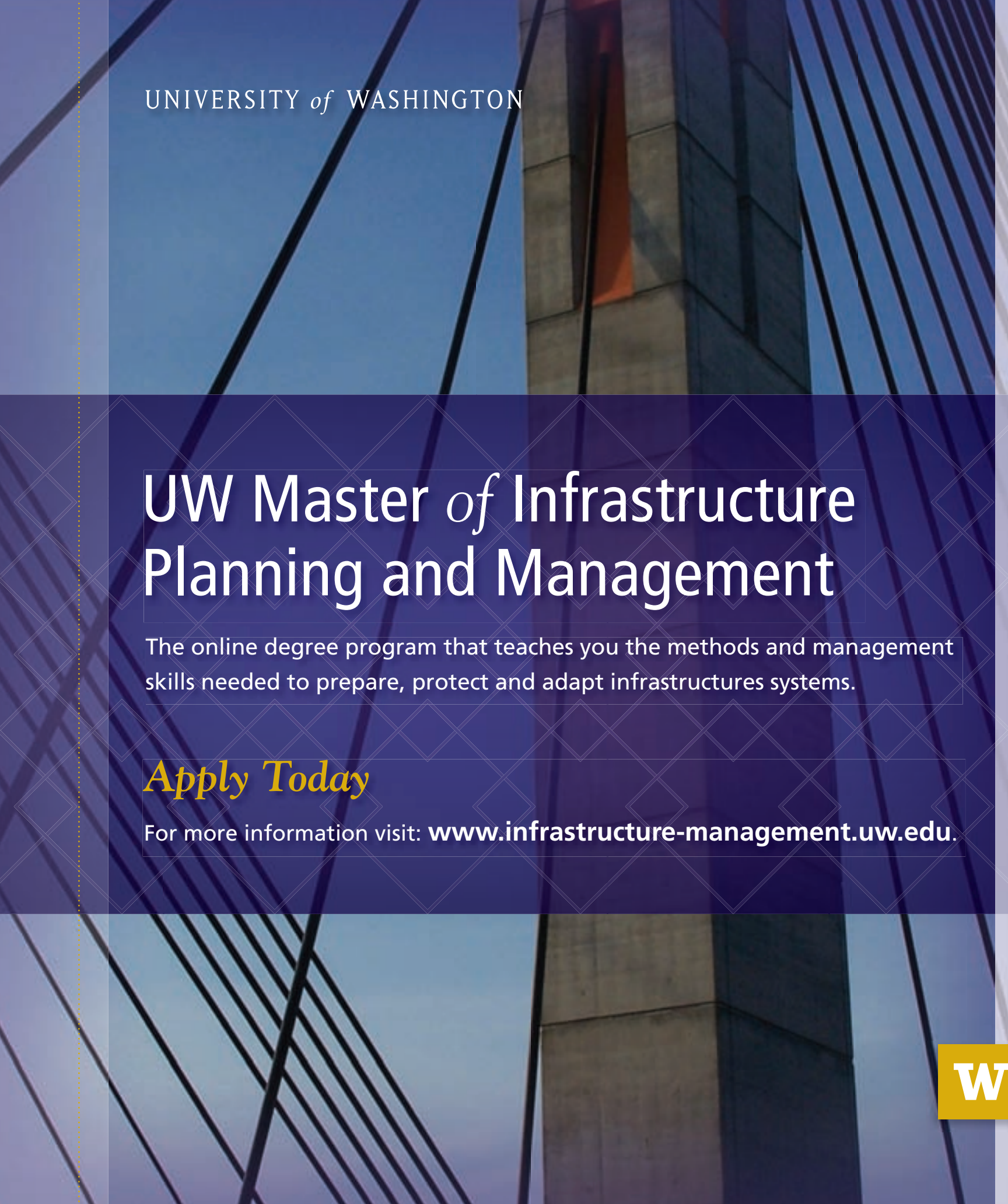
Many railroads do GPS mapping of their lines, but the data is done for engineering and maintenance purposes, and doesn't encompass the land outside the immediate right of way. By integrating two well addressed bases, railroads and the community, emergency outcomes can be improved.

Even if a jurisdiction doesn't GPS map its rail lines, there's a lot one can do to learn about rail operations: Identify the rail dispatch point of control for your jurisdiction; remember there may be more than one railroad in your area; know whom to contact in a rail emergency; understand the railroad's emergency response resources, the freight or passenger loads that can be anticipated, grade crossing locations and access points for difficult locations.

If you have a railroad in your jurisdiction, know the questions to ask so you can ensure that your emergency responders can perform to their peak capacity. Nothing frustrates emergency responders like knowing there is a serious problem and not knowing exactly where it is or how to get there.

Understanding where Milepost 243 is should not be an emergency management mystery.

John Cease is president of Clear Tracks Ahead, a corporation dedicated to the safety of the railroad industry, and formerly the chief of police in Wilmington, N.C., and Roanoke, Va.



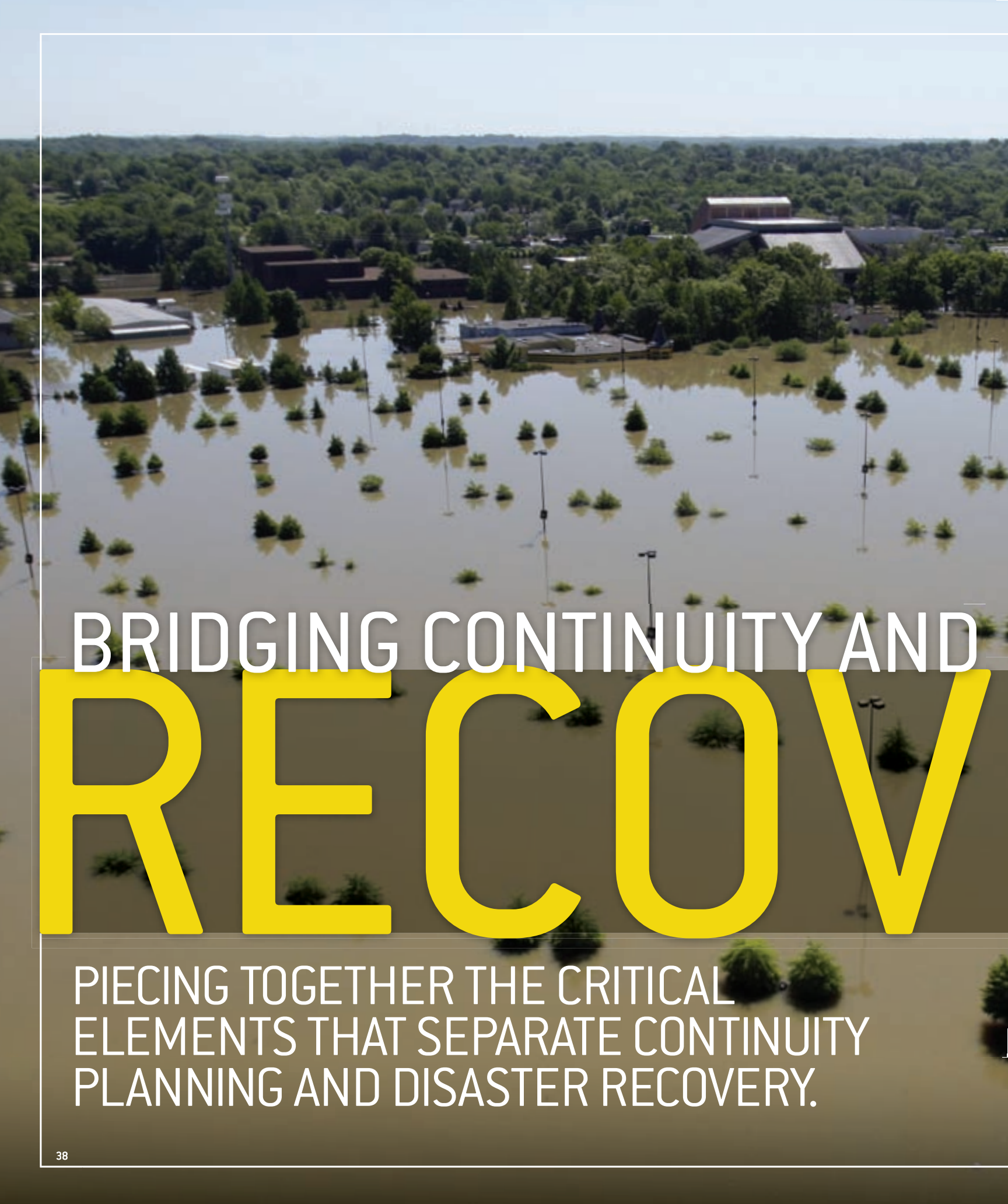
UNIVERSITY of WASHINGTON

UW Master of Infrastructure Planning and Management

The online degree program that teaches you the methods and management skills needed to prepare, protect and adapt infrastructures systems.

Apply Today

For more information visit: **www.infrastructure-management.uw.edu**.



BRIDGING CONTINUITY AND RECOV

PIECING TOGETHER THE CRITICAL ELEMENTS THAT SEPARATE CONTINUITY PLANNING AND DISASTER RECOVERY.

A major flood may have meant the end of business as tenants of this mall knew it.

ERY

BY VALERIE LUCUS-McEWEN CONTRIBUTING WRITER

AP IMAGES

ISTOCKPHOTO.COM

During a disaster, emergency responders tend to "put out the fires" and move on. The other responsibilities, such as continuity — or keeping it all together during and after the response — and recovery — putting it back the way it was or creating resiliency in order to survive the next event — fall to someone else. And unfortunately in most agencies, jurisdictions or companies, that responsibility depends on a group of people — an emergency manager, business continuity manager, risk manager, IT disaster recovery manager or others depending on the circumstances. In this situation, we often see the "Lone Ranger analogy," according to Mike Martinet, principal of the Martinet Group, which trains government agencies on disaster finance issues. "Think of a dozen Lone Rangers, determined to uphold justice and rescue the damsel in distress, who all ride in and surround the bad guy," he said. "And then they start shooting."

Although the bottom line is the same for everyone — restoring the community — the lines between continuity and recovery and who is responsible for what are blurry. All of this is compounded by confusing vernacular, jealously guarded silos and just plain stubbornness.

A hallmark of the Incident Command System is the use of common terminology to avoid the confusion that results when a word or phrase has a different meaning for different groups. Unfortunately neither recovery nor continuity planners appear to subscribe to the Incident Command System.

For example, from an emergency management point of view, disaster recovery is the phase between response and mitigation. From the business continuity point of view, disaster recovery is the process for recovering or continuing a technology infrastructure.

Emergency management is still regularly confused with emergency response. Continuity of operations planning most often refers to the plans developed by governmental agencies to ensure their survival. Its erstwhile predecessor was continuity of government.

PHOTO COURTESY OF DANIEL CIMA/AMERICAN RED CROSS

Multiple businesses in downtown Nashville suffered extensive water damage as a result of flooding of the adjacent Cumberland River in 2010. Many of the businesses took weeks, if not months, to get back on their feet.

Continuity management can have various meanings depending on the context. Business continuity generally relates to ensuring that critical business functions continue with no, or very few, interruptions; academic continuity speaks to the critical teaching-research side of higher education; knowledge continuity is the practice of gathering and maintaining institutional information so it isn't lost when employees leave or retire.

In disaster planning, or even in the middle of a disaster, how those words and phrases play out varies. For David Burns, emergency preparedness manager at the University of California, Los Angeles, and former emergency services coordinator at the El Segundo Fire Department in Southern California, it is as simple as asking the question: Are you dealing with people or business?

The biggest problem, Burns said, is that often the business continuity planning side doesn't always plan for people. "It talks about resiliency where there is an investment, stockholders and a board of directors — all those affect Wall Street," he said. "If you asked the actuaries, they'll tell you people have no actuarial value, no value to the bottom line."

The conflict of either helping people or helping the bottom line is one of the drivers behind the silos and stovepipes in which planners, including actuaries, often put themselves. But concern about people, not only as employees, but also as customers, has been part of business continuity planning for a long time.

"There is no point to continuity if you aren't using it to recover your community. If the community isn't there, you aren't going to have a business to support," Martinet said. "It doesn't matter if you can get Starbucks open if you don't have the staff to run it or the people to purchase a caffe latte.

"Continuity is the bridge that gets you to recovery," he added. "They are both important, and you can't do one without the other."

Nevertheless, questions regarding the lines between recovery and continuity continue to color our discussions. Trying to sort out where these turf wars started goes back to the late 1970s.

At about the time former President Jimmy Carter issued the executive order that created FEMA in 1979, people responsible for the data in mainframe computers began to recognize how dependent their organizations were on computer systems, and the vulnerability of those systems to outside forces. IT disaster recovery grew quickly, driven by the Internet and real-time processing. By the early 1990s, the IT disaster-recovery focus shifted to enterprisewide holistic planning and started becoming known as "business continuity planning."

> "[OFTEN THE BUSINESS CONTINUITY PLANNING SIDE] TALKS ABOUT RESILIENCY WHERE THERE IS AN INVESTMENT, STOCKHOLDERS AND A BOARD OF DIRECTORS — ALL THOSE AFFECT WALL STREET."
>
> — **David Burns**, emergency preparedness manager, University of California, Los Angeles

In the meantime, emergency management was moving forward and trying to create a profession out of its civil defense roots. The U.S. Civil Defense Council, founded in 1952, became the National Coordinating Council of Emergency Managers in 1985 and then the International Association of Emergency Managers in 1996.

By the mid-1990s, a major split between emergency management and business continuity planning ensued. Rick Tobin, president and CEO of TAO Emergency Management Consulting, said it was clear by that point there would be a strong divide between (macro) government interests and (micro) information management.

"Those who were oriented more toward data information and cash flow went on the new path and those who were oriented toward protecting public structure and continuity of government stayed on the old path," Tobin said. Those who were involved in emergency management disaster recovery were less technically oriented, he said. "They didn't understand the systems for moving data. They were still in a world of organizational structure and resources."

The first real wake-up call for both sides was Y2K, according to Tobin. "It became even clearer they hadn't been paying attention to each other and the mistakes they might make could kill people," Tobin said. "It

wasn't very comfortable on either side of that fence."

The uneasiness between emergency management and business continuity was fueled to some extent by the 1995 release of the first National Fire Protection Association (NFPA) 1600 document *Recommended Practice for Disaster Management*, which contained little guidance for restoring the business side of a disaster.

Steve Davis, president of All Hands Consulting, has been in the business for 40 years, long enough to have watched this history unfold. "Recognizing the convergence and obvious interdependencies between business and the community, NFPA involved the business community in the development of [the next version of] NFPA 1600 and consideration was given to their unique concerns," he said.

The 2000 version of NFPA 1600 was called *Disaster/Emergency Management and Business Continuity Programs*. "It is interesting to note that the title was created in an effort to make all of the various participants comfortable with the final product," Davis said.

In 2003, in the aftermath of 9/11, two professional associations for business continuity professionals, the Disaster Recovery Institute International and Business Continuity International, collaborated on a set of Professional Practices for Business Continuity Professionals, and all subsequent versions of NFPA 1600 included a crosswalk between existing emergency management and business continuity practices.

> "THE NEW BEST PRACTICES IN BOTH SECTORS ARE CONSIDERING A MORE COMPREHENSIVE AND HOLISTIC APPROACH TO PLANNING."
>
> — Steve Davis, president, All Hands Consulting

In the past few years, other standards have been introduced or rewritten related to this issue, most of them are on the business continuity side: BSI 25999 (business continuity management); ISO 31000:2009 (risk management principles and guidelines); and ISO/PAS 22399:2007 (*Guideline for Incident Preparedness and Operational Continuity Management*).

Why are standards important? Standards allow a company or jurisdiction to plan for an event that meets the requirements of multiple interests. Standards allow the public, communities, legislators, company executives, government officials and insurance companies to say, "We did our due diligence and met the recognized standards."

Some standardization is necessary to bring emergency management proponents and continuity management proponents together. On the other hand, some argue that the sheer number of standards adds to the confusion and discord, and they don't begin to answer the bottom-line question: How many Lone Rangers does it take to restore a community — the whole community — after a disaster?

Davis sees a greater convergence of public- and private-sector planning efforts. "Businesses have been expanding disaster recovery plans to include continuity of operations and emergency response planning, while governments have been expanding old civil defense and continuity of government concepts to include mitigation and recovery," he said. "There are lots of overlaps and intersections. The new best practices in both sectors are considering a more comprehensive and holistic approach to planning."

That new planning approach might look different than it does today — and may not be as contentiously debated.

The latest approach that attempts to pull the concepts of disaster recovery and

PHOTO COURTESY OF FEMA/TIM BURKITT

The lines between continuity and recovery are blurry and communities can pay for that.

continuity planning together (while factoring in mitigation) is built around resiliency. Because "resilient" is a fairly new term used in an emergency-disaster planning context, the definitions vary. Generally it's defined as the ability of an organization or community to rebound following a crisis or disaster event. What constitutes resiliency are recovery, continuity and mitigation planning.

Claire Rubin, principal of Claire B. Rubin & Associates, an emergency management and homeland security consulting firm, has seen many new concepts in the 33 years she has worked in the field. "Some view resilience as a kind of nirvana, a wonderful state we might reach someday," she said. "Resiliency can't really be defined, and focusing on the new concepts and definitions may sidetrack us from what needs to be done.

"Creating new words and concepts doesn't necessarily help emergency or continuity managers do a more effective job. Maybe what they need is already there, such as comprehensive emergency management, and we should stick with refining an approach and needed actions we already know."

Davis agrees. "There are lots of intersection and overlaps between disaster recovery and continuity planning," he said. "The intersection here is making it all comprehensive. And comprehensive means comprehensive, not limited or restricted."

Davis offered an example of how a comprehensive recovery-continuity should work. He visited a local grocery store that had recently reopened after a prolonged power outage. Despite the lack of power, the frozen foods section was well stocked and customers were making purchases. The store's plan for a power failure was to move all the frozen food to its walk-in freezer that has a generator. "They didn't lose their inventory, they kept their customers, they helped the community," he said. "The plan worked."

Regardless of whether you're in business or government, it is time to think globally and answer these questions: Who are we trying to protect? How can I make this protection more comprehensive?

This is where stubbornness enters the picture. Remember the adage: Insanity is doing the same thing over and over but expecting different results.

If your plan includes all the basic principles of disaster recovery and continuity planning, if it is comprehensive and includes all the players, the cost of response can be minimized — which is good for the business bottom line and the safety of the public.

How insane is it to try to do anything else? If it isn't broken, don't try to fix it.

Valerie Lucus-McEwen is a certified emergency manager, certified business continuity professional and an instructor/lecturer for California State University, Long Beach. She also writes the Disaster Academia blog for *Emergency Management's* website at www.emergencymgmt.com/academia.

By Austen Givens | Contributing Writer

The response effort during the Gulf of Mexico oil spill demonstrated that government's ability to respond will be limited during catastrophic infrastructure collapse in the United States.

The Limits of Government

The Deepwater Horizon oil spill was an ominous sign for the future of America's critical infrastructure.

In the wake of the Deepwater Horizon oil spill in the Gulf of Mexico last year, renewed focus has been trained on ways that emergency managers can further engage the private sector in mitigation, preparedness, response and recovery efforts. With continuing advances in systems of systems — people, processes and technology working together — the need to develop linkages and partnerships to bridge this public-private divide will become increasingly pronounced. Emergency management as a whole should begin to think deeply about proactively building relationships with private-sector partners — and with a renewed urgency linked to the coordination issues identified in the aftermath of the nation's worst environmental disaster.

Two key reports form the basis of public knowledge about the Deepwater Horizon disaster: the National Commission on the BP Deepwater Horizon Oil Spill and Offshore Drilling's *Report to the President*, released in January 2011, and BP's *Deepwater Horizon Accident Investigation Report*, published in September 2010. Perhaps the most jarring finding from the former is that despite government's efforts at all levels to stem the flow of oil in the Gulf, the right combination of equipment, subject-matter expertise and personnel necessary to stop the oil flow at its source was situated squarely within the private-sector domain. Indeed, the commission noted that the mix of knowledge and tools necessary to operate at such depths came exclusively from private-sector sources — not only from BP, but also its competitors.

Drilling for energy deep beneath the Gulf's surface has been compared to operating in outer space. The sophistication of equipment, personnel training and technical expertise required to drill more than a mile beneath the Gulf's surface is remarkably complex. The depths of the Gulf floor,

PHOTO COURTESY OF DVIDSHUB/FLICKR

particularly in the realm of energy extraction, are largely controlled and understood by the private sector. However, with the exception of a handful of private firms now shooting rockets into space, the Earth's orbit remains heavily the domain of government — NASA and its counterpart agencies around the globe — not the business world.

Officials from the U.S. Department of the Interior's Minerals Management Service, the agency charged with monitoring BP's deepwater drilling activities, admitted to the commission that effective oversight of deepwater drilling activities was limited in multiple respects: The scope of oversight was tightly defined, only four to five Minerals Management Service officials in Houston were responsible for monitoring BP's Gulf drilling activities at any given time, and BP had substantially more experience and understanding of the intricacies of deepwater drilling. These factors demonstrate that the private sector, not government, possessed the right mixture of knowledge, skills and equipment to manage a leak the size of the Deepwater Horizon spill.

Today roughly 85 percent of the nation's critical infrastructure is controlled by the private sector.

Examined in aggregate, these observations can lead us to a series of assertions about future trends in emergency management.

First, as complex systems continue to proliferate — converging people, processes and technologies — equally sophisticated failures of those systems are likely to emerge. Therefore public-sector emergency management agencies should begin engaging more deeply with the private sector to head off the effects of complex failures arising from these trends.

Second, and potentially more troubling, is that disasters like Deepwater Horizon that require intense and sustained response and recovery efforts by the private sector, remain a real possibility in the coming years. From supervisory control and data acquisition systems regulating the movement of water behind dams; to firewalls guarding critical research data; to interoperable radio systems bridging local, state and federal agencies, the explosion of complex systems in today's world brings a correspondingly high vulnerability to cascading failures. The commission has cited the Columbia space shuttle disaster and 1989 Exxon Valdez spill in Alaska to highlight the reality of contemporary complex system failures.

Third, and perhaps most critical, is that the private sector controls the majority of the nation's critical infrastructure.

In discussing these potential infrastructure failures, we are not merely describing an inevitability, we are also talking about disasters involving the backbone of American infrastructure — clear response and recovery capabilities that are absent within government.

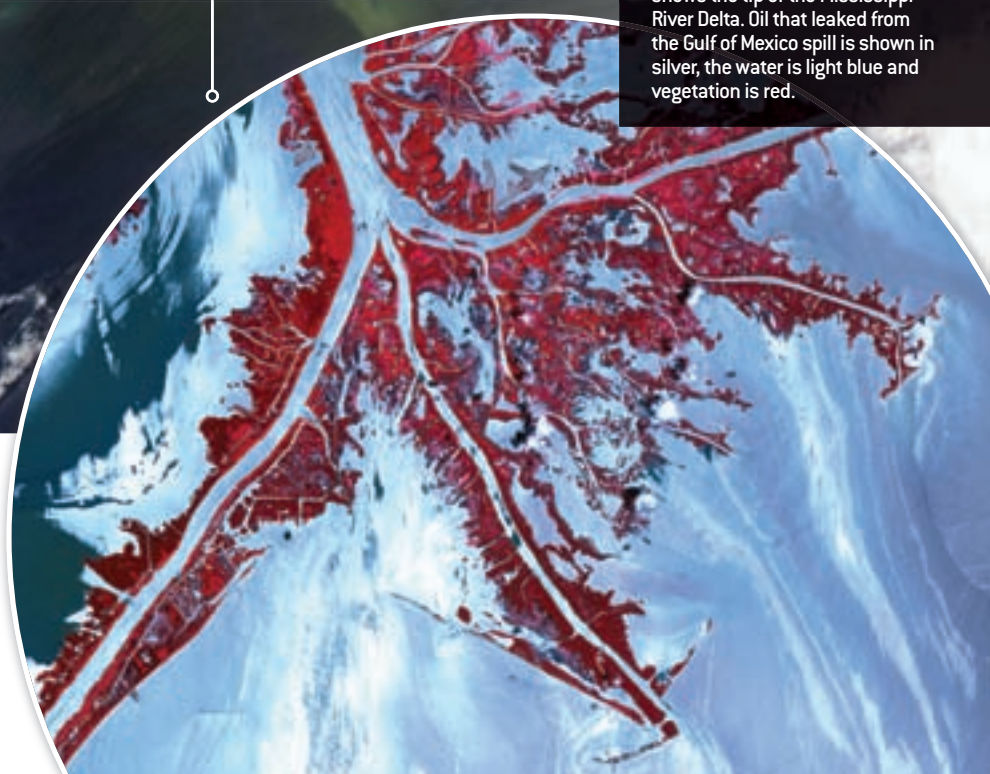
The potentially affected industries and facilities are myriad: Power plants in Virginia, electrical substations in Kentucky and underground gas lines in Louisiana are all captured under the heading of critical infrastructure controlled by the private sector. From Portland, Ore., to Laredo, Texas, thousands of miles of fiber-optic cable connects people by phone and computer.

Certain hospitals in Kansas, banks in New Mexico and the electronic architecture of airports from New York to California are controlled, to varying degrees, by the private sector.

In short, critical infrastructure in our communities is vulnerable to disruption, and the

PHOTO COURTESY OF NASA_GODDARD SPACE FLIGHT CENTER/FLICKR

A view of the Gulf of Mexico on April 25, 2010, five days after an explosion on the Deepwater Horizon drilling rig. The leak was stopped July 15, 2010, after approximately 4.9 million barrels of crude oil had spilled into the Gulf.



A NASA image from May 24, 2010, shows the tip of the Mississippi River Delta. Oil that leaked from the Gulf of Mexico spill is shown in silver, the water is light blue and vegetation is red.

private sector — not government — is in charge of most of it.

The Deepwater Horizon spill shows that more than one mile beneath the surface of the Gulf, government lacks a cohesive, integrated ability to respond to a complex systems failure. Where else are there governmental gaps in capacity to respond to and recover from complex emergencies involving critical infrastructure? A national disruption of Internet connectivity? A regional blackout such as the 2006 Queens blackout that left New Yorkers without power for more than a week? A nuclear power malfunction like Three Mile Island in 1979?

Emergency managers in government can extract many useful lessons from the Deepwater Horizon event about incident management, emergency planning and interoperability of people, agencies and technology. We would be remiss, though, to not look again at how we interact with the energy sector, as well as other private-sector firms and industries in our communities that need to be a part of the broader conversation about emergency management.

OIL SPILL HOT SPOTS

Analysts for the Oil Spill Intelligence Report track oil spills of at least 10,000 gallons and reported that spills in that size range have occurred in the waters of 112 nations since 1960.

They identified the following hot spots for oil spills from vessels:

- Gulf of Mexico (267 spills)
- northeastern U.S. (140 spills)
- Mediterranean Sea (127 spills)
- Persian Gulf (108 spills)
- North Sea (75 spills)
- Japan (60 spills)
- Baltic Sea (52 spills)
- United Kingdom and English Channel (49 spills)
- Malaysia and Singapore (39 spills)
- west coast of France and north and west coasts of Spain (33 spills)
- Korea (32 spills)

SOURCE: NATIONAL OCEANIC AND ATMOSPHERIC ADMINISTRATION PHOTO COURTESY OF NASA_GODDARD SPACE FLIGHT CENTER/FLICKR

To its credit, FEMA has made strides in cultivating ties with the private sector. A dedicated section of the agency's website, www.fema.gov/privatesector, provides emergency preparedness tips, training opportunities and resource documents integral to emergency management in the business world. FEMA's Strategic Foresight Initiative also serves as a valuable national forum for discussion of concerns related to the interaction of governmental and private-sector entities in emergency management.

In a related vein, the Virginia Department of Emergency Management offers regular training on increasing cooperation between public- and private-sector organizations in emergency response.

Headway is being made, and these steps at the federal and state levels are encouraging signs of continued progress.

Putting together a tabletop, functional or full-scale exercise in accordance with the Homeland Security Exercise and Evaluation Program requires significant planning and discussion. During the initial stages of designing your exercise, consider writing in a role for a local private-sector partner. Perhaps on-scene responders need to have 100 hot meals delivered during your exercise, or volunteers need quick access to a cache of cell phones to aid recovery operations.

Create Incentives Together

From senior policymakers to the general public, one of the emergency manager's most challenging responsibilities is to cultivate, build and sustain emergency management capacity across all phases of the cycle — mitigation, preparedness, response and recovery. With this in mind, consider creative ways to build capacity in the partners you seek to engage.

Offer to visit firms and provide a brown bag lunch discussion on the National Incident Management System and Incident Command System.

Frame emergency management concerns in the language of your private-sector partners. Speak clearly about risk management, potential disruption of revenue streams and the long-term value proposition of being prepared.

Develop working relationships with private-sector security professionals and emergency managers.

Consider lobbying your local or state government representatives, in conjunction with private-sector emergency managers, to develop suggested baseline preparedness requirements for businesses in your area.

The Deepwater Horizon disaster offers countless lessons for emergency management on the need to forge deep, lasting ties with the private sector. With 85 percent of the nation's critical infrastructure in the hands of businesses, and complex system failures becoming an increasing reality for emergency managers, building bridges across the public-private sector divide is imperative for emergency managers in government.

Where else are the governmental gaps in capacity to respond to and recover from complex emergencies involving critical infrastructure?

The following practical tips can serve to further clarify the thinking of emergency managers in government, higher education and nonprofits that want to engage more fully with their private-sector partners.

Plan Together

Emergency management scholarship is clear in viewing planning as a process to be worked through, rather than a series of documents to be finalized. Seek out the private-sector firms that have an obvious stake in your operations — electrical companies, gas providers, telecommunications firms and medical providers — and bring them to the table as part of your regular planning cycle. Recurring, biweekly 10-minute phone calls to share information with these organizations can be an effective, low-cost, convenient starting point for enhancing your relationship.

Train Together

Including local first responders in classroom or hands-on training is beneficial to your work as an emergency manager. Consider also inviting representatives from local hardware stores, big box chains (Walmart, Target, Kmart) and commercial food suppliers (Sysco). Few things can bring together new partners in emergency management like joint learning and training, and it all starts with a simple e-mail or phone call invitation.

Austen Givens serves as the director of emergency management at Christopher Newport University in Newport News, Va., and is a fellow with the National Homeland Security Project at Virginia Commonwealth University in Richmond.

PHOTOS BY GRAHAM BLAIR

Ron Lane

Director, San Diego County Office of Emergency Services

Lane has been the director of San Diego County's Office of Emergency Services since 2006. He served as director of the Emergency Operations Center during the 2007 firestorm. Lane has taken the county to new levels of preparation, including for tsunamis. He is a colonel in the U.S. Army Reserve.

What lessons did you learn from the tsunami scare in March?

We only had an advisory in San Diego as opposed to a warning, so we didn't have to do the evacuations. We went through the process of communicating with all our coastal cities and planning a public communication strategy.

So that was a good dry run, and obviously if it was a warning, then we would have been trying to evacuate the 28,000 people who live in our tsunami zone along with most of San Diego. We preregistered those 28,000 people in our [emergency notification] system, called Alert San Diego, and a decision would have been made whether to call and advise them to evacuate. Having just an advisory versus a warning was a good mechanism for us to practice our plans.

What is the greatest risk that you face in San Diego County?

By far our biggest risk is wildfires. We have had two presidentially declared disasters with wildfires in the last eight years: 2003 and 2007. Second would be earthquakes, and third would be terrorism.

> "People get motivated when they see their neighbors doing [preparedness actions] more so than the government."

How do you balance preparation for all of those risks?

For wildfires and earthquakes, a lot of this really focuses on two components long before the response, and that's mitigation and public preparedness. Building codes are the key defense in earthquakes as we saw in Japan, where there was almost no damage even though a huge earthquake happened; obviously the tsunami did tremendous damage. Our work on building codes focuses on retrofitting buildings and ensuring that our properties are earthquake-resistant. Ensuring that the public knows what to do in the time of an earthquake is half the battle and will certainly assist in a response, if we've won the battles with the mitigation and public awareness.

And likewise in wildfires, there is much that can be done in mitigation when it comes to vegetation management and building homes that are in high-risk areas in a way that will survive wildfires; ensuring that we have removed dead and dying trees away from the roadways so that the escape routes remain open. For all our disasters, it really is an all-hazards response when it comes to the mitigation and public awareness component. Obviously the response has different components, but they are all focused on the basic tenets of alert and notification, evacuation, and life and safety response.

Is it difficult to keep the public's attention on emergency preparedness?

We've been battling this since the civic defense days as emergency managers to keep the public engaged and try to create a culture of preparedness — a culture in which people are independent.

People get motivated when they see their neighbors doing [preparedness actions] more so than the government. Instilling a sense of preparedness in neighborhoods, community leaders and community groups, I think, is a major strategy that can be successful.

From an emergency management perspective, we find that just-in-time messaging is a great way to increase awareness. For example, during the recent earthquake and tsunami in Japan, we had precanned and premessaged earthquake and tsunami messages that we immediately publicized on Facebook and Twitter and in editorial and TV interviews.

While people are paying attention to the concept of earthquakes because of what's happening in Japan, it's [opportunistic] to try to get the message out so that people take preparedness seriously here in San Diego for both earthquakes and tsunamis. The best time to get people to prepare for hurricanes is when the hurricane is three days out to sea and coming this way — that's when people pay attention.

Is the county much more prepared than it was three or four years ago?

Absolutely — every year we improve. We are building on our base plans and strategies that have evolved since 9/11 and are really moving on to much more complex and advanced levels

Continued on p. 55

PHOTO BY BRANDON DONNELLY AND STRACOS MEDIA

By Corey McKenna | Staff Writer

NASCAR Testing Ground

Arizona first responders test radios across disparate frequencies in a high-noise environment.

The Subway Fresh Fit 500, a 300-lap NASCAR Sprint Cup race, attracts 75,000 fans to the Phoenix International Raceway each year, doubling the population of the Avondale, Ariz., region.

This year's event took place Feb. 27, but fans began arriving in their fifth wheels and travel trailers to camp out as early as Feb. 21 to attend a week's worth of races, culminating in the marquee race.

"We're managing a small town out there that pops up for one week only," said Lee Baumgarten, director of operations for the Phoenix International Raceway. "So we're challenged to police them and make sure we have fire and medical protection, and all those sort of things."

It was the ideal chance to test multiband radios.

Race officials and the city's ambulance provider were using ultra high frequencies (UHF), firefighters were using very high frequencies (VHF), while law enforcement was using 700 and 800 MHz frequencies. The NASCAR pilot was designed for these responder agencies to test a new model of a full-band full-spectrum radio, called Unity XG-100. Some criteria tested included durability and how well the radios could withstand exposure to heat, liquids, chemicals and sand.

An estimated 400 responders within agencies — including Avondale Fire Department, Maricopa County Sheriff's Office, Glendale and Phoenix police and fire departments, and the Arizona Division of Emergency Management — coordinated activities using 46 of these radios. The pilot results will ideally help smooth over daily communication between responders.

The Arizona Highway Patrol uses UHF, but its officers often interface with local agencies that use a trunked system, said Jesse Cooper, communications/IT project manager for the Phoenix Police Department, and the law enforcement representative on the Phoenix Urban Areas Security Initiative interoperable communications subcommittee.

The Phoenix Fire Department uses VHF radios for hazard-zone operations and also uses a digital

TECHNOLOGIES FOR CRITICAL INCIDENT PREPAREDNESS

TCIP 2011

Conference and Expo

www.tcipexpo.com

Annual Conference and Exposition

August 30–September 1, 2011 • Gaylord National Convention Center

The Technologies for Critical Incident Preparedness Conference and Exposition:

- Highlights DoD, DOJ, and DHS cutting-edge technologies; research, development, test, and evaluation (RDT&E) investments; and training tools for the emergency responder community.
- Provides a forum for emergency responders to discuss best practices and exchange information.
- Offers a unique opportunity for emergency responders; business and industry; academia; and local, tribal, state, and federal stakeholders to network, exchange ideas, and address common critical incident technology, preparedness, response and recovery needs, protocols, and solutions.
- Set on the waterfront of National Harbor, Maryland—with more than 1,200 attendees, and numerous technology exhibits and demonstrations expected—TCIP 2011 is not to be missed.

Attendee Registration—FREE

Register today at www.tcipexpo.com

Presented by:

Department of Defense (DoD), Department of Justice (DOJ), and Department of Homeland Security (DHS)

Sponsored by:

DoD's Office of the Assistant Secretary of Defense for Homeland Defense and Americas' Security Affairs, DOJ's Office of Justice Programs' National Institute of Justice, and DHS's Science and Technology Directorate

Potential Panel Topics:

- Addressing the Active Shooter Threat
- Virtual USA
- Communications Interoperability
- Information Sharing and Intelligence Dissemination
- Open Source Resources for Public Safety
- Deepwater Horizon Oil Spill
- Infrastructure Protection
- Mutual Aid and Regional Partnerships
- Mass Casualty Incidents
- Alerts and Warnings: IPAWS, CMAS, and Social Media
- Personal Location and Physiological Monitoring Technologies
- Cyber Security/Cyber Forensics
- Federal Resources

Advancing Technology

Learning from the past, preparing for the future

Join the Conversation & Follow Conference Updates

trunked system for nonhazard EMS-type calls. Emergency responders in rural areas often use conventional VHF radios.

Cooper sees a place for multiband radios in his department depending on an officer's function. "For standard Phoenix police officers that I manage, they do all of their business day to day on a 700-800 MHz system," he said. "They may not have as much of a need to use the other bands as some of our command and control officers or somebody who is on a task force working with another jurisdiction on a day-to-day basis."

After the race, radios were given to law enforcement agencies statewide to test the concept in their daily operations through the end of March. By mid-month, 20 agencies had joined the pilot.

All Clear

The multiband radios operated over the Phoenix Regional Wireless Consortium (RWC) 800 trunked system, which provided an additional interoperability test. The regional wireless network, composed of 40 towers covering more than 2,000 miles, is built on a Project 25 digital Motorola SmartZone simulcast system, which supports interoperable communications across multiple systems. The RWC network provided the primary communications system used at the raceway, though the UHF and VHF radios operated over separate infrastructure. The pilot was successful, with all radios maintaining constant affiliation with the 800 MHz system, said Morgan Hoaglin, communications coordinator for the Arizona Division of Emergency Management. All tests were completed and police and emergency management officials said the radios' performance was acceptable, give or take a few issues.

> "We're managing a small town out there that pops up for one week only."
>
> **Lee Baumgarten,** director of operations, Phoenix International Raceway

Hoaglin said a metal building used for triage presented the most difficult scenario for testing. "I won't say they did great, but they were better than adequate in that rough coverage area," Hoaglin said. "That's not to say that it didn't go digital for a slight bit of time and you wouldn't lose a syllable every once in a great while. But as far as maintaining communications quality and allowing the operational communications needs to carry on, it was better than minimal. It was good."

In the past, someone typically had to step outside the building to communicate. "This was not the case this time around," he said.

In their initial feedback, Cooper said responders cited ergonomic issues with the antenna being too long and stiff and they would have liked longer battery life. "But we did hear positive feedback from

PHOTO COURTESY OF SHANEY/FLICKR

The Phoenix Fire Department uses VHF radios for hazard-zone operations and also uses a digital trunked system for nonhazard EMS-type calls.

MOBILE INTEROPERABLE VOICE, VIDEO & DATA COMMUNICATIONS SYSTEMS

Connectivity anywhere, anytime, under any conditions. Create your own interoperable network. First Responder friendly. Go live in under five-minutes with one button activation. Low power consumption permits the system to be installed in SUV to full-size mobile command vehicle. Remote diagnostics and live 24/7/365 support.

Bring your command and communications vehicles up to current technology and interoperable capabilities with VisionComms Systems Refresh Service™.

BE READY IN MINUTES, NOT HOURS.

VisionComms

www.vtvisioncomms.com | www.hackneyev.com
+1-252-946-6521 or 1-800-763-0700

VT Hackney

those who were using it that they did like the ability to transition across the three bands using a single radio," he said.

Harris RF Communications, the company that designed the radios used during the pilot, has since designed a more flexible antenna option for the radio.

"The Unity XG-100 is our first true full-band full-spectrum radio in the land-mobile industry," said Dennis Martinez, chief technology officer for Harris. "It operates on all the frequency bands currently used by federal, state and local, which includes frequency bands in the UHF part of the spectrum — VHF, UHF and 700-800 MHz."

In addition, the Unity XG-100 is designed to operate across multiple system types including analog, conventional and trunked, digital and Project 25.

Responders at the track said they'd like to see improvements in how the Unity XG-100 scans across conventional and trunked radio channels. "It's an operation that has certain complexities because of the incompatibilities of conventional and trunking modes," Martinez said.

"It operates on all the frequency bands currently used by federal, state and local, which includes frequency bands in the UHF part of the spectrum — VHF, UHF and 700-800 MHz."

Dennis Martinez, chief technology officer, Harris RF Communications

More Testing to Come

The Arizona test was the first of four planned this year for the Unity XG-100. Details of the other tests haven't been set, but the goal is to test the equipment in various conditions, including deserts; the cold, wet winters of the northeast; and multistate border conditions.

Experience from the Hurricane Katrina response and smoke jumpers fighting wildfires led the U.S. Department of Homeland Security (DHS) to require that the radios use alkaline battery packs for situations in which power grids go down. Another important requirement is that the radios are intrinsically safe for firefighters, said Tom Chirhart, program manager for the DHS Science and Technology Directorate's MultiBand Radio Program. "You need a piece of equipment that will not create a spark so that if a firefighter goes into a building with a report of a gas smell, or a Coast Guardsman goes on board a liquid propane gas tanker — you don't want to see a big hole in the water and nothing left."

The racetrack, with cars whipping by at 200 mph, also provided a chance to test the radio's noise-canceling capabilities. The DHS received reports of responders set up in the center of the track unable to hear the radio over the noise. "It was unintelligible," he said, "so they've had to redevelop the directional microphones and noise-canceling software that will eliminate background noise."

Custom headphones for the noise cancellation worked well, Hoaglin said, as long as the radio's noise cancellation was turned off. "The results were as good as anything I've heard in that noisy of an environment at the track," he said.

In addition to tests of multiband radios from vendors Harris and Thales Liberty, the DHS plans to test radios from other manufacturers, including Motorola, and then compile the findings into a procurement guide to help first responders identify equipment that will meet their needs by February or March 2012.

Smarter, Safer

WITH MORE WAYS TO COLLECT, ANALYZE AND SHARE DATA, TODAY'S JUSTICE AND PUBLIC SAFETY AGENCIES CAN WORK SMARTER AND SAFER.

Introduction

Maps populated with meaningful data allow law enforcement and emergency response personnel to gain better situational awareness.

In public safety, there's no substitute for having key information at the right time. Whether it's a suspect's criminal history, a photo or data on a crime trend, having instant access to current information is critical. That also goes for people working in justice, homeland security and emergency management.

Officers in patrol cars, firefighters, investigators working a case — they all need to act quickly and confidently. When people know they have all the latest information, they can be more confident in their decisions. But too often in the past, critical information was stuck in disparate systems that couldn't communicate with one another. With today's technology, however, those information silos can be eliminated.

New technologies have greatly enabled real-time situational awareness. Fusion centers, real-time crime centers and information analysis centers enable information sharing, analysis and dissemination in ways that weren't possible a few years ago. These centers bring critical data together from numerous sources. They also place the data in front of analysts and investigators who understand what to do with it. So officers and first responders in the field know that the best information, the best people and the best technologies are working together to help them be efficient and safe.

A True Resource

Microsoft has a broad spectrum of tools that can help justice and public safety agencies provide greater safety for the public. The Microsoft Justice and Public Safety Platform provides automated flow of information related to arrests, booking, arraignments and more; integrated data from numerous agencies; connection between disparate databases; case management tools; investigative collaboration features; and mapping for optimum situational awareness.

Microsoft solutions reduce the time investigators need to spend discovering relationships between people, things and events. The solutions break down data silos and put more vital information in officers' hands. Microsoft's Fusion Core Solution (FCS) is one example. FCS is a powerful, structured system for managing the entire fusion center workflow from data intake to dissemination. Tips, leads, suspicious activity reports, trends and other data are delivered to the right people quickly.

Comprehensive and timely situational awareness is crucial, and maps are an effective way to share information visually. With the GIS capabilities from Esri, FCS provides detailed maps depicting personnel, resources, activities or any other critical information related to either day-to-day operations or special events. And activities can be mapped over time.

Microsoft tools give public safety officers appropriate data for decision-making. With too little information (often the case when systems don't talk to one another), officers are put at risk or the bad guys get away. If too much data is collected without the ability to analyze it, it becomes overwhelming and meaningless. Law enforcement officials must also be careful to protect the privacy and civil liberties of citizens while ensuring their safety. The ability to get the data to the right people — different user groups with different levels of access, for example — is also a key consideration.

The Microsoft Justice and Public Safety team focuses intently on the specific needs of law enforcement, courts and the broader public safety community. It knows what public safety agencies need, and how to build solutions that can solve their problems. It knows the business requirements, challenges and standards that need to be met.

With the tools and expertise offered by Microsoft, it's easier than ever to share and analyze information. Connecting databases or agencies for regional, state or interstate information sharing is easier, for example, than it's ever been in the past. And Microsoft systems are relatively simple to maintain and support. It's all part of Microsoft's commitment to providing what justice and public safety agencies really need: greater access to information, and more ways to share it.

New System Enables Core Mission

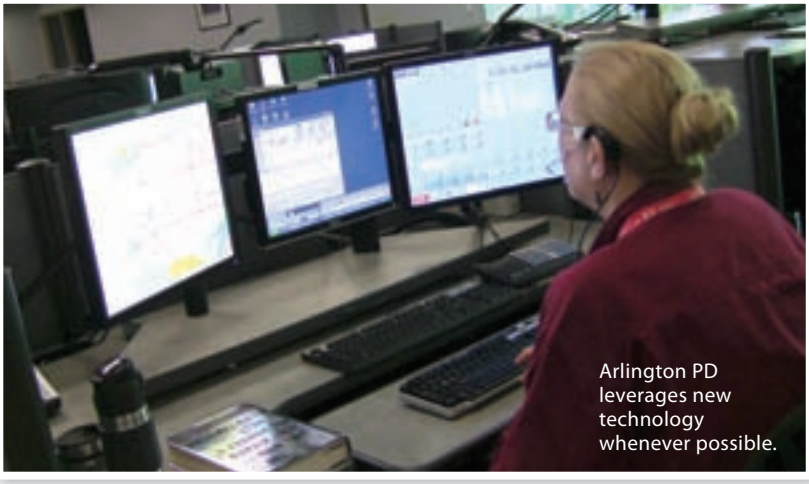
Whether for the Super Bowl or day-to-day operations, a Texas police department depends on data fusion for greater public safety.

Police officers are gaining more access to crucial information.

PHOTO BY PAUL WILLIAMS

What do you do if the Super Bowl is being played in your city? If you're the local police, you'll want a powerful tool to help you share information with numerous other public safety agencies. For the two most recent Super Bowls, played in Miami and Arlington, Texas, respectively, local police chose the same tool — Fusion Core Solution (FCS) from Microsoft.

The Arlington Police Department has 600 officers serving 370,000 residents. But Super Bowl week brings between 100,000 and 200,000 visitors, and public safety becomes a much bigger job. "With the Super Bowl, we have a lot of public safety partners involved in the effort," said Larry Barclay, manager of the Research and Development Division for the department. "That includes federal officials, the FBI, homeland security, state officials and other municipalities in north Texas. To ramp up to that undertaking was not like a typical NFL game. It was much more than that."



Arlington PD leverages new technology whenever possible.

PHOTO BY PAUL WILLIAMS

Now that the game is over, the Arlington Police Department is also planning to use the Microsoft Justice and Public Safety Platform for its daily operations. "We have a decentralized crime-analysis unit; it operates out of four different police stations," said Barclay. "We have seven analysts dispersed throughout the city." The department is planning to centralize the management and increase the effectiveness of those activities by incorporating Microsoft solutions into a new Real Time Crime Center, scheduled to become operational in fall 2011.

More Effective

The center will allow staff there to support officers and investigators working in the field, so they don't have to come in to an office to give and receive data. The Microsoft Justice and Public Safety Platform will allow effective management of data and workflow processes for the department, which needed a solution to help it handle the increasing amount of data it leverages.

"There's an overwhelming amount of information to deal with," said Barclay. "That is the challenge. The Microsoft tools allow us to do a much better job of collecting, organizing and categorizing this information — so we have a chance for every cop to know what every other cop, investigator and intel analyst knows." The GIS capabilities available from Esri will also be used in the future.

Microsoft Services was valuable in setting up the system, noted Barclay. He said it was clear that the team at Microsoft had the expertise to understand what the Arlington Police Department needed.

The department expects to get more from the Microsoft Justice and Public Safety Platform later this year, when it switches from SharePoint 2007 to the 2010 version. "With SharePoint 2010, the framework is greatly expanded, in terms of the capacity to provide tools to the end-user," said Jim Mallard, crime analysis supervisor with the Police Department.

The department regularly collects information from the public, via community watch groups or other community entities. "Eventually we'd like to get that information funneled directly into FCS, so it can be managed without the need to have people route it to other people," said Mallard. Currently it's more of a manual process to look at the data and then send it on to the proper place.

That's just one example of how the department constantly works to become more efficient. It helps to have a good partner, noted Barclay. "I do this work a lot; I work with a lot of vendors," he said. "I don't know that I've ever worked with any company more responsive to our needs than Microsoft."

No More Silos

A California county ties data together seamlessly to create one source for law enforcement data.

The San Diego County Sheriff's Department has approximately 4,000 employees and serves around 3 million residents. The department also operates an information hub for numerous other policing agencies. The San Diego Fusion (SDFusion) system enables the department to collect, analyze and share data. SDFusion also aggregates information from various other systems.

Data from many agencies is accessible via the SDFusion system, and users from other agencies can be added as the system is easily scalable to accommodate future growth. Agencies subscribing to the system can access a wide variety of crime information in a secure fashion with a single sign-on. Users can make a single, federated query when seeking information on a suspect, case, driver's license number or other piece of data. SDFusion quickly checks all the systems connected to it and returns one set of data for the user, which saves a tremendous amount of time.

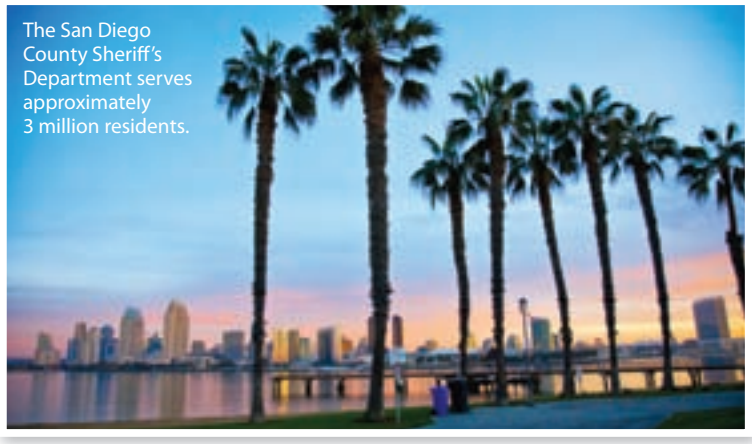
It also puts more data in the hands of public safety personnel. "When you have the ability to access multiple databases, criminal and noncriminal, with a single query, you can get a better picture of who you're dealing with," said Andy Chmielinski, CIO of the Sheriff's Department. "And you know more about the relationships between people. You're able to predict potentially what crimes may take place by an individual or in a particular area. This system is a means to accomplish Sheriff [William] Gore's goals to improve intelligence-led policing."

Several Improvements

Chmielinski also indicated that SDFusion improves officer safety and increases efficiency. Officers in patrol cars, for example, benefit greatly. "They don't have the luxury of time to sit in front of their mobile computer and try to get a better understanding of who they just pulled over. They need an answer now," Chmielinski said. Thanks to SDFusion, officers can retrieve a lot of data before walking up to a vehicle and knocking on the window.

SDFusion also helps investigators working a case. Investigators can cover more ground much more quickly with SDFusion. "They don't have to spend half a day logging into multiple systems and running queries on lots of databases, and then manually attempting to compile all the data and figure out what they have," Chmielinski noted. With SDFusion, users enter a person's name, an address or other data, and the system returns the information related to that entity from all the available databases, in one quick action.

SDFusion is based on several components from Microsoft, including BizTalk Server, the Enterprise Service Bus Toolkit and SQL Server, as well as software from VisionWare, a company based in Glasgow, Scotland. VisionWare's MultiView facilitates an effective search and access to information within disparate systems. MultiView is a rules-based master data management system that further correlates entities establishing "same as" and "probably same as" relationships across all indexed data sources.



The San Diego County Sheriff's Department serves approximately 3 million residents.

SDFusion provides users with greater confidence in the data they receive, since it's an intelligent correlation of all data pulled from numerous sources. The system was built in compliance with national data exchange standards and initiatives. "And for the IT team, it's easier to support and connect to other databases. Those connections can be made much more quickly," said Chmielinski. "Before, contractors would have to do it; it could take months defining what we need, and in the end it would cost us big bucks. We needed the ability to make changes easily and more quickly."

The department worked with Microsoft Services to arrive at the desired solution. "It's a great partnership," Chmielinski said, because the Microsoft Services team understood what the department needed. "We saw how much Microsoft was already doing in the public safety sector," said Chmielinski. "A lot of it is directly applicable to what we're trying to accomplish here."

Microsoft®

For more information, please visit **www. microsoft.com/publicsafety.**

Continued from p. 49

of preparedness. For example, we have initiatives right now on advanced recovery. Instead of just focusing on response, we think about what we can do to accelerate recovery. What actions can we take predisaster that will accelerate recovery?

We have established a lifeline committee to look at interdependencies of our critical lifelines — such as electricity, water, wastewater, communication systems — how they are related, and what things we can do in advance to ensure that we can keep those lifelines operating post-disaster. We have looked at prequalifying contracts so that we have debris removal contracts and other contracts already in place that are needed right after a disaster so that we don't have to go through an RFP process like we did in 2007 for debris removal.

Another area that we are really focused on is integrating the business community. We have a business alliance. We [recently] did a major earthquake tabletop with 160 businesses and we went through azn earthquake scenario for six hours. We also developed a main site where there is two-way communication between the business community and Office of Emergency Services. We found that during the wildfires, individual business was a huge component to the successful response that the county of San Diego had. It was largely an emergent response; it was not orchestrated or preplanned, it was companies like Walmart, Petco and others stepping up and filling in the gaps. We are trying to take advantage of that emergent leadership that we know will occur from the business community and orchestrate it, and provide information that they need to make it even more effective. We are putting a lot of effort in that type of public-private partnership with the business and nonprofits so response can be more orchestrated in a disaster.

Is there anything else you'd like our readers to know?

The only other topic that I see is big in emergency management right now is access of the functional needs and disability community piece that I think is very important. I have been focusing on this since the fires and recognizing how difficult it is to ensure that we are able to provide the kind of response and recovery that we want to the members of the access and functional needs community. I think there is a lot that emergency managers can do in that field, and that is important.

Three areas that are most concerning with access and functional needs is [first] being able to communicate with the disabled, to alert and warn them.

The second is evacuation and having the vehicles to conduct the evacuations, and the third component is sheltering and having a shelter accessible. We have a contract with a company, called Deaf Link, that we send our messages to and in 10 minutes we get back an American Sign Language, Braille and Spanish version that we can provide to the media, as well as on a website to people who sign up to receive our messages in other formats. I think things like that are ways to enhance the communication component.

On the transportation side, the evacuation side, we have agreements with our local Metropolitan Transit and bus services for them to provide handicap accessible buses that we can use during a disaster.

911 Confidential

Dispatchers handle sensitive, confidential information and should be managed as more than just telecommunicators.

By Eric Harne | Contributing Writer

ILLUSTRATION BY TOM McKEITH

In October 2003, Michael Michalski was working as a 911 dispatcher at the Northwest Regional Communications center in Allegheny County, Pa., when his obsession with an ex-girlfriend turned deadly. According to court documents, Michalski used his position to surreptitiously search the center's computer network to determine the whereabouts of Gretchen Ferderbar and her current boyfriend, Mark Phillips. Michalski's supervisor became aware of the searches and suspended him. The suspension, however, was deferred and Michalski remained on the job for another week, continuing his illicit inquiries.

The next week when the suspension took effect, Michalski called the 911 center during the early morning hours seeking assistance in locating Phillips. Two of his co-workers allegedly complied with the request and searched the database. Michalski's supervisor met with him the same day and fired the troubled 21-year-old. Court papers stated that "despite recognizing that Michalski had used the 911 center's computer system to track Mark Phillips, [the supervisor] made no effort to detain Michalski, deter him from reaching Mark Phillips or to warn Mark Phillips of Michalski's potentially violent behavior."

A few hours later, Michalski again contacted his co-workers at the call center. He stated that he "had nothing to live for" and that Ferderbar and Phillips were going to "pay for putting him in his present position." That afternoon Michalski murdered Phillips, Ferderbar and her sister. He pled guilty to the slayings and was sentenced to three life terms.

The Michalski case serves as a cautionary tale about protecting classified data within a public safety environment. Typically the image of a dispatcher is one where an individual sends the fire department, emergency medical services and/or police to an emergency in a timely, efficient manner. This generalization, while not entirely inaccurate, has led to the misnomer "telecommunicator." In reality, dispatchers are information managers who are exposed to highly sensitive data. Criminal histories, terror alerts, Health Insurance Portability and Accountability Act (HIPAA) regulations, and the mundane vacation house check could be misused in the hands of an unscrupulous, desperate or disturbed person. As such, it's imperative that employees understand their obligations regarding the protection and dissemination of information. Furthermore, the call center's management team must be vigilant in identifying abuses and act swiftly to mitigate them.

Background Investigations

No one can deny the importance of a thorough background investigation before hiring an employee at a 911 call center. The selection of trustworthy, competent staff is an integral part of the process.

Pat Shumate, chief communications officer of the Roanoke County, Va., Emergency Communication Center, is ever vigilant in looking for the occasional bad apple.

"Some of the warning signs we find during the background [check] might be a criminal record, bad driving record, bad work history, inconsistencies in the application and poor credit rating," Shumate said. "We look for people who are well thought of in their community with a good employment record and a reputation for honesty."

Problems can arise after the hiring process when successfully vetted individuals later display contempt for the system and then abuse it.

In February 2009, Maury County, Tenn., 911 dispatcher Tamatha Taylor was charged with official misconduct, misuse of official information and accessory after she allegedly tipped off a drug suspect during a police investigation. The suspect was an acquaintance of Taylor's whom she helped elude capture. She had worked at the center since 1994.

A month later in Steuben County, N.Y., 911 dispatcher Jacque Stetler also was charged with official misconduct after allegedly providing sensitive information to an individual about an investigation. Stetler had been employed as a dispatcher for

WHEN THE PUBLIC LOOKS TO YOU FOR SOLUTIONS, WHO DO *YOU* LOOK TO?

Every decision counts when it comes to public safety. That's why our teams are made up of former law enforcement, fire and rescue professionals, and public safety IT experts like Lorne Shackelford, who have extensive experience with precisely the issues you're facing. So if you want options from people who've been there, contact us today.

License Plate Recognition **Mobile and Fixed Video** **Mobile Data Terminals**

BEYOND THE BOX

1.800.INSIGHT ▼ IPS.INSIGHT.COM

Panasonic Toughbook® Arbitrator™ 360º

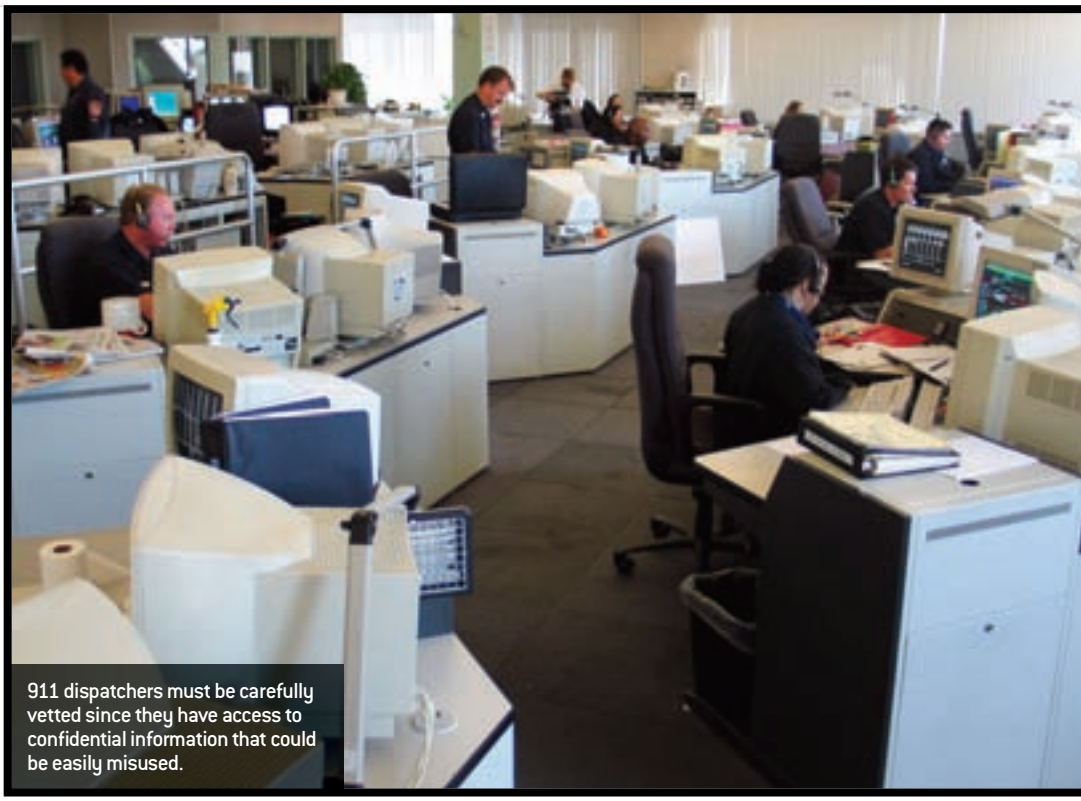
Introducing the groundbreaking Toughbook® Arbitrator 360°, a rugged revolution in law enforcement video capture. The Toughbook Arbitrator 360° is a rugged and durable mobile digital video system that can be used with or without a Toughbook computer. Built with legendary Toughbook reliability, this fully integrated system offers unparalleled video capture (up to 360 degrees), storage and transfer and is designed to work with back-end software for seamless video management, including archiving and retrieving. Capture it all with the Toughbook Arbitrator 360°.

Insight Named Arbitrator Reseller of the Year 2008, 2009

U.S. COMMUNITIES™
GOVERNMENT PURCHASING ALLIANCE

Insight's entire portfolio of public safety products and solutions is available nationally through our U.S. Communities contract. www.ips.insight.com/uscommunities

Insight®
PUBLIC SECTOR



911 dispatchers must be carefully vetted since they have access to confidential information that could be easily misused.

PHOTO COURTESY OF JASON PACK DHS/FEMA NEWS PHOTO

approximately five years. At the time of this writing, Steuben County's 911 website identified Stetler as a recipient of its 2007 Lifesaving Award.

These examples shouldn't be viewed as an indictment of the emergency dispatching profession. They are, however, important to understanding that an employee may change significantly over the course of five years. Drinking, gambling, drug abuse or financial difficulties could compel individuals to commit illegal acts that they would not have considered otherwise. Some might argue that such behavioral changes would have been noticeable in the close quarters environment of a 911 center. Ultimately such abuses may be the result of a lack of vigilance and a failure to address operational issues on a timely basis.

"As a 911 dispatcher, you live in a glass house," Shumate said. "Everyone is watching you, and you must keep yourself above reproach."

Steve Souder, director of the Fairfax County, Va., Department of Public Safety Communications, emphasizes the importance of a half-hour of structured daily roll call before each shift to discuss operational issues. "It is very interactive and a great opportunity to talk about events that have occurred."

Confidential Information Policy

Every 911 center should have a clearly written confidential information policy that employees read, understand and sign annually. The policy must delineate the types of information dispatchers will be exposed to, requirements for protection and restrictions regarding dissemination.

For dispatchers tasked with running database searches for law enforcement personnel, the information gleaned is often highly sensitive. A suspect's criminal history frequently makes for compelling reading and the allure of easy access to such provocative material has led to abuses of the privilege.

It's important to note that the misuse of law enforcement databases is not the line dispatcher's exclusive domain. Sometimes management gets into the act. In October 2008, the Kane County, Ill., State's Attorney's Office issued a press release stating that Steven R. Cordes, director of the northern Kane County dispatch center, was indicted for misusing a criminal background search database. Allegedly "on multiple occasions in 2006, 2007 and 2008, Cordes accessed the state Law Enforcement Agencies Data System to gain information on four persons for his personal use."

Ron Timmons, director of the Plano, Texas, Public Safety Communications Department, cites a department code of ethics that all employees are required to sign as an integral part of the information protection policy. Contained therein is a section stating that employees will not divulge confidential information that's learned during the course of their duties unless such revelation is necessary to perform their jobs.

"We also have specific policies regarding the release of information that would be in violation of HIPAA laws, information obtained through criminal database services and information to the news media," Timmons said.

Dispatcher as Spy?

In May 2008, Nadire Zenelaj, a former 911 operator for Rochester, N.Y., faced felony computer trespassing charges for accessing restricted law enforcement records, including a terrorism watch list. The concern was that Zenelaj, who is a Muslim of Albanian descent, was searching for information on herself, her family and friends.

"We think she was accessing this information to pass it on to others," said Richard Vega, who at the time was the director of the city's Office of Public Integrity. Zenelaj denied the charges, claiming that she was being discriminated against and that she had no terrorist ties. She had been employed by the city for nearly six years.

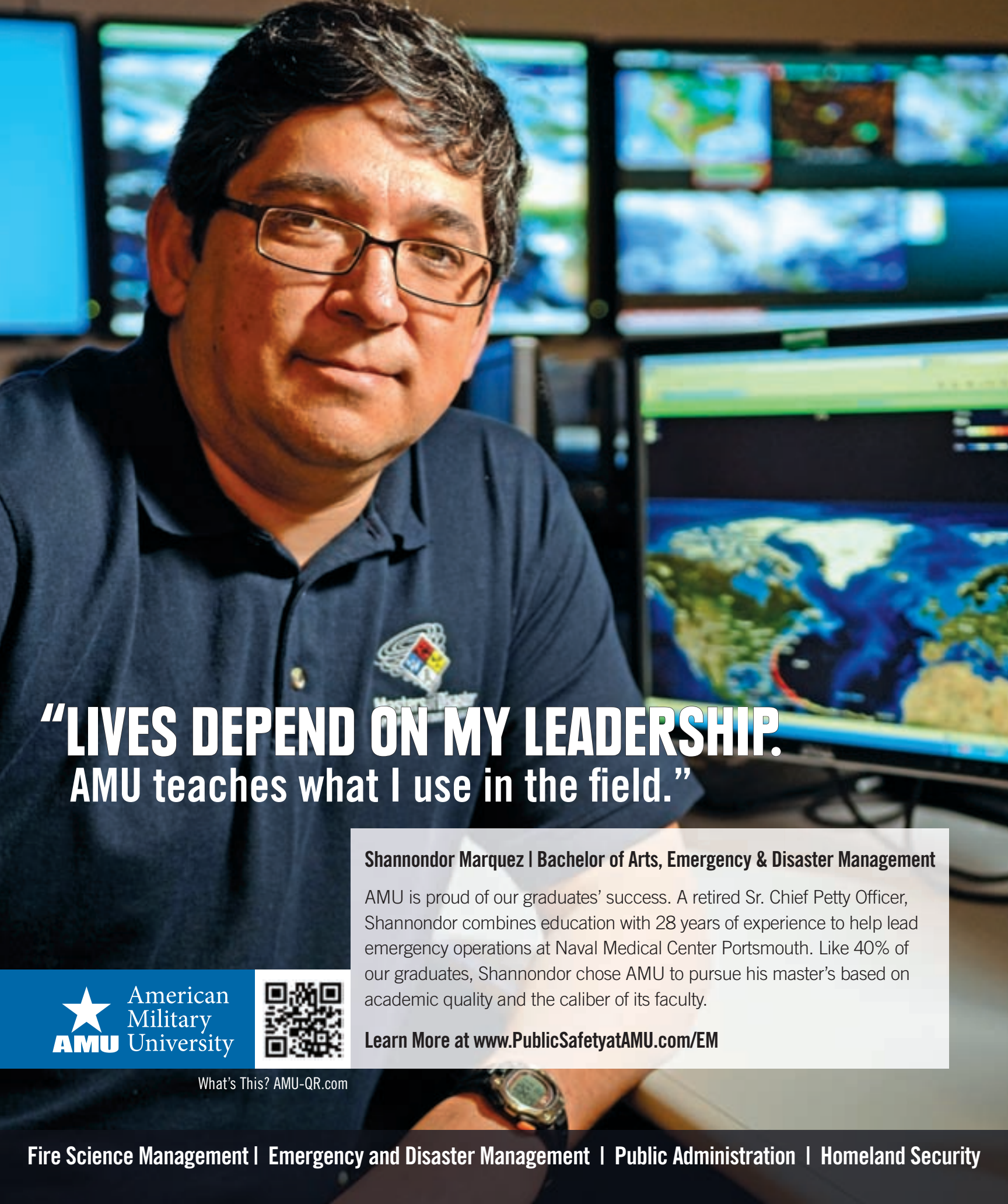
In September 2008, in Orange County, Calif., another 911 dispatcher was charged with providing confidential law enforcement data to a white supremacist group.

Lissa Marie Domanic, who had worked at the Orange County Sheriff's Department since February 2007, had allegedly "supplied members of the gang confidential [Department of Motor Vehicles] information, such as names and addresses and inmate information while she was working for the Sheriff's Department." Part of the investigation focused on whether Domanic had deliberately targeted the Sheriff's Department to penetrate a law enforcement agency.

To vet a possible employee, Plano's Timmons examines an applicant's judgment (or lack thereof) over the last five years. These inquiries include but are not limited to "attendance at social functions at which controlled substances are consumed and such activity is known or should have been known by the applicant; silent acceptance of known illegal conduct by others in his/her presence; workplace behavior/decisions that adversely affect the business or associates, etc."

These incidents are disturbing, and although they rarely occur, they underscore the necessity for protecting confidential information within the dispatching environment. This requires scrutinizing policies, procedures and most importantly, having an effective vetting process for individuals who are charged with an often thankless, unseen job. To do otherwise makes a public safety answering point vulnerable to criminal activity and unwanted public scrutiny.

Eric Harne is a security consultant and writer in Harrisburg, Pa.


"LIVES DEPEND ON MY LEADERSHIP.
AMU teaches what I use in the field."
Shannondor Marquez | Bachelor of Arts, Emergency & Disaster Management
AMU is proud of our graduates' success. A retired Sr. Chief Petty Officer, Shannondor combines education with 28 years of experience to help lead emergency operations at Naval Medical Center Portsmouth. Like 40% of our graduates, Shannondor chose AMU to pursue his master's based on academic quality and the caliber of its faculty.
Learn More at www.PublicSafetyatAMU.com/EM
American Military University
AMU
What's This? AMU-QR.com
Fire Science Management | Emergency and Disaster Management | Public Administration | Homeland Security

Mail Digitization

Electronic scanning can help government agencies identify potentially dangerous mail.

By Jon Love and Bob Ward | Contributing Writers

It's been 15 years since the Unabomber Ted Kaczynski was arrested after a 20-year mail-bombing spree, and 10 years since the anthrax incidents that followed 9/11. But just because mail threats have been out of the media for almost two decades doesn't mean they're no longer an issue. This was made clear recently when a package sent to Maryland Gov. Martin O'Malley ignited in the hands of mailroom employees. No lives were lost, but this security breach is evidence that mail threats are still a real and present danger.

Whether an attack is real, a hoax or an accident, it requires immediate attention. Besides endangering employees, attacks halt the mail stream process, suspend business activities and force buildings to be evacuated, which has a negative effect on productivity, employees and the citizens being served by that government organization. If a biological or chemical hazard is released during mail processing, the cost of cleanup can be astronomical, as witnessed in the anthrax incidents of 2001 and 2002, which cost more to decontaminate the facilities affected than to replace them.

Because mail security breaches can result in severe injury, loss of life and exorbitant cleanup costs, detection and prevention costs should be a priority, even in this time of constrained budgets. Fortunately state and local government agencies can protect themselves from mail threats by employing the latest developments in both detection technology and IT.

ILLUSTRATION BY TOM McKEITH

Detection Through Screening

Depending on the type of threat — chemical, biological, radiological, nuclear or explosive — different levels of screening and technologies are available.

X-ray detectors, like those at airports, are used at many mail screening locations because they are a safe and effective way to screen for explosives.

Software programs and special X-ray scanners use color displays to enhance detection, while other X-ray machines have built-in predictive analytic software that employs pattern algorithms to identify suspect mail pieces.

For radiological and nuclear threats, commercial off-the-shelf detectors are effective at finding materials that are emitting radiological signatures.

Chemicals can be detected by a range of off-the-shelf air-sampling devices. Chemical detectors, along with X-rays, could have intercepted the packages involved in the incidents at O'Malley's office.

Biological agents are the most difficult and time-consuming to handle because of the wide range of potential threats. Although some devices give near real-time readouts, they are

International Association of Chiefs of Police

LEIM 2011

June 13-15, 2011 | San Diego, California

Technology Convergence

Designed by practitioners, for practitioners, the 35th Annual Law Enforcement Information Management Training Conference and Exposition features workshops to enhance the skills, expand the knowledge, broaden the perspective, and support the professional development of law enforcement chiefs, commanders, operational practitioners, and technical support staff.

Plan to attend the 2011 IACP LEIM Conference

- Network with chiefs, command staff, practitioners and technology experts representing all levels of government
- Plenary sessions & focused workshops addressing new & emerging technologies, best practices in policy & practice, strategic planning, project management, performance measurement, social media & law enforcement, predictive policing & technology, cyber crime & digital evidence, communications & interoperability, etc.
- Industry-Leading Solution Providers are featured in the Technology Exposition Hall

Preconference Workshops

- Social Media & Law Enforcement
- Automated License Plate Recognition
- Information Sharing 101: Planning/Operations/Technology

www.theiacp.org/LEIM2011Conference

limited in the number of threats they can accurately examine.

Ultimately there is no panacea for biological threats. External laboratory analysis is generally recommended and employed by government agencies. Each mail item should be opened and examined, often referred to as the "open and extract" approach, in a completely closed environment with controlled airflow and structured filtration. In this negative pressure screening facility, anything released into the air is contained, put through high-efficiency particulate air filtration and removed for analysis. People working in a negative pressure facility should wear personal protective equipment, including a full body suit, gloves, masks, eye protection and a self-contained breathing apparatus.

Ultimate Screening Approach

After the mail is removed from the envelope, it's available for electronic scanning, an additional step in the overall screening process, and the safest and fastest way to deliver mail to the intended recipient.

By converting the mail item from hard copy to an electronic form, the content can be sent to the intended recipient immediately, while the process of physically examining and testing the hard copy for all levels of contaminants can continue, removing the burden of any potential delays.

Through the use of a wide range of properly integrated off-the-shelf technologies, digital mail systems can be seamlessly integrated into an agency's existing IT infrastructure, most notably through the existing e-mail system, or directly into an agency's document management architecture. The digital mail item is also immediately available for a level of processing that's not possible with a hard-copy item. For example, content management software can be used to rapidly identify, extract and distribute the digital mail items to the most appropriate agency sections for immediate action or response. Electronic data extraction of pertinent information, statistics and response tabulations are available.

One of the most important aspects of a digital mail approach is its mobility — recipients can receive their mail anywhere if it's integrated into a secure cloud computing solution. If they have Internet access, they have access to their mail.

Equally important is the way mail-screening technology is deployed. Protecting against mail threats requires that screening and detection solutions are properly placed in the overall mail handling process. For example, it's best to screen mail at an off-site location. Then if there's a threat, only the mail processing facility is shut down, not the actual governmental function. If the governmental function is shut down, a digital mail solution will ensure that the flow of communications continues.

Jon Love is president and **Bob Ward** is director of applied technology of Pitney Bowes Government Solutions.

Advertisers Index *

EMERGENCY MANAGEMENT

All Hazards/ Stakeholders SUMMITS 2011

We Can't Predict. But *We Can* Be Prepared.

These must-attend events are an opportunity to enhance your professional knowledge, build interagency relationships and exchange industry best practices to support regional preparation and response to all types of catastrophic events.

Located in the heart of your jurisdiction, registration is complimentary to public sector professionals!

Learn about registration and sponsorship at:
emergencymgmt.com/summits

EMERGENCY MANAGEMENT

Seattle
March 3

San Francisco
April 26

Washington D.C.
May 10

New York City
May 12

Philadelphia
June 9

San Diego
July 7

Boston
August 3

Denver
September 13

Phoenix
September 15

Los Angeles
November 2

Miami
December 6

Houston
December 8




CONGRATULATIONS!

IN TIMES OF CRISIS YOU:

Positively affect someone's life

★

Go above and beyond to protect your community

★

Inspire with a career devoted to saving others

NOW YOU'VE BEEN CHOSEN

sponsored by Sprint

Find out who ***YOU*** are in Sprint's resource center at:

emergencymgmt.com

PHOTO COURTESY OF WWW.ISATSB.COM

ISAT Seismic Bracing is retrofitting the Redwood Memorial Hospital.

By Corey McKenna | Staff Writer

On Shaky Ground

Despite California's stalled plans for an online tracking system for hospital seismic retrofitting, 80 percent of hospitals are said to be on schedule.

On Feb. 9, 1971, a magnitude 6.6 earthquake shook Southern California's San Fernando Valley, killing 65 people and seriously injuring 2,000. Because most of the deaths occurred in a veterans' hospital, the state Legislature in 1973 passed the Alfred E. Alquist Hospital Facilities Seismic Safety Act, requiring all acute care hospitals at risk of collapse be retrofitted to withstand an earthquake.

Eleven years later, following the 1994 Northridge earthquake, the Legislature passed two bills that strengthened the act's requirements and set deadlines to meet them. Hospitals must determine which buildings are at risk of collapse during a major earthquake (with a magnitude of 7 or greater) and therefore must be seismically retrofitted to remain standing during and after a temblor by 2013. By 2030, they must be seismically retrofit to be able to remain operational immediately following an earthquake.

Even with deadlines in place and standards being set, several obstacles remain — including the high costs of new hospital construction and the lack of funding and financial incentives for the hospitals to complete the work. To keep track of progress, California passed a law in 2009 requiring hospitals with acute care facilities in buildings that face a high risk of collapse during an earthquake to report their progress and expected timeline for completion during a one-year time span.

In November 2009, the Office of Statewide Health Planning and Development (OSHPD) awarded a contract to Accela to build the foundation of a new system that would replace the agency's mix of paper and electronic processes for tracking hospital construction projects. The move was intended to improve accountability of both the OSHPD and hospitals' design teams and to help projects move through the approval process.

Meeting Deadlines

Reports showed that 80 percent of hospitals are on track to be retrofitted by 2015. According to data posted on the OSHPD site, 129 hospitals with 403 buildings will meet the state's hospital seismic requirement by January 2013. Another 55 hospitals with 153 buildings will be compliant by 2015.

The remaining 20 percent plan to complete seismic retrofitting by Jan. 1, 2020, though not every facility that's planning compliance after 2015 has been verified as eligible for such an extension, said OSHPD spokesman David Byrnes.

While the California Hospital Association (CHA) supports the goal of seismically safe hospitals, it notes that the challenge has been to carry out and finance the required retrofitting in a way that doesn't jeopardize patients' access to care.

"A number of hospitals will not be able to comply with the seismic deadlines for financial, scheduling

or other practical reasons," said CHA President and CEO C. Duane Dauner in a statement. "It is essential that lawmakers and hospital officials work collaboratively to address these barriers and keep hospitals open for patients."

One obvious barrier is cost. The cost of making these seismic improvements ranges from $45 billion to $110 billion, according to a 2007 study by the Rand Corp. And financing could double the cost. Complying by 2030 with the mandate that acute care hospitals remain operational following an earthquake could add 20 percent to construction costs.

The CHA plans to sponsor legislation this year to help the remaining hospitals comply with the mandate, said spokeswoman Jan Emerson-Shea. Details of what the legislation is expected to look like will follow additional analysis of the information reported.

Tracking System

A new Web-based system may improve the accountability of the OSHPD and hospital design teams by tracking hospital construction projects. Once fully implemented — expected in January 2012 — the Facilities Development Division (FDD) will use the e-Services Portal to track health-facility plans, reviews and construction, facilitate inspections and certifications, and ensure compliance with state-mandated seismic safety standards.

> "A number of hospitals will not be able to comply with the seismic deadlines for financial, scheduling or other practical reasons. It is essential that lawmakers and hospital officials work collaboratively to address these barriers and keep hospitals open for patients."
>
> **C. Duane Dauner,** president, California Hospital Association

"New programs, as well as changes to existing ones made by changes in the Hospital Seismic Safety Act, would require a substantial investment for reprogramming and modifying an archaic program that was on the verge of becoming unstable," Byrnes said. The current tracking system, Logbook, was created in the early '90s and allows for limited electronic plan submission and review, letting users check the status of projects, but it doesn't provide any analytical capabilities.

According to the OSHPD, the number of projects under review by the FDD has increased substantially since the original system was implemented. Also, the estimated cost of projects under review by the agency has grown from $2 billion to $23 billion annually, prompting the office to replace the system.

The new portal was originally scheduled to go live in summer 2010, but California's budget difficulties have pushed development back to April 2011, meaning citizen access and the system's wireless components for field staff are scheduled for deployment by July 2011.

Going Forward

Even with 80 percent of hospital buildings reportedly on track to meet 2015 seismic safety construction deadlines, hospitals question how to fund the projects with their slim operating margins, which averaged less than 4.5 percent between 2004 and 2008, the OSHPD reported in testimony before a 2010 state Senate health committee hearing on seismic safety of hospitals.

Before the same committee, Mike Boyd, executive director of facilities, planning, design and construction at the University of California, Davis, Sacramento campus, testified that the university system expected to invest $2.75 billion by 2011 in hospital construction projects, which was partially prompted by seismic safety mandates. Of the total investment, 77 percent came from bonds and long-term debt, and 19 percent came from a FEMA grant.

In Los Angeles, the county's Department of Health Services is on schedule and within budget to complete seismic retrofitting projects at five hospitals it oversees using bond capacity already approved by voters, said John Shubin, the department's director of capital projects. The increased time frames to get approval on projects from the OSHPD, he said, have been built into project schedules and budgets.

And following the new Logbook's implementation, the OSHPD expects to roll out a Plan Review Report Card section of its e-Services Portal, though the timing hasn't been determined. "Because of resource constraints during the past two years," Byrnes said, "FDD has put this project on hold and does not currently have an estimated time frame for its reactivation."

When implemented, the report card would track: the amount of time that planning documents have stayed with the FDD and hospital design teams; the number of back-checks for a project; the length of the time it took for a plan to be approved from start to finish; and if any of these factors were above or below average.

"For those projects that perform below average, the hospital owner may wish to consider steps to improve project performance in the future," Byrnes said. "This may result in selecting a different design team, providing the design team with a better defined program and/or performance expectations, more direct involvement by hospitals' owners to assure better outcomes for their projects, etc."

MONEY MATTERS

The cost of making seismic improvements to California hospitals ranges from **$45 billion to $110 billion**, according to a 2007 study by the Rand Corp. And financing could double the cost. Complying by 2030 with the mandate that acute care hospitals remain operational following an earthquake could add 20 percent to construction costs.

Know the Situation

In an emergency, you need to understand what's happening now and what could happen next in order to make the best decisions. Esri® Technology provides you with comprehensive situational awareness and actionable intelligence when you need it most.

Learn more at esri.com/emmag

esri®

Securing Mobile Devices

AirWatch can secure, monitor, manage and support an enterprise's fleet of mobile devices, regardless of device type, manufacturer or location. The most recent release, AirWatch 5.13, secures mobile device deployments through its enhanced public key infrastructure integration and certificate management framework, making it easier to generate and manage certificates on mobile devices for authentication and encryption. After authenticating a mobile device user, AirWatch generates the necessary certificates for the device, speeding the overall mobile device deployment process. www.air-watch.com

Remote Power

The PRO-Cell remote power system delivers continuous power for mission-critical energy applications without relying on the power grid. Sirius Integrator and Solar Stik teamed to offer PRO-Cell, available in three models, with charging capacity ranging from 600 to 2,200 watt hours per day. The models can be employed in any application where a 12-volt DC or 24-volt DC battery system is utilized. PRO-Cells can be used as the primary method of providing power for small loads, but they can also help mitigate against failure when a solar array or wind-generator is the primary means of producing power. www.siriusintegrator.com

On the Go

The Mesa Geo 3G Rugged Notepad provides Bluetooth wireless technology, Wi-Fi, GPS and a digital camera, in addition to a 3G GSM cellular data modem that provides real-time wireless connectivity while working in the field. Juniper Systems' rugged notepad is built to IP67 standards, making it waterproof and dustproof, and tested to MIL-STD-810G standards for water, humidity, sand, dust, vibration, altitude, shock and temperature. Its rugged magnesium and plastic chassis protects the Mesa from drops of up to four feet onto concrete. Features include user-defined shortcuts and 11 screen gadgets for controlling wireless connections, GPS, texting, e-mail, calendar and power functions.
www.junipersys.com

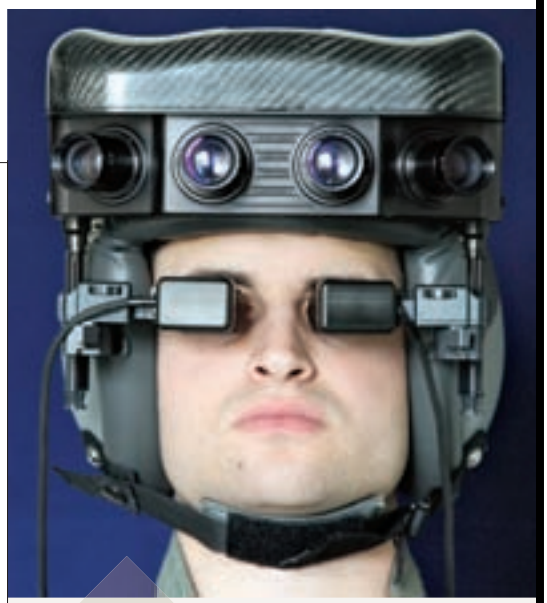
Surveillance System

SightLogix's Rapid Deployment Kit is an intelligent video system designed for outdoor surveillance of critical assets and remote locations. The system enables users to set up and deploy reliable video surveillance quickly and easily at high-risk mobile or short-term venues and events. Packaged in a portable case, each kit includes: one or more SightSensors, or video detection cameras; a ruggedized laptop with SightMonitor software; camera tripod(s); and network video recorder software. www.sightlogix.com

Bright Idea

The new SmithLight IN120LB battery-operated LED work light is a highly durable, bright and versatile lighting solution. ProBuilt Professional Lighting's self-contained system incorporates a sealed battery that operates up to 30 hours on a single charge and can be recharged with either a vehicle or wall adapter. The durable materials are fully weatherproof and dustproof so the light can withstand tough environments.

www.probuiltlighting.com



Night Flight

The High Resolution Night Vision System developed by SA Photonics is a head-mounted display for use by commercial and military pilots of fixed-wing airplanes and rotorcraft. The system was developed in partnership with the Air Force Research Laboratory, the Army's Night Vision Laboratory and Vision Systems International. Benefits include reduced peripheral obscurity, reduced forward projection, zero-halo, and the capabilities for digital image enhancement and recording night vision imagery.

www.saphotonics.com

Flexible Infrastructure

Meridian Technologies' new DigiNET Ethernet signal transport product includes media converters, managed and unmanaged switches, POE switches and SFP optical devices for additional system infrastructure flexibility. The products are hardened to ensure operation under demanding environmental conditions.

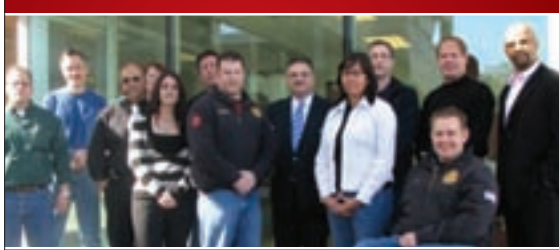
www.meridian-tech.com

Alumni Profile

UNLV Executive Master of Science Degree
In Crises and Emergency Management ECEM

Overview

The University of Nevada, Las Vegas (UNLV) Department of Public Administration is offering the Executive Master of Science Degree In Crises and Emergency Management (ECEM). As a result of national, state, and local experiences such as September 11, 2001, Hurricanes Katrina and Rita in 2005, the United States must come to grips with topics such as government responsibility and accountability, coordinated response and recovery, and citizen awareness and preparedness. UNLV recognizes the continuing need for experienced leaders who can provide direction for our nation in times of great challenge and it is proud to offer the ECEM degree which began in 2003.



This is the 2008 graduating class for ECEM which includes, Richard Wells (Director of GIS at City of Las Vegas), Jim Lopey (Deputy Sheriff of Washoe County), Marc Glasser (Federal Agent), Dustin Olson (Deputy Police Chief for UNLV), Christopher Sproule (Fire Fighter for City of Las Vegas), Stephen Gay (Engineer for North Las Vegas), Kim Ferguson (Director of Emergency Management at Nevada Energy), Monique Sanchez (Los Alamos Labs), Ernest Chambers (Las Vegas Metro), Elliot Jones (City of Las Vegas Fire Fighter) and one faculty member s (Dr. Paul Davis) and a guest lecturer (Dr Wade Ishimoto).

UNLV ECEM Program
4505 Maryland Parkway
Box 456026
Las Vegas, NV 89154

(702) 895-2640

http://sepa.unlv.edu/programs/ecem

UNLV
UNIVERSITY OF NEVADA LAS VEGAS

Tossing the Three-Day Rule

By Eric Holdeman

I've always been a strong supporter of disaster public education. My first exposure to it was in 1992 when I worked at the Washington state Emergency Management Division and was responsible for starting the state's first public education program.

When I moved to the county level as a local director, I made sure we had an active disaster education program. After 9/11, the homeland security grants that followed provided an opportunity to fund a much more robust regional public education program. We formed a regional group to select a campaign slogan, 3 Days, 3 Ways, and then promoted it using a variety of mass media that included TV, radio, billboards and bus signs. We even partnered with the Seattle Mariners for stadium signage. Then Hurricane Katrina hit and it was clear that telling people to be prepared for just three days was not enough. The challenge was that the national message coming from FEMA and the American Red Cross had always been three days of preparedness. I called people I knew at the national offices of both organizations to see if they were considering changing their message. They said no.

To maintain a message consistent with national standards, we modified our materials to warn people to prepare for a minimum of three days.

Now we have another catastrophe in Japan, an industrialized and modern nation with the world's third largest economy. Japan is touted as the most prepared country in the world. When you observe the damages there and think about the types of mega-disasters that are possible in the U.S., it's easy to see why it's time to toss the three-day message and level with our communities. People need to be prepared to be self-sufficient for at least a week.

There are several reasons to make this switch.

We need to be honest with people and manage their expectations. If we tell them three days, we should be prepared to respond to their needs at the end of that time. For catastrophes, it is not a good planning assumption that we will be able to respond to individuals within three days.

The military's planning figure is to be on the ground by 100 hours after the event. If you look at previous responses, it takes a long time to get personnel and equipment in place and to the point where they can make a significant difference.

Disaster response is all about logistics and moving supplies and equipment. This is not a simple task, especially when transportation systems have been impacted. As one speaker so eloquently stated, "Logistics — if it were easy it would be called taxes."

For catastrophes, it is not a good planning assumption that we will be able to respond to individuals within three days.

I don't expect that the aforementioned national programs will change their disaster preparedness messaging. That does not compel us to make the same mistake. It's time to come clean and be real with our constituents. One of my mantras is, "Don't promise what you can't deliver." When it comes to disaster preparedness, slogans might best be stated as: You're on your own for a week, baby!

While I really liked the 3 Days, 3 Ways message, the problem is that it's not realistic and just plain not true.

Eric Holdeman is the former director of the King County, Wash., Office of Emergency Management. His blog is located at **www.disaster-zone.com**.

CAE **VICTOR**

In today's homeland security and emergency management environment, no force responds alone. Whether the response involves just local responders or an integrated state, national, joint or multi-agency response, participating organizations need to effectively share information, collaborate, and interoperate. Multi-agency collaboration has long been challenged by the inability to engage all players to plan, test, and train together. Traditionally, table-top and live exercises have been used to train responders. However, table-top exercises lack realism resulting in less effective participation.

To address these issues, CAE has developed CAE **VICTOR**, virtual incident command for training and operations research. CAE **VICTOR** is a constructive simulation that is capable of supporting both civil and military operations, spanning all aspects of emergency and homeland security operations. The dual use of the simulation tool allows for local, state, national, and multi-agency responders to effectively exercise response plans, conduct threat analyses, and develop best practices for all-hazard events.

As a web-enabled solution, **VICTOR** provides variable level views of all-agency, all-hazard response operations and is a dynamic simulation environment for multi-agency planning, analysis, and training.

The complete solution. CAE **VICTOR** is a complete constructive simulation solution for multi-level training of emergency management personnel. **VICTOR** is a lightweight yet powerful simulation engine. Thousands of autonomous units can be simulated on a single laptop or workstation, including asymmetric threats, weather obstacles, and urban populations.

Scalable to large-scale exercises. CAE **VICTOR** can be used to support small and large-scale exercises using doctrine-compliant intelligent automation to enhance exercise realism and to reduce the need for the number of humans in the loop required to control the movements and behaviors of computer generated forces (CGF).

Manage scenarios. The master event scenario list (MESL) integration within CAE **VICTOR** is accomplished through timeline scripts. These scripts allow the exercise controller to stimulate changes in the situation across the mission, hazard, teams, enemy, terrain, time, and other constraints. These changes can incorporate changes to cultural, political, and socio-economic conditions. These conditions are synchronized and triggered by scenario behaviors and respond to the tactical situation.

CAE VICTOR Supports

- Integration with Common Operating Picture
- Running Simulation Faster than Real-time
- Dynamic Artificial Intelligence
- Integrated After Action Review

For more information go to **http://victor.cae.com**

CAE

one step ahead

A Safer America

By Paul Wormeli and Steven G. Mednick

Homeland Security Secretary Janet Napolitano recently warned Congress that "the terrorist threat … has evolved significantly." Citing an increase in extremists within our borders and the "lone wolf" operators, she pointed out that there is clearly a need for vigilance.

One of the new tools for reporting and analyzing potential threats is the Nationwide Suspicious Activity Reporting Initiative (NSI). This new program builds on what law enforcement and other public safety agencies have been doing for years — gathering information about behaviors and incidents associated with criminal activity. The NSI establishes a standardized process whereby relevant information can be shared among agencies to help detect and prevent terrorism-related activity.

The NSI has faced criticism by various news outlets, including *The Washington Post*, which recently depicted the initiative as an unregulated and undisciplined foray into a world too sophisticated for state and local law enforcement officials.

The truth is that a single observation or report that might not seem significant may, when blended with other actions, materialize as a composite pointing to possible criminal or terrorist activity. When the Department of Justice established an NSI Program Management Office to facilitate the implementation of the initiative across all levels of government, it had two missions: to foster broader sharing of information concerning suspicious activities and to protect and defend privacy, civil rights and civil liberties. The record attests to its success. America is safer, and in three years not a single case has been brought alleging a violation of civil rights.

The NSI is designed to collect data on suspicious acts and behaviors that may have a nexus to criminal or terrorist activity — behaviors, not individuals. A massive training program is under way to acquaint local police with privacy principles and the proper collection of information about suspicious activity as part of a disciplined national system where data is managed and shared among state fusion centers.

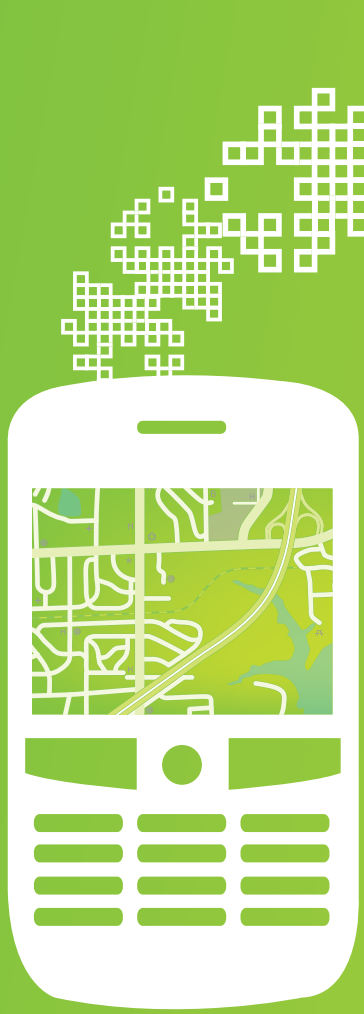
Data collected within the NSI is controlled by the state fusion centers. Access to this distributed system is constricted by a secure portal to preserve privacy and civil rights protections and honor each state's statutory privacy policies. Fusion centers can't participate in the program or have access to data from other centers without first adopting a privacy plan approved by the departments of Justice and Homeland Security.

In 2008-2009, the presidentially appointed program manager for the Information Sharing Environment evaluated the NSI program and concluded that the unified process not only enhanced counterterrorism efforts, but also strengthened privacy, civil rights and civil liberties protections. Today the NSI is one of the nation's most significant accomplishments in counterterrorism efforts and information sharing: an interrelated set of harmonized policies, processes and systems to empower the men and women on the front lines to access and share the information they need to keep the country safe.

There should be no debate about the concerns (shared by public officials, law enforcement and civil libertarians) that there is a need for thoughtful coordination and oversight over programs such as the NSI. A major step forward would be eradication of the stovepipe culture that permeates so much of the thinking in Congress, sectors of the executive branch and the fourth estate.

It could well be that the next attack against a major city will be launched from the suburbs. To be prepared or perhaps to prevent such acts, we need a plan of defense at all government levels. It is clear from the available data that an effective NSI will make us safer. Thoughtful leadership can balance the mission of preventing terrorist acts and advancing national security with the utmost respect for that most fundamental right, personal privacy.

Paul Wormeli and **Steven G. Mednick** are the executive director emeritus and general counsel, respectively, of the IJIS Institute, a nonprofit organization that brings together industry and government to improve national security and promote information sharing. This article represents their personal views.



Better serve your *community*

from more places in the community.

Equip your employees with AT&T's suite of Mobility Solutions for Government. AT&T can help your government agency be even more productive and efficient. Our apps can speed deployment and tracking of emergency response crews. Give inspectors location-specific information before appointments. Provide social workers access to case files from the field. All on the nation's fastest mobile broadband network.

See what our government solutions team can do for your agency at att.com/MobileGOVT

Rethink Possible℠

AT&T's mobile broadband network is not available in all areas.

From the battlefield, To the city streets. Trust Harris.

Around the world, soldiers depend on Harris to deliver secure battlefield communications. We bring that same capability to those who serve on our city streets and rural highways. From P25 multiband radios to secure Internet Protocol critical communications networks, Harris delivers the technology and solutions to keep first responders connected.

Communications you can depend on…
on the battlefield and at home.

harris.com

HARRIS®
assuredcommunications®