

## Communicating & Planning Before, During, and After a Disaster



### *Before Disaster Strikes*

**Five Preparedness Measures  
Every Community Should Know**

By Andrew Sachs, Viewpoint

**The Public Health Role  
During Mass-Fatality Incidents**

By Raphael Barishansky & Audrey Mazurek, Public Health

### *The Joplin Tornado*

**45 Seconds of Danger, a Lifetime of Lessons**

By Craig DeAtley, Health Systems

**Public Health and  
Medical Interoperability Challenges**

By Bruce Clements, Public Health

**NLE 2011: Successful Learning,  
Plus Partnership Building**

By Kay C. Goss, CEM, Emergency Management

**Man-Caused Incidents -  
New Challenges & Systems**

By Steve Grainer, Fire/HazMat

**Antidotes: The Care & Cure for "What Ails You"**

By Joseph Cahill, EMS

**The New PLAN:  
Government Alerts Enter 21<sup>st</sup> Century**

By Rodrigo (Roddy) Moscoso, Law Enforcement

**Manmade Disasters and Interoperability**

By Omar Alkhalaf, Emergency Management

**Changing Trends in Maritime  
Piracy Represent a New Threat**

By Michael S. Brewer & Scott Brewer, Transportation

**California, Nevada, Texas, and New Jersey**

By Adam McLaughlin, State Homeland News



**FIRST RESPONDERS NEED TO BE  
PREPARED FOR ANYTHING...**



For expert and informed discussion on  
how to face your CBRN threat contact:

USA Tel: +1 540 604 4478

Email: [frontline@remploy.com](mailto:frontline@remploy.com)

UK Tel: +44 (0)845 241 2990

Email: [frontline@remploy.co.uk](mailto:frontline@remploy.co.uk)

[www.remplayfrontline.com](http://www.remplayfrontline.com)

**SO DO OUR SUITS**

**Remploy** Frontline

SURVIVAL EVOLUTION



## Editor's Notes

By James D. Hessman, Editor in Chief



Advance planning, astonishing technological breakthroughs, interoperable communications, and many other topics of compelling interest to emergency managers and first responders alike are addressed in considerable detail in this month's issue of *DPJ*. There also are several "lessons learned" discussed – one of them not quite two centuries old – along with a brief mention of a bomb-sniffing dog.

Plus: (a) Some helpful and much needed advice about legal ramifications and financial reimbursement; (b) A report on the "total devastation" of the Saint John's Regional Medical Center in Joplin, Missouri – and the heroism of the hospital staff and other citizens of that fine city during and after the tornado that struck without warning on 22 May; and (c) the much under-publicized marriage of convenience between Somalia-based pirates and several major terrorist groups that, without exaggeration, could become the greatest danger facing the entire world since the Spanish Flu pandemic of 1918-20.

Andrew Sachs leads off with a helpful list of what U.S. cities and states must and should do – well in advance, and in considerable detail – to protect themselves, their citizens, and their treasuries from the physical and fiscal havoc caused by any unforeseen disaster, natural or manmade. Raphael Barishansky and Audrey Mazurek follow up with incisive insights about the need to preserve evidence, work with grieving families, handle decedent remains, and deal with the multitude of other tasks, major and minor, required after any mass-fatality incident. Craig DeAtley rounds up the opening trilogy with an illuminating and sometimes inspiring report on the Joplin response.

The specifics of the piracy/terrorism merger mentioned earlier are spelled out by Michael S. Brewer and Scott Brewer in a chilling report on "Maritime Piracy and Terrorism" that should be required reading for all U.S. decision makers, on Capitol Hill and in the White House, for their counterparts in other nations of the Free World, and for anyone else who does not yet understand the meaning of the term "clear and present danger."

Not all is gloom and doom, though. Bruce Clements focuses on several steps forward that have increased the emergency readiness and operational capabilities of states, individual communities, and the nation as a whole in dealing with any type of disaster, with or without warning. Kay Goss adds a bullish report on the highly successful "Great Central U.S. ShakeOut" – modeled, of course, on the New Madrid Earthquake of 1811. And Steve Grainer provides a helpful tutorial on the growing importance of the "I&I" (Intelligence & Investigations) aspects of a comprehensive disaster-preparedness plan.

Also included in this month's printable issue are: 1. A "how to" plan, by Joseph Cahill, to ensure the safe storage and distribution of medical antidotes. 2. An update by Rodrigo Moscoso on the significantly improved Public Localized Alert Network communications system. 3. An encouraging report, by Omar Alkhalaf, on how Northern Illinois University used the interoperability lessons learned from the London subway bombings and Rhode Island nightclub fire to upgrade its own communications system – and thereby save the lives of an untold number of students as well as faculty members. As always, Adam McLaughlin rounds out the issue with timely reports on recent news items – this month, from the great states of California, Nevada, New Jersey, and Texas.

*About the Cover: Catastrophic damage resulted from the deadly storm and tornado that struck Concord, Alabama, in April 2011. Individual Assistance funds available from the Federal Emergency Management Agency (FEMA) may be used to help eligible storm survivors who are now homeless pay for temporary housing; in addition, FEMA's Public Assistance funds may be allocated to help reimburse the hard-hit community for the cost of its power-restoration and road-repair recovery expenses. (FEMA photo by George Armstrong)*

### Business Office

517 Benfield Road, Suite 303  
Severna Park, MD 21146 USA  
www.DomesticPreparedness.com  
(410) 518-6900

### Staff

Martin Masiuk  
Publisher  
mmasiuk@domprep.com

James D. Hessman  
Editor in Chief  
JamesD@domprep.com

John Morton  
Strategic Advisor  
jmorton@domprep.com

Susan Collins  
Creative Director  
scollins@domprep.com

Catherine Feinman  
Customer Service Representative  
cfeinman@domprep.com

Carole Parker  
Database Manager  
cparker@domprep.com

### Advertisers in This Issue:

AVON Protection

Bruker Detection

Envionics

FLIR Systems Inc.

FRI (Fire Rescue International) 2011

Idaho Technology Inc.

PROENGINE Inc.

Remploy Frontline

Upp Technology Inc.

© Copyright 2011, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

DomPrep Journal is electronically delivered by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; fax: 410-518-6020; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for its use or interpretation.



# Remote **BIOHAZARD** Detection

## **MAB** Portable Biological Alarm Monitor

Our MAB Portable Biohazard Detection System sends an alarm immediately upon detecting any evolution to the atmospheric background. It works on a continuous real-time basis and responds in only seconds. Easily used by untrained people, it has a very low power consumption rate and is especially designed for harsh environments.

MAB has a fast start-up time and can quickly analyze atmospheric particles for chemical signatures of bacteria or toxins such as anthrax, plague, Botox, legionella, etc.

MAB has already been selected by several military forces and is used by several NBC reconnaissance vehicles, as it is not sensitive to diesel vapors and smokes. Test reports are available.



### Characteristics

- Size of the box (LxWxH): 300mm x 160mm x 470mm (11.8" x 6.3" x 18.5")
- Total height: 850mm (33.5")
- Weight: 14 kg (31 lbs)
- Operating temperature: -10°C to +50°C (14°F to +122°F)
- Storage temperature: -39°C to +71°C (-38.2°F to +160°F)
- Autonomy: 10 days (refillable hydrogen cylinder included)
- Power supply: 12 - 32 V DC / 110 - 220 V AC
- Can be remote controlled
- Remote data by RS 485 outlet
- Response time: less than 1 minute
- Field tested / Report available



## Contributors

### First Responders

Kay Goss  
Emergency Management

Joseph Cahill  
EMS

Glen Rudner  
Fire/HazMat

Steven Grainer  
Fire/HazMat

Joseph Trindal  
Law Enforcement

Rodrigo (Roddy) Moscoso  
Law Enforcement

Richard Schoeberl  
Law Enforcement

### Medical Response

Michael Allswede  
Public Health

Raphael Barishansky  
Public Health

Bruce Clements  
Public Health

Craig DeAtley  
Public Health

Theodore (Ted) Tully  
Health Systems

### Government

Corey Ranslem  
Coast Guard

Dennis Schrader  
DRS International LLC

Adam McLaughlin  
State Homeland News

### Infrastructure

Neil Livingstone  
ExecutiveAction

### Industry

Diana Hopkins  
Standards

## Before Disaster Strikes

# Five Preparedness Measures Every Community Should Know

*By Andrew Sachs, Viewpoint*

Preparedness matters. However, many communities get themselves and their citizens ready for a disaster mostly in terms of bottled water and shelter. What many communities do not even think about – until a disaster strikes and they are still mounting a response – are the administrative components that will make or break their recovery. In an effort to expedite a successful recovery from unforeseen incidents, every community should institute the following essential steps required for a successful plan of action:

### **1. Augment the Emergency Management Staff**

Disasters require flexibility to meet unexpected and added workload; therefore, having access to knowledgeable people to assist becomes vital. Volunteer assistance and mutual-aid agreements serve as cost-effective short-term solutions; however, expert consultant support – from disaster-recovery experts – offers longer-term assistance as well as expertise that may not be available locally. If and when using outside staff support, consider building them into pre-disaster training and exercise programs to allow them to integrate seamlessly if and when the need arises.

Disaster recovery is a marathon, not a sprint. Few if any U.S. communities have enough full-time employees necessary to manage the community while also conducting a full-court press on disaster response and long-term recovery operations. Being prepared means having planned for this eventuality.

### **2. Have No-Cost Pre-Event Contracts in Place**

Having pre-event contracts in place with vendors who offer services that will more than likely be needed in the aftermath of a crisis is one of the most important administrative actions a community can take before disaster strikes. Such services include, but are not limited to, the following: augmentation of the Emergency Operations Center staff; debris management and monitoring; engineering and evaluation; and the use of federal disaster program management services.

A pre-event contract is usually available at no cost to the community, and can be activated immediately following a disaster so that there is no lag time in bidding; in addition, more competitive pricing is assured. Pre-event contracting also provides the time needed to find the capable and qualified contractors available to meet the needs of the community – without the pressure of having to concurrently manage a disaster response. Key qualified contractors will possess a broad range of disaster experience, be able to provide references, and will have the expertise needed to work effectively on various federal programs – most importantly, those under the jurisdiction of the Federal Emergency Management Agency (FEMA) – so as to help maximize not only eligibility requirements but also the reimbursement for costs.



Having pre-event contracts in place can dramatically affect, and improve, a community's bottom line. Having expertise on hand is particularly important to advise a community on how to: (a) increase the ability for reimbursement; (b) help the community maximize the disaster assistance available; and (c) avoid major problems that might delay or make a project ineligible for reimbursement. Moreover, pre-event contracts for equipment and services often are more affordable – because they are bid during “peace time” when competition for limited resources has not led to higher prices. Taking the time needed to put pre-event contracts in place also reduces the likelihood of mistakes being made during procurement that not only could lead to significant delays but also to the reduction, or even elimination, of the community's ability to obtain reimbursement altogether.

After a contractor has been secured under a pre-event contract, the community should use the advance time needed to: (a) build a working relationship and train the augmented staff, along with key players; (b) get them better acquainted with one another; (c) help them understand each other's needs; and (d) have common expectations for service delivery.

### **3. Review and Assess the Emergency Authorities**

Disasters make time a very valuable commodity, and the usual “day-to-day” policies and procedures usually do not allow for the urgent, usually immediate, actions required in sufficient time to meet disaster-related needs. The pre-event environment is the best time to review and assess the authorities a community already has, keeping in mind the challenges those authorities may well be facing during a recovery operation.

Communities also need to be thoroughly familiar with the emergency authorities available, and to understand how those authorities will support not only immediate but also long-term recovery needs. To achieve that understanding, several important questions must be addressed – including the following:

- (a) Do the City Charter and/or community by-laws provide a clear chain of authority and ensure the continuity of government?
- (b) Are emergency procurement authorities consistent with both federal and state requirements?
- (c) Do those authorities also provide the ability needed to loosen requirements for building permits to allow for a more rapid recovery?



- (d) Do the emergency provisions address how code enforcement may be accomplished under the crush of disaster reconstruction?

If such a review has not been conducted, guidance can be provided through the state Emergency Management Office – or the community can secure non-governmental professional assistance.

### **4. Maximize Public Infrastructure Grants**

Many communities do not possess much and/or extensive disaster experience, and are therefore unaware of what they are specifically entitled to when FEMA arrives. To help speed up the recovery process, it is particularly important that communities not only are aware of FEMA regulations, and how they have been applied elsewhere around the country, but also how to document costs to justify federal reimbursement.

The Stafford Act, also known as the Disaster Relief and Emergency Assistance Act, provides the guiding legal authority for FEMA recovery programs and is reasonably flexible in meeting the unique needs of communities that arise during a disaster. This flexibility often results, though, in FEMA decisions lacking consistency from one applicant to another, so it is imperative that communities understand not only past precedents but also where some flexibility is available to maximize their eligibility.

A knowledgeable staff member or consultant with experience working the FEMA Public Assistance program

that is the source of many DHS (Department of Homeland Security) grant funds may be able to help substantially increase the amount of funding that a community is provided to rebuild such essential infrastructure as schools, hospitals, libraries, community centers, and other facilities. In short, if a community: (1) is properly educated – before a disaster strikes – about eligibility criteria, applicant responsibilities, mitigation opportunities, and documentation guidelines; and (2) understands, in addition, how federal disaster programs have been applied elsewhere – that community will start its long-term recovery much faster and will achieve more than a community that does not possess this same situational awareness, and as a bonus will have more resources available to support its own efforts.

### 5. Keep an Eye on Cash Flow

Although insurance proceeds, and both federal and state aid, will help with the financial burden caused by a disaster, they often do not cover all – or even most – of the costs such events create. Moreover, reimbursement often occurs long after associated costs are incurred, so most communities should expect a disaster to adversely affect the city's financial situation for what might be an extended period of time.

These and several other post-disaster challenges can cause major community cash-flow problems that not only can adversely affect other community services, but also slow the recovery process itself by extending the timelines needed for reconstruction. High-risk communities should therefore consider establishing a “rainy day” fund well in advance of

a disaster to provide the seed funding needed for the initial recovery efforts. The availability of such funding can help fill the gaps between the time a disaster occurs and the time when insurance and government help arrives.

To help cope with presidentially declared disasters, a community should consider asking for an advance of FEMA funds against damage assessment cost estimates. It is not uncommon for communities to be advanced a percentage of their estimated losses – usually between 25 and 50 percent of estimated eligible damages. Maintaining full and accurate documentation is critical, though, because communities will probably receive no additional recovery funds until documentation has been provided that shows the use of advanced funds for eligible purposes. If such an advance is part of the community's own disaster planning, that information should be provided to senior officials in the state's emergency management agency so that they will be ready and able to support the community needs after an event occurs.

To briefly summarize: The impact of a disaster can drastically affect the economy of a community and in some cases even its long-term existence. Being prepared administratively for a disaster is just as important as being prepared in the traditional and better publicized ways.

---

*Andrew Sachs is the Vice President of Disaster Services at Witt Associates, a public safety and crisis management consulting firm. Sachs has been instrumental in the long-term recovery operations following several major U.S. disasters including the 2008 Iowa floods; Hurricane Katrina; and the Galveston Island recovery operations following Hurricane Ike.*



## DomesticPreparedness.com Survey, Your Opinion Matters! *The Future of Grants in Domestic Preparedness*

With 26 federal agencies offering over 1,000 grant programs annually, it is estimated that almost 100 of these grant programs are considered “preparedness-related” and support the ability to build and improve the capabilities necessary to prevent, protect against, mitigate the effects of, respond to, and recover from threats that pose the greatest risk to national security.

Unfortunately, many grants are in danger because of today's economic conditions:

- Significant financial pressures on local, state, and federal agencies;
- Many local, state, and federal budget reductions;
- Declining budgets adversely affecting preparedness grant programs;
- Declining budgets reducing the government's capacity to meet prior demands for service and support of preparedness capabilities throughout the country.

DomPrep wants to know your opinion on how the future of federal grant funding will impact program priorities, multi-jurisdictional and multi-disciplinary collaboration efforts, and the effective administration of grants.



Sponsored by  
**Booz | Allen | Hamilton**  
delivering results that endure

# The Public Health Role During Mass-Fatality Incidents

By Raphael Barishansky & Audrey Mazurek, Public Health



The term “mass fatality incident” is defined as an incident in which more deaths occur than can be handled by local resources. However, determining what constitutes a mass fatality incident varies from one jurisdiction to another not only because communities differ in both size and resources but also because such incidents can be caused by natural hazards, human-related hazards, or “pro-active” human hazards.

Although different from other types of public health services, and even counter to how most people view public health (i.e., as a sector dedicated to ensuring the health and safety of the public), mass fatality management is actually one of the key responsibilities listed – under the Federal Emergency Management Agency’s National Response Framework – as an Emergency Support Function (ESF). Mass fatality management comes under *ESF #8, Public Health and Medical Services*. In most if not quite all jurisdictions, the public health authority is specifically responsible for ESF #8.

The overall responsibilities for public health in a mass fatality incident vary considerably, though, by jurisdiction and state. However, public health still plays an important role during planning, response, and recovery efforts. Today, public health agencies have greater first-responder and overall preparedness roles than ever before. They also have more experience and are members of partnerships that are vital during major disasters – e.g., working with vulnerable populations, collaborating with community partners and volunteer organizations – and are expanding pre-existing relationships with laboratories and with medical examiners/coroners (ME/Cs).

## Rules, Regulations & Responsibilities – With Numerous Exceptions

It is important to remember, though, that public health’s responsibilities during a mass fatality incident do not supersede those of the ME/Cs – or of such U.S. government agencies as the Federal Bureau of Investigation (FBI) and/or the National Transportation Safety Board (NTSB). However, jurisdictional and/or state authorities spell out the specific responsibilities of public health and other first responders vs. those of the ME/Cs. One example: In the State of Maryland, the Office of the Chief Medical Examiner (OCME) has jurisdiction over “any death which is the result of a casualty or accident, homicide, poisoning, suicide, rape, therapeutic

misadventure, drowning, of suspicious or unusual nature, or of any apparently healthy individual while not under the care of a physician.” In all such cases, local public health departments provide support to OCME and law enforcement agencies – but have jurisdiction over and coordinating authority for all other types of mass fatality incidents that do *not* fall under OCME jurisdiction.

Under normal conditions, approximately 90 percent of the fatalities in Maryland, which result from natural diseases occurring under natural circumstances, are *not* OCME cases. However, approximately 90-95 percent of all of the mass fatality incidents in the state *are* under the jurisdiction of OCME – because they result from accidents, homicides, and/or other unusual or suspicious circumstances. For most jurisdictions, therefore, only a small percentage of mass fatality events fall outside the care of the ME/Cs (which have and must adhere to their own mass fatality plans). Nonetheless, public health and its partners must still develop detailed plans to ensure that: (a) there is a common understanding of their respective roles, responsibilities, and available resources; and (b) essential functions can and will continue during an incident.

After determining the general parameters of responsibilities – as specified by a state or other jurisdiction’s laws – during a mass fatality incident, the next step is to determine what agencies and individuals should be “at the table” at the beginning of the planning process. In that context, what might be and frequently is a very long list obviously should include at least the following: law enforcement agencies and fire departments; emergency medical services (EMS); homeland security/emergency management; hospitals and other healthcare facilities (including mental health providers; ME/Cs; volunteer organizations – the American Red Cross, for example); and representatives of the death care industry (funeral homes, cemeteries, and crematories). A number of state and regional agencies likely to be involved in various ways also should be included.

## The Creative Process – Pitfalls and Problem Areas

The mass fatality management plan developed by the aforementioned stakeholders should not supersede but, rather, be complementary to the ME/C mass fatality plan, other responder plans, and/or state and regional plans. If and when possible, the planning process should review, and use as a template,



existing plans and best practices/resources from other jurisdictions – e.g., “*Managing Mass Fatalities: A Toolkit for Planning*,” developed by the Santa Clara County [California] Public Health Department.

Following are brief descriptions of some but no means all of the principal topics, issues, and potential problem areas that should be included in a truly comprehensive and operationally effective plan:

**Introduction:** The first component of the plan is introductory in nature and states the rationale (purpose and objectives) behind writing the plan, as well as its scope and a list of emergencies covered – in this example, these are almost always health-specific and would probably include, but not be limited to, terrorist acts or threats, infectious-disease emergencies, the dangers caused by contaminated drugs and/or medical devices, food or waterborne disease outbreaks, and/or contamination of a public water supply. This section also should clearly state which incidents fall under the umbrella of law-enforcement agencies, and which do not.

**Authorities and Definitions:** The next section of the plan should list the legal authorities under which the plan is being written – e.g., State codes, local Emergency Operations Plans – as well as the relevant definitions. The latter should be as comprehensive as possible because, for legal purposes, the agencies participating may well have to rely on those definitions at a later date.

**Situation and Assumptions:** This section discusses the jurisdiction’s situation and assumptions, including numerous operational realities: the agencies (and/or officials) that have jurisdiction over decedents; various obstacles that have the potential to challenge a response to mass fatality incidents; the roles played by various federal agencies (e.g., NTSB, FBI); and the responsibilities of Disaster Mortuary Operational Response Teams (DMORTs).

**Command and Control:** This section provides detailed instructions on how an incident or event should be managed (as spelled out in Incident Command System/Unified

Command guidelines) as well as how public health and other response agencies should support the ME/C, federal agencies, and the region, etc. This section might also include a detailed breakdown of the roles and responsibilities of health departments and other response agencies.

**Concept of Operations:** This section, often the longest and most detailed section of the mass fatality management plan, spells out the operational and procedural steps that must be taken to: (a) activate the plan; (b) communicate with partners, media, and the community at large; and (c) carry out the roles/

responsibilities involved in each phase of mass fatality management. (Public health is usually *not* the lead agency designated to carry out the functions/activities under each phase, but it may be the lead coordinating agency and/or play a major supporting role. In addition, it should be remembered that, depending on the responsibilities assigned by local or state authorities, local agencies may be operating under the direction of ME/Cs.)

## A Daunting and Detailed List of Duties

After the legal jurisdictional framework and chain of command have been spelled out, the planning process should shift to the specific tasks and responsibilities likely to be faced immediately following, during, and concluding a specific mass fatality incident. Following are a few specific examples of the mass fatality management phases and some probable public health responsibilities in each such phase.

- **Human Remains Recovery/Retrieval:** Public health supports the lead agency (e.g., Fire/Rescue, EMS, and/or law enforcement) in acquiring supplies and resources, providing subject-matter expertise related to decontamination, and maintaining awareness of operations to anticipate challenges.
- **Transportation:** Public health may coordinate transportation, but the lead agencies are usually the local transportation/public works administration and/or death care industry. Transportation needs should be requested through the Emergency Operations Center (EOC), but public health may offer

*The responsibilities for public health in a mass fatality incident vary considerably by jurisdiction and state; public health plays an important role during planning, response, and recovery efforts; public health agencies have greater first-responder and preparedness roles than ever before*

guidelines for suitable transportation assets and the movement of remains, and maintain awareness of the community transportation needs of the death care industry.

- **Storage:** Public health should work with applicable community partners such as hospitals and emergency management agencies to identify appropriate locations for both the short- and long-term storage of decedent remains.
- **Identification and Tracking:** Although identification of decedents is usually led by law enforcement and the ME/C – with law enforcement serving as the lead in notifying the next of kin – all of the response agencies involved, including public health, are responsible for ensuring the careful and respectful tracking of decedents, body parts, and personal effects.

**Interment:** If remains cannot be stored in a refrigerated facility while awaiting final disposition, temporary interment (i.e., burial) may be considered. Public health assists in selecting appropriate temporary interment sites, ensuring that the appropriate resources are available, and – at the conclusion of the mass fatality incident – assisting with the process of re-interment.

**Disposition:** A key goal during a mass fatality incident is to ensure that each body reaches the “final disposition” stage in accordance with his or her religious and cultural practices as well as the wishes of the victim’s family. In support of this goal, public health assists the death care industry in developing a viable continuity of operations plan (COOP), providing situational awareness and appropriate public messaging capability, and ensuring that the resources needed are available.

**Death Certificates:** Although physicians and ME/Cs are responsible for filling out and signing death certificates, public health plays a key role in communities in which the health department processes death certificates. (The health department’s COOP may have to be activated, though, to ensure that the resources needed are readily available to help in the processing of death certificates.)

**Law Enforcement/Security:** Public health keeps law enforcement informed of security needs, a particularly important responsibility at all mass fatality incident operational areas – storage sites as well as incident sites.

**Supply and Volunteer Management:** Public health works with community partners, volunteer groups – the Medical Re-

serve Corps (MRC), for example, and Community Emergency Response Teams (CERTs) – and faith-based organizations to ensure that volunteers are appropriately trained, possess the equipment and other material resources needed, and fully understand their individual and collective roles and responsibilities (and limitations) during the event.

**Family Assistance:** The family assistance center (FAC) is a particularly important component of the jurisdictional infrastructure both during the planning process and during the event. Depending on the type of incident, the FAC, which can be either a physical or “virtual” location (a designated hotline, for example), usually serves as a primary resource for families that want to exchange information about missing and deceased relatives. The FAC also assists in the re-unification of families with decedents, and provides many of the resources and services needed not only by survivors but also their families (e.g., disaster behavioral health services, final disposition options, grief counseling).

**Demobilization/Recovery:** Depending on the type of incident, public health may have to provide immediate and/or ongoing support to mass fatality management to work toward a respectful resolution and final resting place for decedent remains. In addition, public health probably will have to manage certain environmental-surety issues such as decontamination, determining a safe return to facilities, and both water and soil sampling.

## Laminated Checklists And Other Odds & Ends

Among several essential appendices to the completed plan would be such helpful data as the following: “Key Contacts” information (particularly valuable for agencies and organizations in the death care industry); a list of decedent storage and handling sites; local public and media communications outlets; religious and/or cultural organizations in the local community; a death management process checklist; communications links to ME/Cs; and the steps needed to access state, local, and/or regional mass fatality management plans available to the public.

It should be kept in mind at all times, moreover, that one of the most challenging aspects of the planning process is not writing the plan per se but, rather, ensuring that it is operationally possible, useful, and easy to follow during an actual emergency. Because a mass fatality plan is more technical in nature – and differs in several important ways from most other public health



# RELIABLE



# BIO DETECTION

RAZOR™ EX The Complete Field BioThreat Solution

[www.RAZOREX.info](http://www.RAZOREX.info)



plans – it is particularly important that all of the agencies and individuals involved clearly understand not only their own roles but also the rationale used for the development and organization of the plan.

In addition to training and exercises, each response agency also should develop checklists or tip sheets of the plan – i.e., a relatively short (no more than 4-5 pages) document summarizing the key points and definitions used in the plan. Also included should be a checklist of the planning, response, and recovery responsibilities of each participating agency. These checklists can and should be laminated and should be carried by the units – police, fire, EMS, and health agencies, usually – most likely to be first on the scene for their respective agencies.

Incidents that produce large numbers of fatalities are more common today than ever before, and for that reason alone there is a compelling need to prepare and plan much more effectively than ever before – and earlier – for emergency responses of all types. Weather events such as the deadly tornadoes that devastated several U.S. communities earlier this year, Hurricane Katrina, the Japan tsunami/earthquake – compounded by the 9/11 attacks and other terrorist incidents, as well as aviation accidents and other “manmade” disasters – serve as stern but absolutely essential reminders of how traditional responses have been replaced in recent years by the compelling need for a much broader understanding of the comprehensive planning needed to deal effectively with complex mass fatality events.

#### **For additional information:**

On the 15 Emergency Support Functions, click on the National Response Framework at [www.fema.gov/emergency/nrf](http://www.fema.gov/emergency/nrf)

On the Santa Clara (California) County Public Health Department’s “Managing Mass Fatalities: A Toolkit for Planning,” click on [www.sccgov.org/sites/sccphd/en-us/HealthProviders/BePrepared/Pages/Managing-Mass-Fatalities.aspx](http://www.sccgov.org/sites/sccphd/en-us/HealthProviders/BePrepared/Pages/Managing-Mass-Fatalities.aspx)

*Raphael M. Barishansky, MPH (pictured), is currently the program chief for Public Health Emergency Preparedness for the Prince George’s County (Md.) Department of Health. Prior to establishing himself in this position, he served as executive director of the Hudson Valley Regional EMS (Emergency Medical Services) Council, based in Newburgh, N.Y. He is a frequent contributor to various journals, and can be reached at [rbarishansky@gmail.com](mailto:rbarishansky@gmail.com)*

*Audrey Mazurek is a senior associate at ICF International and a public health preparedness planner for the Prince George’s County (Md.) Health Department. She also serves as an adjunct analyst at the Homeland Security Studies and Analysis Institute (HSI). Previous to assuming those positions, she was a program manager at the National Association of County and City Health Officials (NACCHO).*

## **The Joplin Tornado**

# **45 Seconds of Danger, A Lifetime of Lessons**

By Craig DeAtley, Health Systems



The EF5 tornado that struck Joplin, Missouri, during the evening of 22 May 2011 was among the deadliest in U.S. history. More than 140 persons died, over 1,000 were injured, and thousands of others were left homeless. In addition, it has been estimated that the cost to “rebuild” Joplin could be as much as \$3 billion.

Over the past two weeks, hundreds of emails, blog reports, and both print and broadcast media stories reported on the heroic actions, selfless dedication, and creative determination displayed by the staffs of many Joplin healthcare facilities, conspicuously including the doctors, nurses, and other staff of the St. John’s Regional Medical Center, which was totally devastated.

The 228-bed facility was one of Joplin’s two main hospitals, and is now one of the few hospitals in the nation ever to be all but completely destroyed by a tornado – the last one was hit in Americus, Georgia, in 2007. If nothing else, though, the initial reports from Joplin serve as a reminder to other hospitals and long-term healthcare facilities, not only in the United States but everywhere in the modern world, about some very important lessons to remember.

## **Planning Ahead – Starting Yesterday**

Tornadoes are well known in Missouri and the states surrounding it, and no doubt appear high on every healthcare facility’s hazard-vulnerability analysis. Based on what St. John’s encountered, a truly comprehensive plan must address an exceptionally broad spectrum of extremely complex issues and potential problems – including, but not limited to, the following:

- The operational and economic ramifications of running a hospital that has been heavily damaged or destroyed;
- The operational demands on the staff that would be needed to rescue and care for the injured – probably including other staff members;
- The necessity of providing ongoing in-patient care while simultaneously overcoming complete utility, phone line, and radio failures;



- The parallel need of providing emergency care for newly arriving patients who were injured elsewhere in the same general area (but outside the hospital itself);
- The urgent requirement, if and when it becomes mandatory, to transfer all in-house patients to other healthcare facilities, including hospitals that are perhaps hundreds of miles away;
- The use of both medical and non-medical volunteers, many from the local community and others from healthcare facilities both in and out of state;
- The need to establish, and follow, a complete and reliable medical-record recovery procedure that takes into account not only print materials but also x-rays (some of St. John's records were found two counties away);
- The management of in-patient deaths caused by and/or otherwise related to the storm;
- The difficulties encountered in carrying out a reliable damage assessment – while at the same time trying to establish a new, albeit temporary, facility a few miles away;
- The importance of immediately securing, insofar as possible, critical “economic/fiscal” departments or areas of the facility such as the pharmacy, the gift shop, debit machines, and hazardous-material storage sites; and, last but not least,
- The problems involved in: (a) quickly relocating the additional medical resources needed; (b) transferring those resources to newly established triage and treatment sites; and (c) eventually moving all usable equipment to temporary alternative-care sites.

## Responding, Recovering & Remembering

Although the tornado's physical impact on the St. John's Center lasted only about 45 seconds or so, there had been, fortunately, a general 20-minute alert to the entire Joplin area. That providential warning gave the St. John's staff enough time to move many patients into the hospital's hallways and stairwells. However, when the explosive pressure and storm winds knocked out most windows, the flying glass and other debris injured a number of the still exposed patients and their protective staff. The burst pipes pouring huge quantities of water onto the floors and down the stairs, coupled with the rapidly approaching general darkness, further complicated the situation.

Carrying out their duties in accordance with the hospital's response plan – and/or possibly by mere human instinct – staff members quickly organized themselves, implemented the facility's incident-command guidelines, and started moving

patients to safer areas both inside and outside the hospital. All available resources – tables, chairs, and doors, for example – were among the “equipment” creatively used to carry out the massive transfer. These initial efforts were supplemented by those of other rapidly arriving hospital staff – as well as by local police, firemen, EMS, and community volunteers who came to help in any way needed – moving patients, caring for the injuring, and/or even transporting patients in their own trucks and SUVs to other hospitals. For patients awaiting transfer, medical care was provided using the limited quantities of available medical supplies; medications, especially pain medicines, were in high demand.

Within the next several days, a mobile hospital – consisting primarily of an 18-bed Emergency Department and 60-bed in-patient capability – was being staffed by St. John's personnel and by state and federal healthcare providers (Missouri's Disaster Medical Assistance Team 1, for example). An engineering evaluation of the damaged facility is still being carried out to determine the viability of rebuilding options. In the meantime, all movable items – including the pharmacy inventory, hospital beds, x-ray equipment, ventilators, and IV pumps – have been relocated for use elsewhere.

The other major hospital in Joplin, the multi-facility Freeman Health System, was spared major damage and has remained fully operational. The Freeman staff are now working with St. John's administrators – and with local, state, and federal health and emergency management officials – to determine how the community's healthcare needs will be met in the months and, quite possibly, years to come. The Missouri Hospital Association has also played a major leadership role both by assisting local communities with their initial responses and by helping orchestrate the overall planning for the future.

In time, the real-life storytellers who lived and worked through the horrors and challenges of the Joplin tornado will share their firsthand accounts. Until then, the early reports that are read or heard in emails, blogs, print and broadcast media, and various social networks have provided a wealth of preliminary lessons that healthcare facilities should start studying immediately – before, and just in case, one of them becomes “the next Joplin.”

---

*Craig DeAtley is the Director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region's largest hospital, Emergency Manager for National Rehabilitation Hospital and co-executive director of the Center for HICS Education and Training. Prior to assuming his current position, he was an Associate Professor of Emergency Medicine at George Washington University for 28 years, before leaving to start the Institute.*

# Public Health and Medical Interoperability Challenges

By Bruce Clements, *Public Health*



Interoperability continues to pose substantial challenges across all emergency support functions. Although it is most often focused on communications between and among first responders – and on equipment shared through mutual-aid events – health and medical interoperability poses unique challenges as well. In addition to sharing communication challenges, public health and medical professionals involved in preparedness and response activities face a number of interoperability issues ranging from the systems and devices used in clinical settings to electronic medical records, epidemiological surveillance and laboratory data, Geographical Information Systems (GIS), and patient tracking systems. However, large-scale emergencies involving the deployment of public health and medical assets across multiple jurisdictions and/or the widespread sharing of related data are infrequent, which means there are fewer opportunities to test these assets and systems for interoperability.

Meanwhile, the growing complexity of technology across the full continuum of healthcare delivery is posing additional interoperability challenges. Medical devices are rapidly becoming more automated, for example, and generating more patient data than was ever before possible. Even the basic monitoring of vital signs has advanced to the point where it can capture extremely detailed patient data – quickly, and in large quantities – and share it for a variety of uses, including telemedicine. Although this technology has tremendous promise for future emergency response activities, the systems now emerging often cannot communicate with one another. This lack of plug-and-play connectivity and interoperability poses new operational challenges to healthcare providers – and, of greater importance, increases the risks to patient safety.

The transition to electronic medical records (EMRs) has started, though, and promises to change U.S. healthcare as much, and as dramatically, as the introduction of credit cards and on-line banking in recent decades changed personal and corporate financial practices. EMRs will similarly transform the ways care is provided during public health emergencies and major disasters. Today, as individual citizens arrive at emergency-treatment or patient-evacuation locations, providers seldom have adequate information on the patients' treatment history, drug allergies, and/or pre-existing conditions. Even if a patient has a paper medical record immediately available, the accuracy and completeness of the information in that record may be questionable, for two reasons: (1) the fragmentation of healthcare delivery in the United States; and (2) the fact that the healthcare records of most U.S. citizens have, over a period

of many years – sometimes decades – been compiled by a number of previous primary-care physicians in several healthcare delivery settings. The compilation and ready availability of integrated and interoperable EMRs will alleviate this problem considerably by providing much-needed “longitudinal” health information during a response – and, as an additional benefit, also provide an effective mechanism to document the care provided during an emergency, even in austere conditions.

## The Two-Headed Challenge Blocking a “Dramatic” Upgrade

An additional challenge to the creation and use of EMR interoperability involves the often conflicting needs to maintain patient confidentiality while also compiling a complex mass of healthcare information. The building of a truly interoperable EMR system, therefore, requires a solution to the perceived dichotomy between the need to rapidly share complex personal information while at the same keeping that information as secure as possible. Nonetheless, when (not if) the U.S. healthcare community resolves this issue and interoperable EMR data becomes the new standard, the national shift to an EMR-based healthcare system will dramatically improve how care is provided during large-scale emergencies.

Effective epidemiological surveillance can usually determine if and when a public health risk is developing, primarily through the early detection of emerging diseases or of a bioterrorism attack. Typically, the surveillance also measures how effectively a response is being managed, in large part by providing population-based data on key health indicators.

Unfortunately, many surveillance systems currently in use are not interoperable. In fact, a high percentage of the healthcare professionals serving in epidemiologist roles, gathering and analyzing this critical data, still receive much of their information through hand-written notes or faxes. Even worse is the fact that the data they receive is often entered twice – first into a system designed to meet reporting requirements, and then into another program designed to help the epidemiologist complete his or her own analysis. This process not only is labor intensive but also raises legitimate concerns about the integrity and consistency of the data being entered. The implementation of automated and interoperable surveillance systems could alleviate and eventually eliminate these double-entry problems and enhance the effectiveness of epidemiologists by significantly reducing the time it takes medical researchers to detect emerging public health threats.





# INTRODUCING MASS SPEC FOR THE MASSES

**GRIFFIN™** | **460**

The Griffin™ 460 mobile GC/MS with multi-modal sample introduction is ideal for field-based forensics and other mobile laboratory applications, as well as for integration into facility air handling systems for rapid detection and identification of a chemical agent release. The simplified sample handling along with the continuous direct air monitoring capability and easy to understand user interface enables non-technical users and analytical chemists alike to employ the system with success.

Detection, confirmation and continuous monitoring in a single instrument — the Griffin 460.

[www.flir.com/griffin460](http://www.flir.com/griffin460)

 **FLIR®**  
Extraordinary Protection

Much like the challenges facing epidemiology, public health laboratories often receive and share information through the use of written notes and faxes. Progress in modernizing this approach has been made in recent years through the Public Health Laboratory Interoperability Project – a collaborative initiative between the Association of Public Health Laboratories (APHL) and the Centers for Disease Control and Prevention (CDC). The project, which started in 2006 with six state laboratories and the CDC, has since expanded to 22 states. Significant progress toward full interoperability is already being achieved through the collaborative efforts between the IT (information technology) staff and laboratory professionals, who are working together to: (a) define what the ideal laboratory IT infrastructure should look like; and then (b) standardize the complex laboratory messaging and documentation needed to create such an infrastructure.

### **Numerous Ancillary Benefits Also Predicted**

The work being done by the APHL and CDC participants should help reduce the multiple interfaces and communication inconsistencies that are now relatively common. Moreover, as the project defines needs more precisely, shares the lessons learned, and standardizes the processes now used, a high percentage of the nation's laboratory systems will become better integrated and more interoperable.

As electronic medical records become the new standard and associated epidemiology and laboratory information becomes both more integrated and interoperable, one major result will be the more rapid detection of naturally occurring or emerging infectious disease outbreaks. The new EMR system will also assist in quickly gauging the effectiveness of a specific public health emergency intervention or response. That capacity – combined with other well integrated, and interoperable, GIS and patient tracking tools – can facilitate a robust public health and medical response to any emerging public health threat.

That type of system is attainable today – but unfortunately is likely to be many years away from becoming a reality. The reason is more administrative in nature than it is the technological challenges that still must be overcome. The problem is easy to describe, but difficult to resolve: Engineering interoperability into the nation's public health and medical preparedness and response system is hampered considerably by the decentralized nature of public health. One of the operational strengths of public health is that it is typically decentralized and locally focused. However, that decentralization makes effective standardization more difficult to achieve. One example: there are and have been for quite a few years many epidemiological surveillance tools available to epidemiologists throughout the country. When funding for public health preparedness rapidly increased after the terrorist attacks of 2001, markets responded to the opportunity by

creating even more tools. However, while public-sector vendors were introducing a variety of superb new surveillance systems and devices, there was little consideration of mandating interoperability as one of the goals to be achieved.

### **Vigorous But Fragmented Responses & a DOD-Based Solution**

That problem is likely to continue, and expand, for some time to come. As new requirements emerge in the absence of a singular national approach, vendors will continue to respond as they did before, and the surveillance systems in use will likely remain fragmented. For that reason alone, the nation's public health and medical leaders should carefully consider how other federal agencies have overcome similar problems in their own areas of responsibility.

One example worth serious consideration is the procurement system used by the U.S. Department of Defense (DOD), which provides detailed specifications of what products will meet its combat needs. U.S. (and foreign) contractors compete with one another by developing various design and program packages that will: (a) build the new weapons systems needed by U.S. naval and military forces; (b) provide the support and maintenance equipment also needed; and (c) even field the necessary training programs that will be needed. For very complex weapons systems – the Joint Strike Fighter, to cite but one prominent example – the RDT&E (research, development, test, and evaluation) process mandated before the start of actual production may take nearly a decade. The long timeline postulated, of course, results primarily from the complexity of the weapons system.

Surprisingly, perhaps, the question facing the U.S. healthcare community is even more difficult to answer. Why, one might ask – how much more complex is the U.S. public health and medical infrastructure? The answer is not technological but political in nature – more specifically, the fact that the annual nature of federal preparedness funding usually limits spending to off-the-shelf products that lack the much-needed interoperability and integration discussed above.

Nonetheless, the prognosis for the U.S. healthcare community, and for the American people, is promising – but with several conditions attached. There is little doubt that the nation's healthcare system as a whole will “get there” eventually. But with the current relatively meager funding approach, reaching that elusive goal will probably take many years more than it should.

---

*Bruce Clements is the Public Health Preparedness Director for the Texas Department of State Health Services in Austin, Texas, and in that post is responsible for health and medical preparedness and response programs ranging from pandemic influenza to the health impact of hurricanes.*

# NLE 2011: Successful Learning, Plus Partnership Building

By Kay C. Goss CEM, Emergency Management



In April and May of this year, more than three million U.S. citizens in or around Alabama, Arkansas, Georgia, Illinois, Indiana, Kentucky, Mississippi, Missouri, Oklahoma, South Carolina, and Tennessee took part in the largest earthquake preparedness efforts ever in the history of what is called the “New Madrid region.” Exercise design, development, preparedness, and implementation for “the Great Central U.S. ShakeOut” took more than two years. The mantra for the exercise was the same as it is and has been for all earthquakes: “Drop, Cover, and Hold On.”

This year’s National Level Event (NLE) was designed primarily to encourage public-sector, private-sector, and nonprofit organizations to: (a) consider how, working together as a team, they would react if a real earthquake were to strike; and (b) encourage them to have in place, before such an event occurs, the preventive and preparedness measures needed to cope with it.

At the same time, coincidentally – while the final plans for NLE 2011 were still being discussed – a number of violent storms, historic floods, and devastating tornadoes were causing widespread destruction and killing hundreds of people in a number of U.S. states in various areas of the country. In fact, many responders and decision makers who originally intended to participate in the ShakeOut were forced to alter their plans because of the real-life disasters occurring in their home communities.

The Great Central U.S. ShakeOut was modeled after the Great California ShakeOut drills, which have been scheduled annually since 2008. All of the ShakeOut drills incorporate best practices lessons learned at the Southern California Earthquake Center and the Earthquake Country Alliance – which partnered with the Central United States Earthquake Consortium (CUSEC). The New Madrid states’

governors, including their staffs, and the consortium’s director, Jim Wilkerson, and his staff compose CUSEC. The U.S. Geological Survey and dozens of other federal agencies and related organizations throughout the country also provided support, technical assistance, and the “players” needed for various stages of NLE 2011.

*While the final plans were still being discussed, a number of violent storms, historic floods, and devastating tornadoes were causing widespread destruction and killing hundreds of people in various areas of the country; in fact, many responders and decision makers who intended to participate in the ShakeOut were forced to alter their plans because of the real-life disasters in their home communities*

## Fugate: Studying, Learning & Actually “Doing”

Only a few days earlier – i.e., at the 18-22 April 2011 National Hurricane Conference in Atlanta, Georgia – Federal Emergency Management Agency (FEMA) Administrator Craig Fugate not only set the stage for NLE 2011 but also articulated the profound opportunities ahead by pointing out that such multilayered exercises of catastrophic scenarios “provide a better opportunity for studying and learning from the decision-making process than do real-life disasters.”

The NLE scenario postulated a massive earthquake occurring along the New Madrid fault, which is named after a series of earthquakes, the largest ever recorded in the United States, starting on 16 December 1811 not far from New Madrid, Missouri, and causing major damage over an area of about 50,000 square miles. (The much better publicized San Francisco earthquake of 1906 caused damage over an area of about 6,000 square miles, for example.) The 1811 earthquake, according to contemporary accounts, was reported to have “rung the church bells all of the way to Boston, and caused the Mississippi River to run backwards for three days.”

The historic significance of the 2011 ShakeOut, deliberately scheduled close to the 200th anniversary of the 1811 disaster, added an important and dramatic element of realism to this year’s series of exercises. Partly for that reason, almost two million people, many of them using social media, signed up to participate in the exercise and/or to keep advised of NLE



2011's progress. The CUSEC stepped up, as did the National Emergency Management Association (NEMA), to support FEMA, the federal agencies, and the many states participating in what turned out to be an enormously vigorous effort.

In preparation for the exercise, state emergency management directors agreed that they had been fairly well prepared for, and had planned well, for the allocation of resources they already had on hand – but had not planned nearly as well for the resources they did *not* have on hand. To solve that problem, FEMA, CUSEC, and various state agencies worked in close cooperation in regional Resources Allocation Workshops. Thus, NLE 2011 not only gained greater attention, more innovation, and an enhanced national focus, but also received more widespread support with actionable results, than most other similar exercises. Additionally, Administrator Fugate's emphasis on the involvement of all elements of the emergency management team in "the Whole of Community" certainly bore fruit in NLE 2011, with a most robust participation level ever achieved in an exercise.

## Planning, Coordination, And a Stronger Focus on Processes

Following is a brief synopsis of some of the many lessons learned during NLE 2011 – both about the exercise itself and/or worth follow-up consideration by jurisdictions and leaders participating, as well as by emergency management leaders throughout the world:

The states participating in NLE 2011 launched an initiative to spend more time and effort in planning for the resources they might need during a catastrophic event but presently do not have in their current inventory of material and personnel resources. Where and how they would acquire these needed resources, as well as the processes available for accomplishing this task, are the principal questions that must be addressed. This will be helpful to other states, outside the New Madrid area, as they prepare for other catastrophic events.

- As with many other real-life disasters, keeping all exercise participants, including high-level decision makers, fully informed about all aspects of the unfolding disaster was and will be a continuing challenge.
- Improved operational processes are needed for continuing efforts in making and integrating mission assignments.

- The equally important "alert" and notification processes, structured to ensure that all participants with "need to know" responsibilities, are kept fully informed when the decision is made to activate a notification process.
- Improved coordination of all modes of transportation during evacuations also helps to ensure an enhanced, seamless process is in place to cope with all catastrophic events – especially, this year, during what could be a particularly dangerous hurricane season.
- The continued upgrade of resource support processes now in place will prove quite beneficial going forward. Fortunately, the federal National Response Framework (NRF) covers resource management extensively, and appropriate standards are being developed, and NLE 2011 showed that these and other processes are crucial to full and effective operational preparedness.

To briefly summarize: Huge but immeasurable quantities of hard work, professional and personal commitments, and long hours – years, actually – of unstinting effort were invested in NLE 2011, and many successful results were achieved. Future planning will reap the benefit of these efforts, and future exercises will be able to more precisely pinpoint the potential as well as actual improvements that are most urgently needed. Most important of all, everyone involved in this year's series of exercises – a broad spectrum of participants ranging from government officials to private-sector businesses and nonprofit organizations to everyday citizens – learned an immense amount of helpful information from the Great Central U.S. ShakeOut. Many valuable partnerships in preparedness were developed and enhanced. Thanks to all who made this possible!

---

### **For additional information on:**

*The Great Central U.S. ShakeOut*, visit <http://www.shakeout.org/centralus>

*Drop, Cover and Hold On*, visit <http://www.cusec.org/earthquake-safety/drop-cover-a-hold.html>

---

*Kay C. Goss, CEM, possesses more than 30 years of experience – as a federal and state administrator and in the private sector – in the fields of emergency management, homeland security, and both public finance and intergovernmental operations. A former associate FEMA director in charge of national preparedness training and exercises, she is a noted lecturer as well as the author of several books and numerous articles and reports in the fields of homeland defense and emergency management.*

# Man-Caused Incidents – New Challenges & Systems

By Steve Grainer, Fire/HazMat



By all estimates, major emergencies and disasters are likely to continue to increase in frequency for the foreseeable future. Moreover, the severity of such disasters seems to be intensifying. Since the 1980s, most preparedness efforts throughout the United States have focused on an all-hazards approach that minimizes any distinctions between natural and man-caused incidents. However, although the all-hazards philosophy provides a consistent baseline for planning, those responsible for operations, emergency management, and response resources must also base their strategic and tactical decisions on incident factors that reflect the cause, if only because inclusion of that information may help significantly in determining how best to act.

Historically, the impacts – both economic and psychological – from natural disasters such as hurricanes and earthquakes have been far greater than the losses and impacts from man-caused disasters. Man-caused emergencies, however, present challenges that are significantly different from those posed by natural disasters – which almost always have a clearly identifiable cause. A hurricane, for example, is characterized by high winds, flooding, storm surge, and other effects.

In addition, and with only a few exceptions, the impact of a natural disaster can often be forecast or predicted in advance. In contrast, the occurrence and cumulative effects of man-caused disasters are usually more speculative than predictive.

## Precipitating Conditions, Factual Projections & Intended Dangers

When planning for man-caused incidents, decision makers can build hazard, risk, and vulnerability assessments using a formula similar to those used in planning for natural disasters. For example, planners can often (but not always) project such fac-

tors as the size of the population likely to be affected and/or the potential economic impact. However, unlike natural incidents, the precipitating conditions (such as weather systems) usually cannot be accurately predicted. The answers to the “when,” “where,” “what,” and “how” questions, therefore, are frequently more a matter of guesswork than of factual projections.

Perhaps of much greater importance when confronted with a man-caused incident, response managers and operational personnel must quickly determine whether the emergency is incidental (i.e., accidental) or if it is intentional. In the case of an intentional act, the urgency of response actions must be tempered by a recognition that the precipitating event may be only one of several intended dangers. There have been, in fact, a number of incidents documented in recent years in which more than one intentional action was coupled with one or more additional or secondary hostile actions. For example, a terrorist may detonate an explosive device or cause a disturbance that would generate an initial emergency response. The first emergency responders arriving at the scene of the incident may be subjected to danger from another device and/or potentially exposed to other and sometimes greater hazards. For that reason alone, the planning for and responding to a man-caused incident must reflect a very careful initial assessment and, in most cases, include additional precautions.

This “just in case” added requirement obviously increases the urgency of accurately, and completely, defining

and categorizing both the nature and the scope of any man-caused incident. When planning for such incidents, therefore, responders and incident commanders must do everything possible to identify the potential for secondary actions and/or “cascading events” – which can be described as situations in which one problem leads to another, and then another, etc., in what could be a long series.

*Man-caused emergencies present challenges that are significantly different from those posed by natural disasters, which almost always have a clearly identifiable cause; in addition, and with only a few exceptions, the impact of a natural disaster can often be forecast or predicted in advance – in contrast, the occurrence and cumulative effects of man-caused disasters are usually more speculative than predictive*



## Still and Always

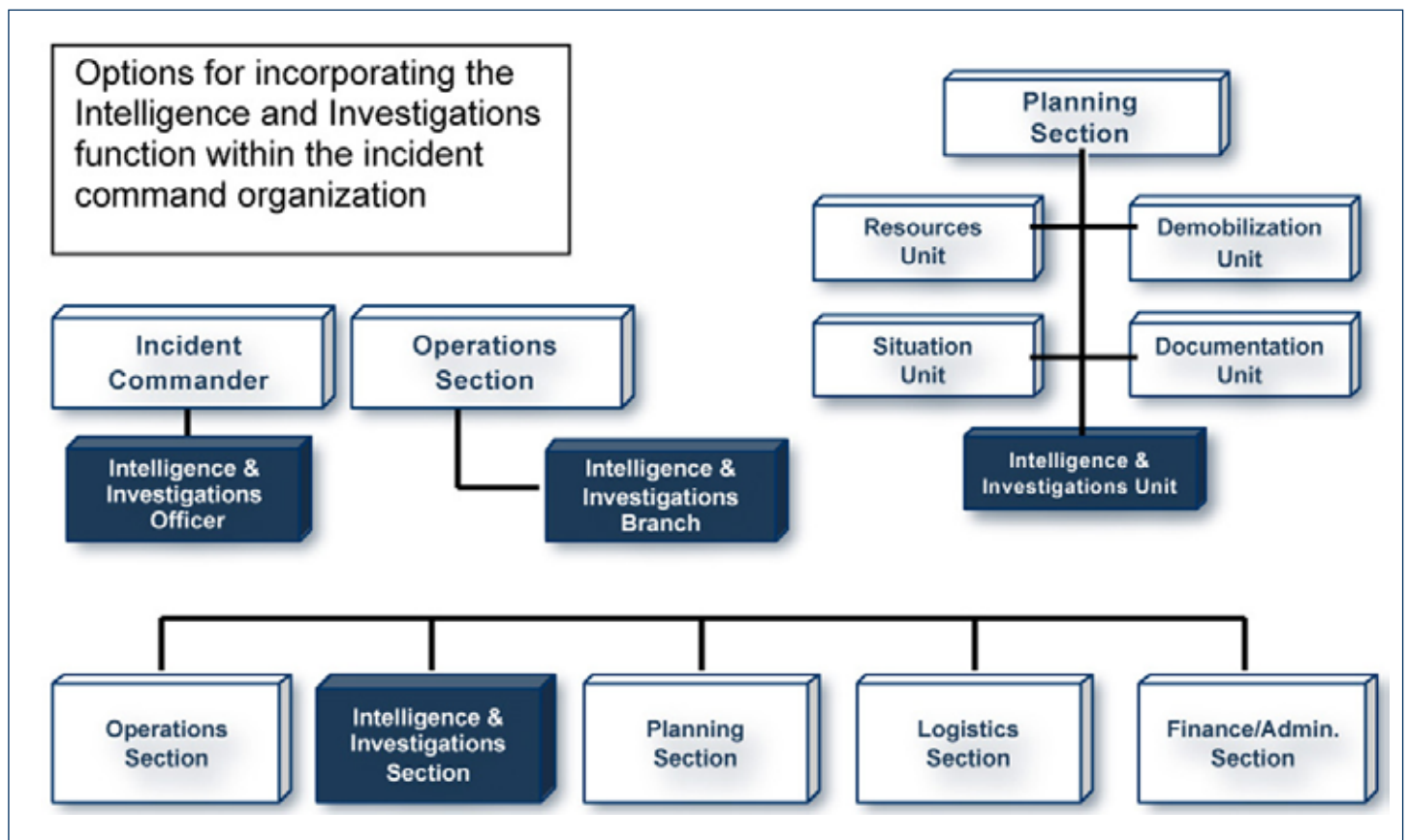
### The Highest Priority: Saving Lives

Fortunately, incident-response priorities never change. Those priorities will always remain: (1) The safety of human life; (2) Stabilization of the incident scene; and (3) Preservation of the on-scene property and other material resources and assets. Focusing on those priorities, in that order, provides a consistent baseline that planners and incident commanders are able to use in establishing their decision-making guidelines. However, the strategies and subsequent tactical decisions derived from those priorities will almost assuredly be based on the identified incident conditions – including a determination of whether the obvious hazards are the sole concern or if other risks also must be considered and additional precautions implemented. Clearly, ensuring life safety must remain the highest priority in any case.

Incident response strategies will be developed based on whether the circumstances are incidental (accidental), and/or whether the incident was intentional. Similarly, the operational tactics selected should reflect any concerns about additional – particularly intentional – hazards and risks likely to be encountered. For example, the traditional,

and time-honored, emergency responder mindset of initiating aggressive intervention operations just as soon as possible must be tempered by a recognition of potential additional hazards or intended cascading events.

Among the other factors that also must rapidly be assessed is determining whether the incident involves simple negligence or willful negligence. Simple negligence typically results from unintentionally omitting or ignoring a step in a process, and that omission results in an undesirable outcome. Willful negligence is generally characterized by situations in which the responsible party intentionally and knowingly disregards important procedures or processes. A key distinction between the two is that willful negligence, if properly documented, is more subject to criminal and/or civil prosecution. For the incident commander at a man-caused incident, this means that the preservation of evidence that can assist in these determinations is of critical importance. For that reason, the strategies and tactics recommended – or mandated – in the planning process may well include the actions needed not only to properly document and preserve evidence but also to establish a valid “custody chain” for later prosecution.



## The Recognition and Growing Importance of I&I

All of these determinations drive the need for relatively new considerations when establishing the command guidelines for a man-caused incident. When the National Incident Management System (NIMS) was conceived in 2003, a conceptual component was added to the core functions of the Incident Command System (ICS). That component was initially titled “Information and Intelligence” but in 2007 was revised to “Intelligence and Investigations” (I&I).

The purpose of the I&I function was, and is, to create the organizational and functional capabilities needed to collect intelligence data and conduct investigations into the cause, origin, and intent of the perpetrator or originator of a man-caused incident. In practice, this means that the incident commander must not only determine what has happened but also who may have caused it and what his or her intent was. The incident command/unified command also must: (a) determine whether man-caused incidents are accidental or intentional; and (b) help assess the potential of such incidents to cause greater risk, harm, or loss.

There are many additional benefits provided by proper and effective use of the I&I function, but the principal value of I&I is usually that it gives the incident command organization an effective tool to support decision-making that is based upon identification of the incident’s cause, intent, and intended outcome.

The I&I function has historically been considered to be “part and parcel” of the planning section. Fundamentally, this was based on the notion that planning must be based on information, or intelligence, gathered for each incident operational period. The NIMS concepts expanded the options for the incident commander (IC) to include the designation of I&I as: (1) a new Command Staff Position; or (2) a discrete branch within the Operations Section; or (3) a separate (fifth) general staff function – along with Operations, Planning, Logistics, and Finance/Administration.

Ultimately, though, the determination of whether the I&I function is needed and in what capacity it will be assigned rests largely with the incident commander. However, under NIMS, the incident commander has several options to choose from, and these will usually be based on the incident factors identified. (The graph accompanying this article

shows the various options available for incorporating the Intelligence and Investigations Function within an incident-command organization.)

## First Answer the Questions, Then Make the Determinations

In summary, when confronted with a man-caused incident, the incident management organization must rapidly make a number of determinations. Prominent among the many questions that must be asked before making those determinations are the following:

1. Is the situation incidental (accidental) or was it intentional?
2. Is there a potential for cascading events or multiple occurrences?
3. If cascading events or multiple dangers do exist, what are they likely to be, and what additional precautions are needed?
4. Who or what caused the incident? (The answer to this question may be of critical importance if criminal or civil prosecution seems likely in the post-incident phase of operations.)
5. Is it necessary to carry out investigative actions, preserve evidence, and establish a valid chain of custody for evidence – and, if so, how will these actions be performed?
6. What changes to current strategies and tactics should be made?
7. What is the most suitable framework within which to incorporate measures for gathering incident intelligence and/or conducting investigations? (Note: The I&I function may initially be established in one configuration but later adjusted to another – if, as, and when necessary.)

In addition to the preceding steps required to establish an effective incident command of any type, officials confronted with a man-caused emergency must assess these factors to determine how to support the command process through establishment of an Intelligence & Investigations function.

---

*Steve Grainer is the chief of IMS programs for the Virginia Department of Fire Programs. He has served Virginia fire and emergency services and emergency management coordination since 1972 in assignments ranging from firefighter to chief officer. As a curriculum developer, content evaluator, and instructor, he currently is developing and managing VDFP programs to enable emergency responders and others to achieve NIMS compliance requirements for incident management.*



# Antidotes: The Care and Cure for “What Ails You”

By Joseph Cahill, EMS



A successful “antidote” program focuses on three principal and closely interrelated factors: (a) supply; (b) training; and (c) security. There are currently many antidote kits that are either commercially available in the industrial community, or in the nation’s chemical weapons arsenals, that can be used to fight the threats posed by accidental or even deliberate spills of hazardous chemicals. However, for various security and “deployment” reasons, those kits can be divided into two groups – those with a significant potential for abuse, and those without.

Although there might be only a slight possibility that medications “without” a significant abuse potential could and/would be diverted by otherwise conscientious staff – “so they can have them available for themselves or their families,” is one plausible reason that has been cited – that would be a relatively limited problem that could usually be reduced, or kept to a minimum, by a rigorous program of frequent inspections, many of them unannounced, and a continuing emphasis on both personal and collective accountability.

Of much greater concern are the medications “with” abuse potential because they must be secured more strenuously than the others, which often translates into additional levels of security – and that means, in turn, that these medications may be less readily available when immediately needed. To consider but one example: A supply of Diazepam (also known as Valium) is and should be an essential component of an effective nerve-agent antidote program. But it is a “Schedule 3” medication with high abuse potential and therefore must be secured – but at the same time be quickly available if the unthinkable happens. If staff members are diverting Diazepam for recreational use, which could seriously impede decision making, the staff members involved must be not only identified but also removed from the patient-care arena before any injuries or even deaths can occur.

*One strategy used to create and maintain a secure antidote program in which the medications needed are still accessible is to require paramedics to inspect, and sign for, a quickly measurable supply of the medications available at the start of each shift – as [they] already do for the Diazepam they carry to treat seizures*

## Frequent Inspections Plus Personal Responsibility

One strategy used to create and maintain a secure antidote program in which the medications needed are still accessible is to require paramedics to inspect, and sign for, a quickly measurable supply of the medications available at the start of each shift – as paramedics already do for the Diazepam they carry to treat seizures. That distribution model has two principal advantages: (a) the medication is inspected at least once or more every day; and (b) each succeeding paramedic is personally responsible for checking the medications turned over by the individual paramedic he or she is relieving. There are two additional points that should be kept in mind, though: (1) If the policy adopted is the same as that used for other medications with abuse potential, there will be at least some additional training required; (2) There also is a possibility that the variety and the bulk of the medications signed for may make this model unwieldy.

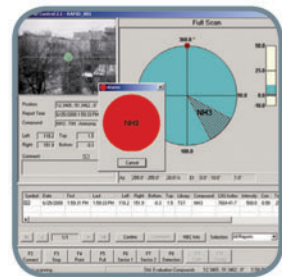
Another likely model is to have a stockpile of various medicines, including Diazepam, that, although kept under tight security, could be made immediately available for transport to the scene of an emergency. This model allows for tighter security because the day-to-day supply would be kept under the control of a very limited number of people. The “stockpile” model also may be impractical, though – particularly in agencies responsible for operations over a relatively large geographic area – because the transport time from the stockpile cache to the emergency scene might be much greater.

The “average” paramedic unit usually carries enough supplies already, including medicines, to treat some if not all types of chemical poisoning. For example, the recommended treatment for hydrofluoric acid usually includes the use of calcium gluconate or calcium chloride, which currently may be carried by paramedics to treat cardiac problems. However, that antidote does no good if

# RAPID

## Stand-off Detector for Atmospheric Pollutants

- For the remote detection of atmospheric pollutants and chemical warfare agents
- Allows for measurements in the spectral wavelength range from 14  $\mu\text{m}$  to 8  $\mu\text{m}$
- Four libraries of chemical compounds, can detect up to several kilometers line-of-sight



+1 (978) 663-3660 x 1418 • [nbc-sales@bdal.com](mailto:nbc-sales@bdal.com) • [www.bruker.com/detection](http://www.bruker.com/detection)

think forward

CBRNE Detection

the paramedics – and/or the physicians who support them – are unaware of all of its possible uses. Again, additional training probably would be needed.

## Protocols, Procedures, And Other Practical Realities

Treatment protocols – i.e., the legal rules and regulations that paramedics must follow when administering medications – must also be specified, in considerable detail, well in advance to not only provide the directions on when and how to use the medications but also to serve as the legal basis for their use. Unfortunately, without sufficient paramedic training related to these treatment protocols, the protocols themselves are useless. Moreover, the medications usually stockpiled to cope with CBRNE (chemical, biological, radiological, nuclear, explosive) attacks or incidents are useless if the responding EMTs and/or other medical staff do not know how to access and administer them.

In short, maintaining security over a supply of antidotes requires much more than simply ensuring that they are not diverted for recreational use. It is at least equally important to

protect not only the specific locations of the various caches involved but also the operational details of the supply procedures used.

Thanks to the already validated assumption that there are forces in the world able and willing to use chemical weapons (and/or industrial chemicals) to attack civilian populations, it is not a far stretch of the imagination to recognize that those same forces would also be willing to attack the individual responders – and material resources, including antidotes – that the nation would and must use to counteract such attacks.

---

*Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. Much in demand as a speaker – he has addressed venues as diverse as the national EMS Today conferences and local volunteer EMS agencies – Cahill also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montfiore Hospital.*

**NH15**  
ESCAPE HOOD

**WE'VE REDUCED THE SIZE,  
NOT THE PROTECTION.**

**AVON**  
PROTECTION

1 888 286 6440  
www.avon-protection.com

© 2011 Avon Protection Systems, Inc.



# The New PLAN: Government Alerts Enter the 21st Century

By Rodrigo (Roddy) Moscoso, Law Enforcement



The Federal Communications Commission (FCC), the Federal Emergency Management Agency (FEMA), and the commercial cellular industry have joined forces to create the nation's first geo-targeted "alert and notification"

warning system for the general public. The new Public Localized Alert Network (PLAN), formerly known as the Commercial Mobile Alert System (CMAS), will take advantage of the latest wireless handheld technology to deliver text alerts to citizens throughout the country, no matter what their exact physical location.

Covering three alert types – Amber, Imminent Threat, and Presidential Messages – compatible cell phones will receive 90-character alerts relating directly to that phone's present location rather than the traditional "opt in" text alerts normally associated with a specific zip code or jurisdiction. Unlike the old Emergency Broadcast System – which would send, for example, a tornado warning across a wide geographic area – PLAN notifications will affect only those within the specific warning area. The result will be a far more efficient system of forwarding alerts to the general public. In other words, alerts will appear on a receiving device only if that device is physically located in the area specifically affected.

The development of the PLAN system is the result of an almost decade-long effort to standardize the ways in which alert messages are formatted, collected, and disseminated. Building on the Common Alerting Protocol (CAP) XML message standard, alerts can be easily exchanged with multiple organizations and systems for redistribution. Using the "geo-aware" CAP standard, alert messages will then be aggregated via FEMA's Integrated Public Alert and Warning System (IPAWS) Open Platform for Emergency Networks (OPEN).

The aforementioned "alphabet soup" of standards and acronyms may seem a bit confusing at first glance, but the new PLAN system is actually a major step forward: Standard messages are being integrated by a standard interface designed specifically for real-time alerting. IPAWS modernizes the Emergency Broadcast System (long-tone warnings), which dates back nearly 50 years and that most users are familiar with. The final piece of the puzzle involves the distribution of alerts, moving them from the limited reaches of radios and television sets to the pockets and purses of individual citizens everywhere.

## April 2012: The Countdown to Full Compatibility

The FCC has worked closely with companies in the cellular wireless industry to ensure their ability to quickly access and distribute alerts from FEMA's OPEN system to their customers' devices. Every 15 seconds, commercial providers – e.g., Sprint, AT&T, and Verizon – will "poll" the OPEN system for alerts. Equally important, the distribution of a specific alert will use a separate networking "channel" for communicating with mobile devices, which users generally agree should not have to compete with the bandwidths reserved for phone calls and internet downloads (which also may be overloaded during a catastrophic event). At present, there are only a few compatible mobile devices that can receive the PLAN messages, but all new devices must be compatible when PLAN goes into effect nationally in April 2012.

The unique partnership between FEMA, the FCC, and the commercial wireless industry should help buffer certain criticisms and accusations of "big brother" monitoring the general public. Because it will be serving only as the aggregator for alerts, FEMA will not have the technological capability to monitor the locations of individual citizens receiving the alerts. Commercial carriers



will access the alerts from FEMA (not the other way around) and then handle the distribution to their customers. In this way, the relationship between citizens and the specific organization(s) “aware” of their current whereabouts is only between those citizens and their chosen commercial providers, not the government.

Moreover, users can choose to “opt-out” of all but Presidential alerts – and will be able to do so directly (via their carriers). Although this solution will not satisfy the fears and suspicions of some users, others may find (and even may expect) some comfort in the fact that their present wireless providers have some sense of where they are. In an emergency situation, these same users may actually appreciate (and hope) that they can be located by their carriers if and when disaster strikes – and/or when they are, perhaps, unconscious and in need of medical assistance.

During a major disaster, natural or manmade, the ability to quickly send a geo-targeted alert may well be a major factor in minimizing the loss of life during the event. The robust and tested infrastructure that serves as the foundation for PLAN therefore represents a significant step forward in achieving this highly desirable objective. The end result should be an automated system that enables a radiological sensor, for example, to transmit an alert that, a few seconds later, will be displayed only on the mobile devices in the area directly affected. In the aftermath of the Fukushima earthquake and tsunami that devastated many areas of Japan earlier this year, the promising impact of the new PLAN technology is eagerly anticipated.

---

*Rodrigo (Roddy) Moscoso currently serves as Communications Manager for the Capital Wireless Information Net (CapWIN) Program at the University of Maryland. Formerly with IBM Business Consulting Services, he has over 15 years of experience supporting large-scale IT implementation projects, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.*

## Manmade Disasters: The Need for Interoperable Communications

*By Omar Alkhalaf, Emergency Management*

Interoperable communication is an important aspect of emergency management and response. In particular, during man-made emergencies, ensuring the availability of effective interoperable communications plans allows for the exchange of critical information in a timely fashion. The responses to the 2003 Station Night Club fire in West Warwick, Rhode Island, and the 2005 London transit bombings would probably have been smoother with stronger, more established interoperability plans. In contrast, the response to the Northern Illinois University (NIU) campus shooting in 2008 provides an excellent example of the benefits of having pre-established interoperable communications plans in place well before they are needed in a real-life incident.

In February 2003, a pyrotechnics display ignited a massive fire during a concert at the Station Night Club in West Warwick. Almost 600 firefighters, police, and emergency medical services personnel from more than 35 state and local agencies responded to the incident. An investigator from the Office of the Medical Examiner (OME) also was dispatched to the scene. Unfortunately, the lack of interoperable communications equipment caused problems with the response effort. The OME investigator’s vehicle was not equipped with a radio or a computer; the investigator was forced, therefore, to rely on his cellular telephone to receive situational-awareness updates while en route. However, because the investigator was using his personal cellular telephone to communicate, he lacked a list of contact numbers of the responders on-site, and this prevented him from receiving the most up-to-date information available. His lack of information about the growing number of casualties, it was later determined, adversely affected the response level.

The 2005 London transit bombings provided another and somewhat different example of the need for interoperable communications systems. Four suicide bombers detonated



explosives on three underground commuter trains and one street bus in central London. The London Ambulance Service (LAS) was unable to communicate efficiently in the aftermath of the bombings, causing a shortage of information on the nature and precise locations of the bomb explosions. As a result, the LAS was initially told, erroneously, that there were seven different incident sites, and resources were deployed to several incorrect locations. The several response problems that resulted were caused primarily by the LAS's dependence on cellular phones as the primary means of communication during incidents. Moreover, the massive influx in cellular traffic strained the system beyond its planned capacity and prevented critical communications from going through.

### **Another Incident, A Different Approach, A Happier Ending**

The Northern Illinois University (NIU) shootings in 2008 serve as a much better example of the benefits of developing, and following, interoperable communications plans. On 14 February 2008, an NIU alumnus shot and killed five students and wounded 18 others. Fortunately, NIU emergency planners had already recognized – after the Columbine shootings in 1999 – the need for interoperable communications plans on their own campus, and one result was that the NIU Department of Police and Public Safety started to carry out a number of planning sessions not only with NIU administrators but also with representatives from state and local response agencies.

The partnerships formed and plans developed as a result of those meetings enabled NIU – and the state and local response agencies – to establish and maintain interoperable communications throughout the initial response phase of the 2008 shootings. Police officers at the scene were able not

only to provide critical information to the responders in the staging area, for example, but also to issue an “all clear” for emergency medical personnel waiting to enter the incident scene after it was declared safe to do so.

The West Warwick nightclub fire and London subway bombings highlight the response difficulties caused by a

lack of interoperable communications when responding to emergencies. In both incidents, a faster response and more effective deployment of resources would undoubtedly have saved many lives if adequate plans had been agreed upon and were in place beforehand.

The NIU incident, on the other hand, shows the benefits of having a detailed and fully developed interoperable communications plan. The lesson for other communities is obvious: By ensuring the development and promulgation of an interoperable communications plan, emergency responders will be in a much better position to gather and disseminate critical information as and when needed at the time of an unforeseen, and unforeseeable, emergency.

*The responses to the 2003 Station Night Club fire in West Warwick, R.I., and the 2005 London transit bombings would probably have been smoother with stronger interoperability plans; in contrast, the response to the Northern Illinois University campus shooting in 2008 provides an excellent example of the benefits of having pre-established interoperable communications plans in place well before they are needed in a real-life incident*

---

*For information on similar incidents and detailed after-action reports, please visit the Lessons Learned Information Sharing Web site at [www.llis.dhs.gov](http://www.llis.dhs.gov).*

---

*Omar Alkhalaf is an outreach and operations analyst for Lessons Learned Information Sharing (LLIS.gov), the U.S. Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best practices, and innovative ideas for the nation's homeland security and emergency management communities. He received a bachelor's degree in Global Affairs with dual concentrations in Global Diplomacy and Governance/Middle East & North Africa Region from George Mason University in Northern Virginia.*



# Changing Trends in Maritime Piracy: A New & Major Threat

By Michael S. Brewer and Scott Brewer, *Transportation*



The recent killings of four American hostages on board their captured yacht, *S/V Quest*, provides a stark indicator to both the commercial maritime sector and the U.S. public at large that maritime piracy is no longer an easily dismissed “cost of doing business,” but a serious impediment to freedom of movement on the seas as well as a deadly crime against humanity. The sheer volume of trade and commerce flowing through high-risk-of-piracy areas such as the Indian Ocean also make maritime piracy a serious U.S. domestic concern. American mariners, imports, exports, and ships all traverse these areas of the world’s oceans regularly, supporting not only international commerce, but also humanitarian efforts such as the World Food Program.

Modern maritime piracy continues to use age-old techniques to serve age-old motivations – grand theft for major economic gain. Piracy as a business model has a long-established and consistently proven track record – seize commercial ships (with or without hostages) and ransom the ships (and/or hostages) for profit.

However, there are some distinctly contemporary concerns and effects that present new and exceedingly complex dangers to U.S. and international communities. Not only does the equipment used today differ considerably from that used in the so-called “Golden Age of Piracy” in the late 17th and early 18th centuries, but the pirate methodologies themselves are “evolving.”

## 2010: The First Step On an Evolutionary Ladder?

In terms of maritime piracy, 2010 was a particularly important year. First, there were more acts of maritime piracy in 2010 than in any previous year of the modern era. Second, the cost of ransoms soared from an average of \$80,500 per incident in 2005 to over \$1 million in 2010. In purely financial terms, this escalation places maritime piracy among the highest-growth “industries” on the planet. In practical terms, maritime piracy has become big business with huge profits. For that reason alone, modern pirates – as well as those who benefit not only economically but also politically from their attacks – will go to great lengths to ensure that nothing changes these new operational realities of maritime life.

There are, though, four critical changes in pirates’ methodology that have emerged in recent years, each of them marking the potential genesis of a still evolving adaptation that carries with

it the ability to thwart and/or otherwise mitigate counter-piracy efforts. Those changes are: (a) using large commercial vessels both as mother ships and as mobile “attack platforms”; (b) using hostages aboard mother ships, and in some cases aboard skiffs or other small vessels, as human shields; (c) forcing hostages to take part in boarding activities; and (d) brokering deals with terrorist organizations, both for financial reasons and for the guaranteed “freedom to operate” without outside interference – particularly from the United States and/or other nations of the Free World.

Each of these tactics provides a greater degree of security to the pirates, mitigating if not completely eliminating potentially effective counter-piracy operations. In addition, each has the potential, if used on a broad scale, to greatly hamper counter-piracy efforts throughout the region and the world. U.S. and allied policy makers often discuss armed security as the first option needed to effectively address the pirate threat, and the public debates the need for the world’s navies to do more. For these reasons, among others, many of the pirates’ tactics are shifting to a new or greater focus on defeating armed responses.

To fully comprehend the ramifications of the four tactical changes mentioned earlier, it is important to first understand two new truths of the modern maritime world: (a) piracy is a profitable endeavor that its participants are willing to risk their lives (and, more often, the lives of others) to preserve; and (b) pirates are typically not radical ideologues, but profit-motivated criminals. In that context and under those circumstances, it becomes clear that pirates’ responses are likely to be both indirect and asymmetrical, and can be achieved primarily by focusing their strengths on the weaknesses of counter-piracy forces.

## Using Captured Merchant Vessels as Attack Platforms

The first way in which pirates apply asymmetric tactics is through “dispersion.” The combined maritime forces operating on counter-piracy missions in the Horn of Africa and Gulf of Aden region number approximately 30 ships at any given time. To cover the greatly expanded areas of the Indian Ocean as well, this force would have to patrol an area exceeding 20 million square miles, which would make the search akin to looking for the proverbial needle in a haystack. In short, by extending their range and operating across a much broader

# CHEMPRO

Handheld Chemical Detector **100i**

The ChemPro100i is a handheld gas & vapor detector for the field detection and classification of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). The ChemPro100i can be used daily in "normal" HazMat and for the less common CWA incident.

- Designed for the rigors of military CWA detection
- Versatile enough for sniffing TICs in daily HazMat operations
- Easy to use and its non-threatening design won't alarm civilians
- No maintenance costs for 5 years



Environics USA Inc.  
1308 Continental Drive, Suite J  
Abingdon, MD 21009, USA  
tel. +1 410 612 1250  
fax. +1 410 612 1251  
[www.EnvironicsUSA.com](http://www.EnvironicsUSA.com)  
[sales@environicsusa.com](mailto:sales@environicsusa.com)



expanse of ocean, pirates have significantly reduced the risk of interdiction by the world's navies.

In the past 18 months alone, at least five large captured merchant vessels were used as mother ships by pirates. In all of those cases, crew members of the merchant vessels were kept aboard as hostages during the pirates' follow-on operations. Use of these commercial ships extended the operational reach of the pirates to unprecedented distances. Pirate attacks beyond 200 miles offshore were exceedingly rare in 2005, but by 2010 the pirates had extended their effective operational range to nearly 1,500 miles.

The faster and more frequent attacks in recent years – carried out over a vastly expanded operational range – have greatly reduced the risks that pirates face from counter-piracy forces, making the pirates' use of large commercial vessels a trend that is likely to continue.

### **The Use of Hostages as Human Shields**

In addition to capturing a valuable ship and its cargo, pirates have sought to use the ship's crew either for ransom or as human shields. The hostages held aboard ships, in addition to others (passengers and/or crew members) who were disembarked and held captive elsewhere, can help the pirates ward off counter-piracy or rescue operations because the pirates can threaten to immediately execute the hostages (ashore as well as afloat) if and when such operations are launched. In those circumstances, even a "successful" hostage rescue may not be viewed as a complete victory because, for every hostage rescued, other hostages held elsewhere may be killed or punished in other ways. Without diminishing in any respect the heroic efforts of those who have previously rescued captive mariners in such operations, it is now recognized by most maritime nations that the use of violence against pirates carries with it the risk of retribution against hostages ashore (or on other pirate ships) who cannot be rescued at the same time.

In 2010, there was a dramatic spike in the use of hostages as human shields during pirate operations. Large ships are not only easier to spot but also harder for relatively small bands of pirates to control in the event of a counter-piracy boarding by military forces. Largely to mitigate that risk, pirates have elected to keep hostages aboard during their own operations, thus reducing the possibility that a military rescue force would risk harming the hostages by launching an attack against the pirates. The holding of hostages also gives pirates the ability to bargain for supplies, fuel, and safe passage, even as ransom negotiations are ongoing.

Another evolution of this tactic was seen in the case of the crew of the South Korea-owned *F/V Golden Wave*. It was reported in February 2011 that Somali pirates forced some of that ship's 43-member crew to participate in the hijacking and/or raiding of 17 other vessels – picked off one at a time. One *Golden Wave* crew member later said that the hostages were given three choices: (a) persuading the ship's owner(s) to pay a \$6 million ransom; (b) having the ship's captain beheaded; and/or (c) participating in the raids on the other ships.

The pirates' use of this tactic obviously presents yet another difficulty to counter-piracy operations, because armed security teams might very easily mistake, for pirate raiders, the hostages being forced to raid client vessels. Although the February 2011 incident was the first report of pirates using such a tactic, use of that option clearly reduces the pirates' own personal and collective risks when attacking commercial ships protected by well-armed security teams.

### **Piracy's Links to Terrorism – The Emperor's New Clothes**

Although some analysts downplay the possibility of tangible links between Somali piracy and the spread of radical Islamic terrorism in Somalia, top secret intelligence reports leaked to the press over three years ago clearly indicate that such links of convenience do exist – and are growing in magnitude. Negotiations between various pirate groups and the Somalia-based al Qaeda-affiliated al-Shabaab group are and have been commonplace. In areas such as Harardhere, on the central coast of Somalia – where al-Shabaab has, for most practical purposes, relative control of the countryside – the terrorist negotiators often demand 20 percent or more of the ransoms in exchange for allowing the pirate groups to operate freely in the offshore waters.

The pirates also benefit when al-Shabaab fighters keep government forces occupied or at bay. According to a December 2009 report by Stewart Bell in Canada's *National Post*, deals had been made earlier that year whereby al-Shabaab would train pirates in the use of weapons, in return for which pirates would give al-Shabaab a share of their plunder and ransoms. How many similar deals have been made is not certain, but the end result is that, willingly or not, pirate groups now contribute hundreds of thousands if not millions of dollars annually to terrorist organizations – and by doing so are not only permitted but frequently assisted by the terrorists, in various ways, in their maritime piracy operations.

Although the piracy/terrorism relationship may not yet be systemic, cooperation occurs at several different levels, and



through a host of separate channels. It is known, for example, that pirate fundraisers and sponsors often share links with al-Shabaab backers. Indicators of regular negotiations between these bankrollers and al-Shabaab terrorists can be seen in operations almost anywhere in the world in which pirate operating bases and terrorist offensives overlap – which is exactly what happened in February 2011 when al-Shabaab extremists “arrested” four pirate leaders in order to “negotiate” a richer share of pirate ransoms.

The complexities of the political as well as financial relationships between the two groups suggest, moreover, that the pirate/terrorist relationship is one that neither can terminate easily. That difficult situation makes clear what many experts have long suspected – namely, that there is in fact a close working relationship, for business purposes or otherwise, between various pirate groups and al-Shabaab. That relationship is a clear strategic threat to U.S. and international interests because it represents one of the most important illicit revenue streams to the al Qaeda-affiliated terrorist network. Moreover, as the piracy/terrorism relationship grows, so does the degree of danger posed to those same U.S. and allied interests.

### **Proactive Measures Needed to Seize Initiative**

The growing piracy problem posed by Somali pirates to the world’s maritime commerce begs for a solution. Commercial shippers have searched for years for an effective, long-term, purpose-built, ship-level, self-defense capability. The possession and use of such a capability would significantly augment the protection currently offered by naval forces of several nations, which operate under different rules of engagement and with different means at their disposal, but share a common end goal.

It is generally agreed that the key to meeting and defeating the clear and present danger posed by modern piracy would be to ensure that naval and commercial efforts to thwart pirate attacks mutually support one another. At the tactical level, this would require that ship-based anti-piracy operations be fully integrated through development and use of: (a) a cohesive intelligence capability that can communicate both with military forces and with commercial shippers; (b) ship-based defensive measures built upon a layered or “concentric” model; and (c) the application of new and/or upgraded technology to facilitate much more rapid responses during a piracy incident. The same integrated capabilities also would address the “before, during, and after” phases of counter-piracy operations: predictive analytics, deterrence and defense, ransom negotiations, and the management and use of critical-incident tools and services.

Groups such as the United Nations International Maritime Organization’s Maritime Security Council, headquartered in London, and the U.S.-based internet service Global Incident Tracker, among others, would act as the principal information dissemination centers for the collective knowledge of the shipping industry and open-source government releases, as well as specialized predictive analytical products designed to warn of specific piracy threats.

In the private sector, insurance markets would work in tandem with anti-piracy equipment manufacturers to incentivize the use of their products throughout the shipping industry, thereby not only reducing the risk to the insurers but also decreasing the number and amounts of payouts. The equipment manufacturers themselves would design and build more effective defensive systems to work in tandem with other systems across the spectrum of lethal and non-lethal systems already operational. The newer systems also would incorporate the newest state-of-the-art technologies to help the world’s navies in their responses to critical incidents. Each facet of this cooperative effort would, in short, provide an added degree of protection – and each would complement the others in both form and function.

Like the current and ongoing evolutions in pirate tactics, the new solutions to piracy must constantly evolve to not merely overtake but actually outpace the problems threatening maritime commerce in the 21st century. To begin with, the pirates’ new operational environment must be both directly and adversely affected so that evolutionary adaptations work for, rather than against, the world’s counter-piracy forces and humanitarian as well as commercial interests. Cooperation between and among the world’s military, commercial, and private sectors is needed now more than ever before. Such cooperation has too often been lacking in the past, but its transformation into a positive force for good also can be seen as a necessary evolution.

---

*Michael S. Brewer (pictured) is the CEO and Co-Founder of International Maritime Security Corporation (IMSC), a service-disabled, veteran-owned small business built upon the principle of protecting ships, their cargo, and, most importantly, their crews from pirate and terrorist threats. He has served as a Special Operations soldier in the United States Army, and has been a subject matter expert on terrorism and piracy for numerous civilian firms and government agencies over the past 13 years.*

*Scott Brewer is the President and Co-Founder of International Maritime Security Corporation as well as a lifelong blue water sailor. With service in the U.S. Army, as well as subject matter expertise on terrorism and piracy, he has been consulted by senior policy makers and industry leaders for solutions to the world’s most pressing maritime security issues.*

*Lawrence O’Connell, Mark Gillespie, and Brad Garrison, all of IMSC, also contributed to the writing of this report.*

# California, Nevada, Texas, and New Jersey

By Adam McLaughlin, State Homeland News



## **California** **Conducts Major Exercise in** **Mitigation of Catastrophic Floods**

A statewide flood in California has dire implications for all residents, which is why the state's efforts to protect the Sacramento-San Joaquin Delta levee system are the key to avoiding a major catastrophe.

That is the principal reason that several state agencies, 21 counties, and more than 5,000 state and local first responders from communities throughout California participated, willingly and vigorously, in California's seventh Golden Guardian exercise, 17-19 May, to practice the collaborative tests, drills, and operations required to mitigate a potentially disastrous incident, or incidents, in the critical delta.

The delta itself covers 700 square miles and consists primarily of a patchwork of nearly 60 islands and tracts, plus numerous sloughs and channels. A levee break could be catastrophic to the state, leaving millions without drinking water and contaminating the entire system.

"We have eight critical islands in the delta," said Michael Miller, spokesman for the California Department of Water Resources, at a staging site in the middle of the delta on May 18. "If we lose these islands, there's a chance we would have saltwater intrusion that would come in to the center of the delta, which could cause a cessation of pumping of water for up to 25 million people and 3.5 million acres of agricultural land.

"If any of these levees break," he continued, "these whole islands flood because most of these eight critical islands are below sea level and, anytime you have a levee break, the whole island has to flood in order for the land to equalize before we can actually start preparing the levee and putting in rocks. And then we have to pump it out."

Even as he spoke, California Conservation Corps members were filling sandbags nearby to hold down a tarp on one of the levees – which is but one example of some of the numerous steps that would be required to mitigate seepage and/or instability on a flooding island.

The state already has stockpiled virtual mountains of supplies, such as rock materials and sandbags, in warehouses positioned in several strategic locations around the delta for easy and quick access. "Stockpiled material allows us to decrease flood response time so we can deal with problems when they're small, before they get big," Miller commented.

The state's Department of Water Resources partnered with the California Emergency Management Agency (Cal EMA) and other agencies in the effort to train all participants in the Golden Gate exercise so thoroughly that they already know their responsibilities before having to deploy "if and when."

"The purpose of the exercises is really to ensure that people are on top of their game," said Mike Dayton, acting secretary of Cal EMA. "There is turnover in state government just like in local government, so it's really important to exercise these processes so people can respond quickly and the relationships are built up ahead of time."

## **Nevada** **Las Vegas Fusion Center Serves** **As Model for Public-Private Collaboration**

Each year, more than 30 million visitors are drawn to Nevada by the luster and glamour traditional in Las Vegas – where, beyond the proverbial "cop on the street," there is also an underlying, and unusually effective, layer of security that has been extremely successful for many years and is the envy of many much larger jurisdictions. For local residents, and businesses, that security starts with the fusion center – i.e., the Southern Nevada Counter-Terrorism Center (SNCTC), an all-hazards 24/7 model for public-private collaboration.

In an unassuming building near McCarran International Airport in Las Vegas, 14 different agencies from a broad spectrum of federal, state, and local government departments work together to achieve one goal: keep residents and tourists safe. The SNCTC is one of three fusion centers in the state, but stands out because it is an all-hours operation that focuses not only on terrorism, but also on all types of crime and a broad spectrum of other hazards and dangers.

Not long after the 9/11 attacks, the U.S. Department of Homeland Security (DHS) recognized the need for creating a broad





A New Five-Part White Paper Series by

# Dr. Craig Vanderwagen

M.D., RADM, USPHS (Retired)

## Implementing the National Health Security Strategy



“The public health mission to protect the health of the public and prevent disease is dependent upon effective and useful logistical systems designed specifically for the purposes of the public health practitioner.”

From August 2006 until July 2009, **Dr. Vanderwagen** was the founding Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services.

The *Implementing the National Health Security Strategy* white paper series, written by the first Assistant Secretary for Preparedness and Response, Dr. Craig Vanderwagen, explores issues that affect the success of the public health practitioner in meeting the needs of the public's health, and by doing so, increasing the resilience of communities and the Nation.

The series takes as its guiding framework, the National Health Security Strategy (NHSS) developed and released by the U.S. Department of Health and Human Services (HHS) in December 2009. The development and public release of this strategic document was directed by Congress as part of the Pandemic and All Hazards Preparedness Act of December 2006. The document is the product of a wide variety of stakeholder discussions and an examination of the real threat issues confronting the Nation. It is a national

document, not just a federal document.

The NHSS has 10 stated strategic goals. This series explores the practical applications of tools that will be major elements in the successful achievement of at least four of them (Integrated/Scalable Health Care Systems; Effective Countermeasure Enterprise; Post Incident Recovery; and Situational Awareness) and add materially to the achievement of at least two others (Science, Evaluation, and Quality Assurance Improvements and Timely and Effective Communications). By bringing focus and effort to these practical considerations the public health practitioner can indeed contribute to the implementation and success of the NHSS which is a portion of our overall national security enterprise.

### White Papers Now Available for Download:

- The Role of Logistics in Public Health Practice
- The Role of Patient Tracking in Public Health Practice
- The Public Health Challenge in Mass Evacuation and Shelter Care

White Paper Series Underwritten by:

**Upp Technology, Inc.**

800.777.6092

upp@upp.com

**innovative  
technology  
solutions**

Download the White Papers today at [upp.com](http://upp.com)



spectrum of fusion centers – there are now 72 of them throughout the country – that could analyze and gather threat-related information from agencies at all levels of government (and from other sources). The goal of the SNCTC, which opened in July 2007, is to “connect the dots” between crimes that might at first seem to be unrelated – but could be precursors to a much larger incident or event – while also working with the community, and the state’s busy tourism industry, to collect information about suspicious activities of any type.

The SNCTC is divided into two sections – intelligence collections; and crime analysis – that, working together, try to determine if suspicious reports and/or criminal activities may be linked to something much greater in scope (the preparations for a terrorist attack, to cite but one example). The intelligence-collections section of the SNCTC uses both overt and covert squads to carry out its missions. Officers are charged with, among other responsibilities, following up on suspicious activity reports, collecting information in the field, carrying out surveillance missions, and developing information sources.

The center’s crime analysis group reviews all types of crime occurring in the valley, ranging from robberies to rapes and murders, to analyze and detect potential trends. The valley is home to about two million people and is protected by, among other agencies, the Henderson Police Department, the North Las Vegas Police Department, the Boulder City Police Department, and the Las Vegas Metropolitan Police Department, as well as a number of other state police and federal agencies.

The reason for the representation of so many departments and agencies in one group is that a police officer who handles a robbery in one jurisdiction may be totally unaware that a similar type of robbery has happened in another area, which is but one of many reasons why 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.”

The SNCTC’s personnel are tasked with, among other duties and responsibilities, looking into and tracking “anything and everything suspicious” that happens in the valley. Anything that to the average person seems like a “typical” or “standard” occurrence – a natural gas leak, for example – can cause an analyst’s internal alarms to sound. “Maybe a natural gas leak is

not just a faulty pipe. ... [It could be] someone planning something,” said Lt. Dennis Domansky of the Las Vegas Metropolitan Police Department. Which is precisely why, he continued, the center “is looking at all those things and doing that analytical work, trying to identify the worst-case scenario.”

## Texas **New Comm Network for Fort Worth/T.C. City Operations Center**

Crisis situations have become much quieter in the Fort Worth/Tarrant County Joint Emergency Operations Center (JEOC) in Texas. But the change is not necessarily due to a lack of incidents. In early June, the center upgraded its entire communications network, allowing users from numerous agencies to monitor radio channels and document events silently through computer workstations.

The problems encountered in managing an ever-increasing noise level was the key factor leading to the overhaul, according to Juan Ortiz, emergency management coordinator with Fort Worth’s Emergency Management Office. The project included high-tech discussions and decisions leading to the use of a radio-over-IP tool, integrated audio-video conferencing, and a Web-based crisis information management system.

“One of the challenges was when you have ... radios at the workstations, you have a competition of audio,” Ortiz said. “Part of our solution was to bring that audio to the ... [computer] and let users decide what they want to listen to.”

JEOC officials opted for RadioConnect for Sametime – a social software tool from IBM and UnifiedEdge that allows operators to use headsets to listen to several channels at a computer. Ortiz said the tool cost roughly \$230,000, a price tag that includes costs related to some components of the infrastructure, such as the new or upgraded antennas and cables that were installed. The computer-based radio monitoring tool also gives users the ability to instant message with others on the system, opening up an expanded variety of communication options during a crisis situation. In addition, the radio-over-IP technology allows operators to identify the actual person communicating, his or her rank, and other details not previously discernible when monitoring chatter on a radio.

Although the individual technologies being used at the JEOC are not new, the combined use of them in difficult situations is not yet widespread among emergency operations centers,

according to Ortiz. Caleb Barlow, IBM's director of unified communications and collaboration, agrees – and pointed out that, although some fire and police departments might use one or two of these technologies in crisis situations, the Fort Worth/Tarrant County JEOC is, to the best of his knowledge, the only public safety initiative that has combined them in one system.

“The concept here is simple ... and there are bits and pieces of this [technology] that have been around for a while,” Barlow said. “But this project looked at how to operate across the board. Half of that is the technology – but the other half that is just as impressive are the logistics, politics, and standardization that the city rolled out across all these. That is a huge accomplishment.”

## **New Jersey** **Transit Riders to ‘Text Against Terror’**

Mass transit riders who see suspicious items will be able to send text alerts to law enforcement agencies under a plan unveiled by NJ Transit one week ago today.

The new “Text Against Terror” initiative was announced as the newest homeland security measure for the system on Wednesday, 8 June, during the transit agency’s board meeting. The initiative will allow customers to text reports to 65873 if passengers do not want to call the existing terror hotline (1-888-TIPS-NJT).

“Our customers and employees are our first line of defense in the war against terror,” NJ Transit Executive Director James Weinstein commented in his presentation to the board.

The texting campaign, funded with a grant from the U.S. Department of Homeland Security, is one of the first of its kind for a U.S. transit system, according to NJ Transit Police Chief Christopher Trucillo. NJ Transit, the nation’s third largest mass-transit system, carries about a million passengers daily during the normal work week.

Trucillo briefed board members on his department’s terrorism initiatives, which include not only increasing the police and canine unit presence at stations following the death of Osama bin Laden but also, and probably of greater importance in the long term, establishing a counterterrorism unit in the department. He said the duties assigned to the counterterrorism unit include working to develop the intelligence information needed to identify potential threats to the transit system.

Trucillo also noted that his department also is working with local, county, and state police officials on terrorism prevention, and has an officer assigned to the FBI’s terrorism task force. The emphasis on working more closely with other agencies “is about partnerships,” he said. “No agency can do it alone.”

The announcement of the texting program comes less than a month after NJ Transit police responded to: (a) the discovery of a suspicious package on a Raritan Valley Line train in Cranford; and (b) a bomb scare at the Chatham train station. Neither of those incidents, as it turned out, involved an actual explosive device.

During a press availability following the meeting, Trucillo said that his deputy chief had recently met with Cranford law-enforcement officials to discuss the “suspicious package” incident and plan for the future. That meeting, he noted, is but one of an extended series of meetings his staff has been holding with local police officials in the New Jersey communities with NJ Transit stations.

His police officers also have been conducting an “outreach” operation, to businesses in a line of sight of all train stations, Trucillo said, to remind them to call the police if there are any unresolved issues or problems to be discussed. He said that over 5,000 businesses have already been visited by members of his department.

Trucillo used his presentation to the board to focus attention on the department’s equally important 2001 crime-fighting activities, and announced that, as of early June, crime in the transit system had decreased by just over 25 percent compared to the same period last year. He also showcased the department’s canine unit by the imaginative use of a bomb-sniffing dog to demonstrate how to find a potential bomb in a bag.

---

*Adam McLaughlin, CEM, MS, MPA, is the operations manager for Elizabethtown Gas, an AGL Resources Company that delivers service to approximately 273,000 residential, business, and industrial natural gas customers in New Jersey. He previously served, for over six years, as the manager of emergency readiness, Office of Emergency Management of the Port Authority of New York & New Jersey. His responsibilities in that post included the development and coordination of Port Authority interagency all-hazard plans, and the design and development of emergency preparedness exercises. Prior to assuming the Port Authority post, he served in the Army for 10 years as an infantry and military intelligence officer; he is a combat veteran of Afghanistan.*

Global Forum For Leadership

# FRI 2011

FIRE-RESCUE INTERNATIONAL



GEORGIA WORLD CONGRESS CENTER • ATLANTA, GEORGIA  
AUGUST 24 - 27, 2011 • EXHIBITS: AUGUST 26 - 27, 2011



## CHANGE IS HAPPENING— EXPERIENCE THE DIFFERENCE!



Using your feedback, we're making changes that provide greater networking opportunities and an enhanced FRI experience. **NEW FOR 2011:**

- **INTERACTIVE SESSIONS** with audience response
- **ACCESS TO EXPERTS** in the New Resource Bar
- **VIP EXPO TOURS** by product category
- **EDUCATION SEMINARS** on the Expo Floor
- **GENERAL SESSIONS** have moved to Friday & Saturday



Plus, check out the FRI podcast series and follow us on Twitter for the latest conference updates.



Powered by the IAFC



# WWW.IAFC.ORG/FRI