domesticpreparedness.com

DomPrep Journal

Monthly Edition

US $100 Annual

Volume IV, Issue 8 August 2008

A Lethal Dose Rate?

A Closer Look At Radiation

For more details, visit:
DomesticPreparedness.com
Since 1998, Integrating Professional Communities of Homeland Security

Are you doing all you can to secure your most valued health-care assets from radiation contamination?

In today's health care environment, safety and security are essential. Thermo Fisher Scientific detection systems make it simple to protect your facility while providing peace of mind for employees and the public.

Strategically placed radiation detectors identify dangerous, non-medical radiation sources, combined with video and the Thermo Scientific ViewPoint™ Enterprise system to quickly isolate non-medical radiation sources. The real-time monitoring and notification capability of the ViewPoint™ system can help prevent the long-term closure of your facility (and subsequent revenue loss) for efforts to decontaminate critical areas and equipment.

Integrated Solutions

Thermo Scientific radiation detectors and systems provide the full coverage needed by today's health care facilities managers.

For more information on the ViewPoint™ Enterprise and the full line of Thermo Fisher Scientific radiation detectors:

+1 (800) 274-4212
www.thermo.com/medrad

Moving science forward

Thermo SCIENTIFIC

Part of Thermo Fisher Scientific

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
Managing Editor & Interviews
jmorton@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Sharon Stovall
Web Content Coordinator
sstovall@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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.

IMR GROUP

Editor's Notes

By James D. Hessman, Editor in Chief

Seven years minus two weeks, but still counting. That is how long the American people have been looking back at the 11 September 2001 terrorist attacks against the United States and asking themselves if similar attacks could happen again.

There are two answers to that question. The short, honest, but not quite complete answer is "Yes." But "new" attacks, if and when – many experts in this field say "*not* if, but *when*" – would probably not be the same type of attacks (converting passenger aircraft into huge guided missiles), but on the other hand could be immensely more deadly. That would be particularly true of attacks using nuclear, biological, radiological, and/or chemical weapons.

The use of nuclear weapons or devices cannot be discounted, but most if not quite all counterterrorism experts say that biological, radiological, or chemical weapons are much more likely to be the next terrorist weapons of choice. Such weapons are easier to build (or purchase), to hide, to transport, and to detonate. They also would be less costly.

This printable issue of *DPJ* takes a close look not only at some of those weapons and the dangers they pose to the American people but also at some of the many preventive and remedial programs that have been developed by the federal government – working in close cooperation with state, local, and private-sector partners – to detect such weapons, deter terrorists from using them, and in a worst-case scenario deal with the destructive aftermath.

Glen Rudner begins the discussion with a report on the new generation of radiation dosimeters – sturdier, easier to use, and more accurate than their predecessors – now entering the inventory. Theodore Tully follows up with a look at hospital decontamination requirements, the high cost of always being prepared, and a number of legislative and regulatory complications that also must be considered. Joseph Trindal adds a complementary review of new federal requirements governing the development and implementation of Chemical Facility Anti-Terrorism Standards. And Judith Kanne reports on two new responder "tool kits" (one for doctors, nurses, and other healthcare providers, one for public-health officials) developed and being distributed by the Centers for Disease Control and Prevention.

Two important related issues also receive expert scrutiny: Rodrigo Moscoso reports on several still-unresolved questions involving the credentialing of first responders; and James Mason points out that state and federal laws regarding the disposition of bodies must still be obeyed – even in the aftermath of mass-casualty incidents.

Not all is doom and gloom, though. As Dr. Neil C. Livingstone points out in his insightful commentary, the war against terrorism has resulted in major advances in "battlefield forensics" – and these new combat capabilities are being passed quickly to the private sector as well.

Rounding out the issue are: (1) A comprehensive, detailed, and forward-looking summary, by Diana Hopkins, of the major advances being made at all levels of government, and in the private sector, in the sharing of intelligence related to terrorism, weapons of mass destruction, and other information of all types (the lack of such sharing was cited by the 9-11 Commission as a major factor contributing to the success of the 2001 terrorist attacks); and (2) States-of-Preparedness reports, by Adam McLaughlin, on initiatives taken by four states (California, Indiana, South Carolina, and Virginia) to better protect their own citizens and otherwise enhance domestic tranquility.

About the Cover: Sergeants Aaron Tinsley (left) and David Power, both of whom are members of the Indiana National Guard's 53rd Civil Support Team, test radiation levels from "Ground Zero" at the Muscatatuck Urban Training Center during the 10 May 2007 Vigilant Guard joint military and civilian training exercise, which simulated the detonation of a nuclear device in a major metropolitan area. (Indiana Army National Guard photo by Sergeant Michael B. Krieg.)

The Knowledge Foundation's 13th International Conference

DETECTION TECHNOLOGIES 2008

New Developments in Identification of Microorganisms & Chemicals

November 13-14, 2008
Phoenix, AZ USA

Conveniently timed with

NanoKAP 2008
Utlizing Nanotechnology for Detection of Toxins and Pathogens
November 12, 2008

KNOWLEDGE FOUNDATION
TECHNOLOGY COMMERCIALIZATION ALLIANCE

www.knowledgefoundation.com

Radiation Detection: Dosimeters Plus Common Sense

By Glen Rudner, Fire/HazMat

The reality of a radiation emergency differs little from that caused by a chemical or biological release – any or all of them are either accidental or intentional. But in either case the emergency-response community is tasked with determining the type, size, and impact that the incident has on the population. Today there are many agencies involved with the development of detection equipment; however, the initial response is often carried out using secondary indications of the hazards – e.g., labels, signs, or placards indicating the possible presence of a hazardous material, the appearance of various medical symptoms in exposed individuals, and/or readings from specialized instruments.

Radiation is colorless, odorless, tasteless, and invisible. The only way to determine whether radioactive material has been involved in an event is to perform *radiological surveys* with specialized equipment. That equipment is designed to assist the responder, in the simplest of terms, in determining how much radiation is present and where it is. It also has, or should have, the capability of indicating how much radiation has been absorbed by the responder. The terms that are most commonly used in these measurements are dose and dose rate. The dose is the total amount of radiation accumulated by the responder or victim during a given period of time. The dose rate is how fast the radiation is traveling.

Many agencies have used current funding streams to purchase quick-response equipment for radiological incidents. Most if not all of these agencies are equipped with and now using dosimeters that are much more technologically accurate and more user-friendly than predecessor systems. Prior to the late 1990s, the most common dosimeter used was the so-called analog pen filament type. The analog radiation dosimeter is cylindrical, and about the size of a pen. It is called, appropriately enough, a pen dosimeter. The readout of the pen dosimeter is displayed by looking through the cylinder, in front of a light source, to see a red hash mark on a scale that marks the exposure. The pen dosimeter is then zeroed with a dosimeter charger.

The emergency responder must determine what appropriate actions to take, basing his/her decisions on the data received from instrumentation at an incident scene. When using radiological instrumentation, a clear understanding of how to calculate dose based upon dose-rate readings from an instrument is important to the safety of the first responders themselves. (Photo courtesy of the Virginia Department of Emergency Management.)

New, Better, More Precise, Easier to Use

Recent advances have led to the introduction of an electronic self-reading dosimeter, which is in the shape and size of a pager. The dosimeter displays the dose in the form of a digital readout and sounds an alarm when the radiation level exceeds the threshold level. Both types of dosimeters are usually clipped to the exterior of the user's clothing. The

pen dosimeters are made to measure in different ranges. Occupational exposure ranges for dosimeters usually measure up to 500 mrem [Milli Roentgen] (5 mSv) [MilliSievert], which exceeds the normal U.S. yearly dose of 360 mrem (3.6 mSv), whereas the newer electronic self-reading dosimeters are auto-scaling – a feature that permits a larger range of measurement as well as greater accuracy.

A more modern-design dosimeter is the thermoluminescent dosimeter (TLD). Although not a direct reading instrument, the TLD plays an important role in the several dose-control issues that develop for responders over a longer period of time. The TLD contains a tiny crystal of lithium fluoride that undergoes cumulative structural changes when it is exposed to ionizing radiation. When heated, the crystal glows, giving off an amount of light proportional to its radiation exposure. This light is observed by an electronic sensor in a readout unit and recorded digitally. After the incident or exposure has ended the TLD is collected and sent to a lab to be read.

Most agencies are equipped with and now using dosimeters that are much more technologically accurate and more user-friendly than predecessor systems

Time and experience have shown that local emergency-response agencies – e.g., fire departments and both EMS and law-enforcement agencies – will play the most important roles in the initial responses to a radiological emergency. The radiological emergency may be accidental – e.g., caused by an accidental release from a nuclear power plant – or intentional (in a terrorist attack). Whatever the cause, federal officials may well have an important role to play in supporting the response at the local level. However, the local response still will be key in determining the course of actions during the crucial early stages of a radiation incident.

Glen D. Rudner is the Hazardous Materials Response Officer for the Virginia Department of Emergency Management; he has been assigned to the Northern Virginia Region for the last nine years. During the past 25 years he has been closely involved in the development, management, and delivery of numerous local, state, federal, and international programs in his areas of expertise for several organizations and public agencies.

New Radiological Tool Kits Available from CDC

By Judith Kanne, Public Health

Using audience research that identified significant knowledge gaps and under-developed skills affecting the ability of clinical and public health professionals to respond to radiological emergencies, the Centers for Disease Control and Prevention (CDC) has produced two new radiological tool kits to address both of these problems. One tool kit is specifically designed for use by physicians, nurses, and emergency-services personnel; the other is designed for use by public health officials. Each of the CDC tool kits includes a variety of education and training materials.

"Just-in-Time training is one of our key DVDs in the clinician kit," said Charles W. Miller, chief of the Radiation Studies Branch of CDC's National Center for Environmental Health, " … [and serves as] a critical component for educating physicians and nurses." The 17-minute DVD, which covers key radiation principles and procedures, includes application demonstrations in several patient-care scenarios that take place within an emergency-service setting.

Clinicians in hospital emergency areas would serve as the first receivers of casualties from a radiological event. Others – e.g., physicians, nurses, laboratory personnel – would report to hospitals in order to assist following a radiological event. At the same time, the public health work force would be called upon both to protect the health of the local community and to allay the public's fear of radiation. Because of the multitude of issues involved in disaster and mass-casualty management situations – particularly those unique to dealing with radiation exposure and contamination – pre-event education and training are imperative for hospital and public health personnel.

A specific example of the materials available in the public health tool kit is a planners' guide on population monitoring. That guide sets forth the process of identifying, screening, and monitoring those people who were (or might have been) exposed to radiation or contamination from radioactive materials. The guide also presents an introduction to population monitoring for public health officials and emergency preparedness planners at both the state and local levels. These materials are currently available, and are free of charge.

For Additional Information:

On the current clinician training tool kit materials, click on: http://emergency.cdc.gov/radiation/clinicians.asp

On the current public health training materials, click on: http://emergency.cdc.gov/radiation/publichealth.asp

To order tool kits: please email cdcinfo@cdc.gov, providing specific information on the materials needed.

Following are some additional resources for education and training:

The Department of Health and Human Services (HHS) website: http://www.remm.nlm.gov/

The Radiation Emergency Assistance Center/Training Site (REAC/TS) website: http://orise.orau.gov/reacts/

The Food and Drug Administration (FDA) website: http://www.fda.gov/cdrh/radhealth/

The Environmental Protection Agency (EPA) website: http://www.epa.gov/radiation/

The Armed Forces Radiobiology Research Institute (AFRRI) website: http://www.afrri.usuhs.mil/

Judith (Judi) L. Kanne has worked at the Centers for Disease Control and Prevention (CDC) as a nurse/health educator/health communication specialist under varied contracts since the early 1990s. She also has worked as a medical writer/editor and as creator of a number of public health presentations and other educational materials. She uses her degrees in nursing and journalism to provide readers with clinically credible health information in an easy-to-understand format. Since 2001, she has focused primarily on emergency communications, and recently worked with CDC's Radiation Studies Branch on clinician-related educational products.

Hospital Decontamination: Many Questions, But Few Answers

By Theodore Tully, Health Systems

One of the most difficult and costly requirements for the nation's hospitals to comply with in the field of emergency preparedness involves the planning for mass-decontamination situations. The Joint Commission recommendations and most state departments of health require that U.S. hospitals be prepared not only for incidents requiring decontamination but also for the protection of patients and staff before, during, and after the decontamination process. These requirements have been widely interpreted as requiring hospitals to be prepared to decontaminate large numbers of patients (mass decontamination) as opposed to the small number of patients that might realistically be expected in most situations.

All hospitals should understand, of course, that some level of decontamination preparedness is needed. An event as simple as a traffic accident could contaminate patients exposed to gasoline fumes and/or diesel fuel. The subsequent "off-gassing" of such chemicals from a patient's clothes, in a confined trauma room or elsewhere in a hospital's emergency department, could have dangerous consequences for patients and staff alike. If patients "self-refer" themselves to a hospital – as happened in the aftermath of the 1995 Sarin gas attack on the Tokyo subway system – prior to decontamination of the scene by healthcare or fire services personnel, the hospital itself is given additional responsibility it did not ask for and may not be prepared for.

National surveys show that U.S. hospitals run the spectrum from "reasonably prepared" to almost totally unprepared when it comes to the level of decontamination they are supposed to be prepared for. Some are trained and equipped to carry out what are called "level B" decontamination procedures, but others are capable only of level-C decontamination – or something less. The principal factors determining what level of decontamination is or should be provided would be the air system and personal protective equipment (PPE) used during decontamination. Level B calls for use of a Self-Contained Breathing Apparatus (SCBA) unit capable of supplying air in a fully encapsulated suit similar to that worn by a municipal hazmat technician. Level C or below would designate a lower level of preparedness – e.g., the use of Positive Air Purification Respirators (PAPRs) and fully hooded suits with no exposed body parts.

The High Cost Of Basic Capabilities

To provide even modified Level C decontamination, however, requires equipment, a water source, a remote location, and appropriately trained staff (quickly available 24 hours a day, however, seven days a week). The proper equipment can range in cost (depending on the number of showers available) from $25,000 for a basic system to a cost in excess of $250,000 for more elaborate systems. The training for staff probably is the most costly budget line, though, and creates a problematic issue for many hospitals – most of which are seeking answers to two important and interrelated questions: (1) How many staff members must be retained/trained to carry out decontamination operations? (2) What is the best way to ensure that those staff members retain their decon skills?

If hospitals want to be able to provide a decontamination team on a 24/7 basis, they may have no choice but to rely on clinical staff at least part of the time. If they do so, however, it will decrease the hospital's ability to use those same staff members to provide medical care for patients. Moreover, if staff members themselves are victims of an incident requiring decontamination it not only would eliminate them as decon staff but also increase the number of patients in need of medical care. If hospitals choose to train non-clinical staff the principal question is whether those staff members will be able to recognize the signs and symptoms of health problems so that treatment can be initiated quickly. The obvious approach, therefore, might well be to have a blend of both clinical and non-clinical staff.

Hospitals must for that reason not only organize training to the level of decontamination they want and need, but also realize that skill and refresher training needs should be scheduled and practiced on a regular basis. The PPE gear available must be relied on by staff and they will have to train while wearing that gear, in all types of climates. Not until then can questions about the number of staff in need of training be answered with any reasonable degree of accuracy.

Six People, Ninety Minutes, In the Middle of the Night

Most small "two-lane" decontamination systems usually need a minimum of six staff members to operate: Two on the "hot" or entrance side, two on the "cold" or exit side, and two available to be suited up if a problem develops or a need for a rescue develops. These six can possibly operate (depending on the environment) from 30 to 60 minutes in PPE gear before they have to be replaced. The arithmetic is simple: Three six-member teams will provide only 90 to 180 minutes of staff time to decontaminate patients. The upper total just barely reaches

SafetyTech™
International, Inc.
A Subsidiary of TVI Corporation

Powered Air Solutions for Decontamination

The lightweight **FlexAir**™ powered air respirator can be used with two HEPA filters or converted to three chemical cartridges.

- designed for first receivers
- dedicated low flow and low battery alarms
- eliminates fit testing
- blower converts to 2 HEPA's for pandemic with a new light weight Tyvek™ hood

SafetyTech International, Inc.
5703 Industry Lane
Frederick, MD 21704
Toll free: 1-888-744-6462
Direct: 301-624-5600
sales@safetytechint.com
www.safetytechint.com

the 180 minutes usually targeted for a mass-decontamination operation. From a management point of view, this means that – at 2:00 a.m., perhaps – a relatively small community hospital needs to have a system in which 18 knowledgeable and well trained staff members will be consistently available to effectively and safely respond to a decontamination incident.

Another important question facing decision making officials: What should a hospital do to prepare for mass-decontamination events? Here it should be noted that most of the nation's hospitals usually are involved only a few times a year in relatively small decontamination events – i.e., events in which one, two, or a handful of patients need decontamination. In that context, mass decontamination for a hospital can be conservatively put in the same hazard class as the proverbial "50-year storm" – and, depending on the hospital's location, even that rare situation might be a worst-case scenario.

Such events can and do happen, though. And when one does happen, it almost always will take help to deal with it, and patients may die in even a best-case situation. The question that the nation's hospitals need to ask themselves, therefore, is whether they are any better prepared to deal with these events than they were prior to 9/11, given the equipment and training they have purchased – or do they simply accept the fact that they are doing "something" to prepare for this type of event, and that something is better than nothing?

Greater Awareness But Lower Funding Levels

There is an increasing awareness at all levels of government that most U.S. hospitals are still not fully prepared to deal with a mass-decontamination situation. Decreases in funding are putting decontamination requirements under scrutiny by hospital emergency planners as well. Answers are hard to come by, but there seems to be general agreement that, if nothing else, all U.S. hospitals should at least have the ability to safely decontaminate a small number of victims, if only to ensure that those victims do not contaminate the hospital itself and/or the hospital staff.

The proper equipment can range in cost (depending on the number of showers available) from $25,000 for a basic system to in excess of $250,000 for more elaborate systems

Most disaster victims can be decontaminated simply by disrobing them and requiring them to go through a thorough washdown process. Local fire departments can be relied on in most scenarios if the number of victims is too large for a hospital to manage on its own. The biggest concern here, probably, is that the fire departments are likely to be otherwise occupied at the incident scene. The end result could be that dozens of contaminated patients might arrive at a hospital within a very short time frame, and there might not be enough responders available to handle them both safely and effectively.

The training issue alone is so daunting a challenge for hospitals that few can do it safely, and even fewer do it well. Requiring medical staff to wear PAPRs or SCBAs can injure staff if it is done wrong and probably would eliminate those staff members from being able to adequately evaluate and/or care for patients. Another important question for hospitals to consider is this: If patients are so contaminated that they are not able to decontaminate themselves, will those patients even survive? Fortunately, patients who self-refer to a hospital are probably not the ones in the greatest need of high-level decontamination – and for that reason probably *could* decontaminate themselves. Hospitals must ask themselves, therefore, if they are better served: (a) by training with fire-service or hazmat teams to assist them in decontamination; (b) by setting up systems that permit self-presenting patients to decontaminate themselves; and/or (c) by spending time to train staff on awareness – and, perhaps, by counting on the effective decontamination of perhaps only one to five patients (a much higher probability than a mass-decontamination event).

Because of the reduced funding now available to hospitals and the increasing demands of emergency preparedness, hospitals have to make smart choices on what they can afford to do. Which leads to a final question: If it is virtually impossible for most hospitals to prepare for a mass-casualty event, involving dozens of contaminated victims, that may never happen in 50 years – and, when it does occur, find that not enough staff is adequately trained or equipped to handle it – then why do hospitals still insist on spending money and allocating valuable staff time on such unlikely possibilities?

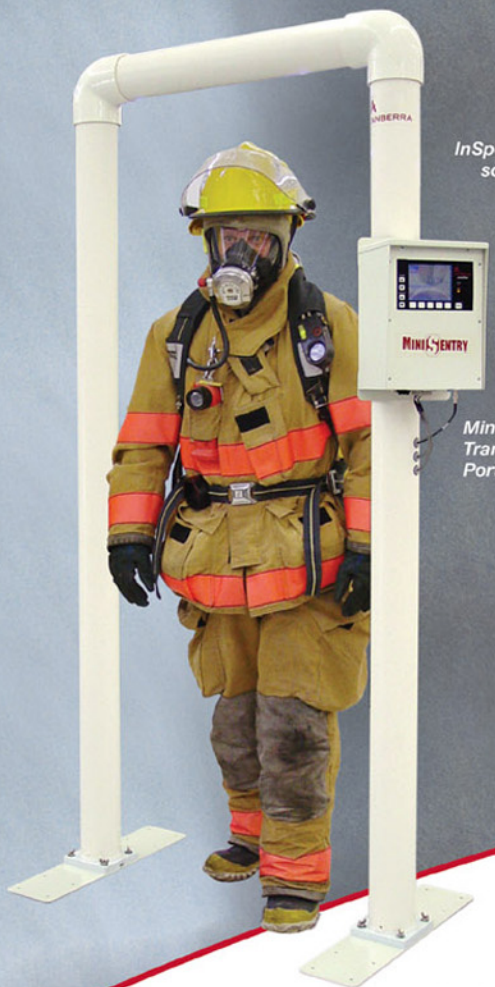
Theodore Tully has been director of Trauma and Emergency Services at the Westchester Medical Center (WMC) in Westchester County, N.Y., since 1994. Prior to assuming that post he served as a police paramedic/detective and as the Westchester County EMS (emergency medical services) coordinator. He also helped create and administer the WMC Regional Resource Center, which is responsible for coordinating the emergency plans of 32 hospitals in the greater Westchester County area.

Your One Source for Radiological Incident Response

UltraRadiac Personal Radiation Monitor

Radiagem Kit for surveying

InSpector 1000 for source location and nuclide identification



MiniSentry Transportable Portal Monitor

In the event of a radiological terror attack or radiation accident, emergency responders need the very best tools.

With the CANBERRA UltraRadiac first responders get fast responding, ultra rugged radiation monitoring. The large display is easy to read — even through masks — and audible, visual and vibrating alarms ensure the first responder always knows the hazard level at his/her own location.

As the situation unfolds, emergency responders need to control and contain contamination. Deploy a MiniSentry Transportable Portal Monitor in less than 10 minutes to begin screening victims, responders, and the public — keeping contaminated material from leaving the scene. Then use ergonomically designed Radiagem survey kits and InSpector 1000 radiation identifiers to quickly locate and identify contamination for removal — minimizing the radiation exposure of both victims and responders.

Best equipment solves only part of the problem. CANBERRA also offers training courses designed specifically for the first responder — free of technical jargon and focused on the practical aspects of first response to incidents and attacks.

Prepare now!
Call CANBERRA today or visit our web site!

www.canberra-hs.com

Canberra Industries, Inc.
800 Research Parkway – Meriden, CT 06450 U.S.A.
Tel: (203) 238-2351 – Toll free: 1-800-243-4422
Fax: (203) 235-1347

CANBERRA

CANBERRA Industries, Inc. is an AREVA company. The AREVA Group, worldwide leader in nuclear power.

First Responder Credentialing: Still a Secondary Priority

By Rodrigo (Roddy) Moscoso, Law Enforcement

As the October 2008 deadline looms for implementation of Homeland Security Presidential Directive 12 (HSPD-12), which requires federal agencies to issue new "smart" identification cards to their employees, many agencies are now working tirelessly to comply with that mandate. So-called "Smart Cards" – which incorporate photos, biometric data (fingerprints), a personal identification number, and individual access rights – are designed both to facilitate secure access to buildings and computer networks and to create a standard government-wide mechanism for identity verification and management.

Complementing this effort, several state and local public safety agencies have piloted the use of First Responder Authentication Credentials (FRAC) ID cards, which are designed to be used in the field by incident commanders to quickly identify responders at the scene of an incident. The FRAC cards interoperate with the HSPD-12 infrastructure, enabling authorized personnel across all levels of government to support an incident response.

The need for more effective credentialing was one of the principal lessons learned during the response to the 11 September 2001 terrorist attack on the Pentagon. Immediately after the attack, first responders from numerous federal, state, and local agencies converged on the incident scene to assist – and encountered several credentialing-related problems. Because of the intensity of the attack and the widespread havoc that followed, most of the responders who reported to the scene – either on their own or as members of a team – were allowed entry without restriction. However, an unauthorized person *could* have gained access to the scene, it later was realized, and might even have driven away with a fire truck.

Difficulties, Complications, And Other Problems

At certain other checkpoints, though, legitimate local, state, and federal responders were denied access to the scene. Another quickly noticed complication was that the incident commanders on the scene were frequently unaware of the specific skills and abilities of the many responders

at the scene from other agencies, and that lack of background information made the efficient use of personnel considerably more difficult.

In March 2007, Arlington County, Virginia – which has incident command responsibility for the Pentagon – became the first agency to deploy FRAC cards, issuing them to 1,400 of its own emergency service workers. Those cards, paid for by a $750,000 Virginia state grant, were intended to be used to test a new common infrastructure for field-level credentialing and identity verification that had been developed for use by local, state, and federal agencies responding to an incident scene in the greater Washington, D.C., area.

Although the FRAC cards have successfully demonstrated the potential capability of HSPD-12 systems, their relatively high cost remains what is perhaps the largest obstacle to full implementation of the HSPD-12 directive. In today's economic environment, many state and local agencies simply do not have the funding necessary to acquire and maintain a FRAC system of their own. In a time of frequent budget cuts, FRAC represents what many officials consider to be an unfunded mandate imposed by the federal government on state and local agencies. In Arlington County, for example, because of funding constraints, no FRAC cards have been issued to new employees since March 2007.

Operational Concerns And Both Good and Bad News

There also are some operational concerns blocking full implementation. A firefighter arriving at an incident scene in full "turnout gear," for example, is unlikely to be able to present a FRAC card quickly or easily at a control point. Moreover, private and commercial wireless (and wired) network access may be interrupted during a significant incident, making real-time identity verification extremely difficult if not impossible.

The good news is that efforts to demonstrate FRAC capabilities have resulted in updates to many regional personnel-management systems that have facilitated low-tech solutions to the problems of identity verification, particularly in response to field incidents. Although not as efficient as quickly swiping a card through an electronic reader, the use by incident commanders of up-to-date lists (even in hard copy form) of emergency personnel and their skill sets could go a long way toward avoiding the problems experienced at the Pentagon following the 11 September attack.

Clearly, much work remains to be done to streamline identity management and verification throughout the nation's public safety community. Not quite seven years after the 9/11 attacks, many command-level responders still carry with them more than a half dozen of the ID cards needed to gain access to incident scenes, high-security facilities, and various computer and communications networks. The development and distribution of a single totally secure identification card remains an important goal, therefore, but hard deadlines will not necessarily ensure success, even among and within the federal agencies required to both set and implement the deadlines mandated by HSPD-12. As of June 2008, to consider but one example, the Department of Justice (DOJ) had issued 1,014 smart cards to its employees and contractors – leaving only 105,723 to go by October 31.

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.

Dead Reckoning: EMS, Death, and Resource Management

By James Mason, EMS

"Unresponsive to stimulus; without breathing or heart beat" – that is a common description used by EMS (emergency medical services) staff in reporting the status of someone believed to be already dead. However, it may still be appropriate to transport that patient by ambulance to a hospital or other healthcare facility because, under some conditions, rapid transport, combined with the medical care provided by EMS responders, may give the patient a chance to survive. In most of the United States an EMS crew can usually determine that a patient is beyond help. However, and despite appearances, that person is sometimes transported as a living patient, and still receiving care.

There is another, larger, pool of patients who share the same general description but are *not* viable and therefore are *not* transported by ambulance. Included in this pool are patients whom EMS starts to treat, but without improvement, and care is then officially terminated.

Laws related to death and dying are generally enacted at the state level, as are the regulations governing EMS care. In the United States, the forensic investigations of death are under the jurisdiction of medical examiners and coroners. A medical examiner, or ME, is a physician, typically a forensic pathologist; a coroner is usually an elected layman.

All states have enacted statutes requiring that certain types of deaths – including all deaths outside of a hospital or hospice setting – be reported to the ME or coroner within the local jurisdiction. This requirement gives those officials the opportunity to determine whether the remains of the deceased can be released to a funeral home or must be taken under their own jurisdiction. In the majority of cases the remains are removed from the scene, by either the ME's or coroner's staff – or by the funeral home staff – after the jurisdictional decision has been made.

> ***In many states, the transportation of human remains in an ambulance, regardless of how recently death might have occurred, is prohibited except under very limited circumstances***

A Short List Of Mandatory Prerequisites

In many states, the transportation of human remains in an ambulance, regardless of how recently death might have occurred, is prohibited except under very limited circumstances. Decisions in this area, though, are considered separately from those governing the transportation of patients, described earlier, who are without a heartbeat or breathing but are still receiving care. The circumstances under which a dead body can be transported often include situations in which the deceased is in public view. New York City's EMS procedures, for example, permit the removal of a patient who has a presumptive diagnosis of death only when the removal is requested by police, the remains are in public view, and the removal also has been approved by the shift supervisor – even then, the removal can be carried out only by an EMT unit.

The decision to transport a presumably dead body is an important issue for EMS staff, because the ambulance carrying the remains not only is lost from the system for the duration of the transfer but also may have to be decontaminated afterward. From an EMS system-management perspective the result is a loss of productivity and for that reason such transport is approved only for reasons that serve the greater community. Another factor to be considered is that paramedic units are not and should not be used for transport duties because such units are not only few in number but also require more equipment and training.

Even a large-scale loss of life at a disaster does not necessarily justify the use of ambulances for removal of the dead. In many large-scale mass-casualty events, of course, many remains or partial remains will have to be moved if only to facilitate the still ongoing rescue work or for other life-saving tasks. In these situations, though, the location and position of the remains should be documented – as fully and as accurately as possible – by trained death investigators, through photographs, site maps, and even GPS (global positioning system) units, to ensure that future investigators will have a clear picture of the accident scene – and of the remains of the victims as they were immediately after death.

James Mason is the pen name used by an EMS professional with over 25 years of service; he has worked as an emergency medical services technician, and as a paramedic, in three of the nation's 100 largest EMS systems, and in others that operate a single unit. In addition, he has served as a medic on a transport jet, as a member of a DMAT team, in an emergency room, and in a hyperbaric chamber. He also has been an instructor at New York City's EMS Academy, at the Philadelphia (Pa.) Fire Academy, and in other world-class training programs. He is the author of over 50 articles in the fields of EMS and emergency management.

The DuoDote™ Auto-Injector (atropine 2.1 mg/0.7 mL and pralidoxime chloride 600 mg/2 mL) is indicated for the treatment of poisoning by organophosphorus nerve agents as well as organophosphorus insecticides.

Important Safety Information

The DuoDote Auto-Injector is intended as an initial treatment of the symptoms of organophosphorus insecticide or nerve agent poisonings; definitive medical care should be sought immediately. The DuoDote Auto-Injector should be administered by Emergency Medical Services personnel who have had adequate training in the recognition and treatment of nerve agent or insecticide intoxication.

Individuals should not rely solely upon agents such as atropine and pralidoxime to provide complete protection from chemical nerve agents and insecticide poisoning. Primary protection against exposure to chemical nerve agents and insecticide poisoning is the wearing of protective garments including masks designed specifically for this use. Evacuation and decontamination procedures should be undertaken as soon as possible. **Medical personnel assisting evacuated victims of nerve agent poisoning should avoid contaminating themselves by exposure to the victim's clothing.**

In the presence of life-threatening poisoning by organophosphorus nerve agents or insecticides, there are no absolute contraindications to the use of the DuoDote Auto-Injector. When symptoms of poisoning are not severe, DuoDote Auto-Injector should be used with extreme caution in people with heart disease, arrhythmias, recent myocardial infarction, severe narrow angle glaucoma, pyloric stenosis, prostatic hypertrophy, significant renal insufficiency, chronic pulmonary disease, or hypersensitivity to any component of the product.

Please see brief summary of full Prescribing Information on adjacent page.

References: 1. DuoDote™ (atropine and pralidoxime chloride injection) Auto-Injector [package insert]. Columbia, MD: Meridian Medical Technologies™, Inc.; 2007. **2.** Agency for Toxic Substances and Disease Registry. Medical Management Guidelines (MMGs) for nerve agents: tabun (GA); sarin (GB); soman (GD); and VX. Available at: http://www.atsdr.cdc.gov/MHMI/mmg166.html. Accessed February 21, 2007. **3.** Holstege CP, Dobmeier SG. Nerve agent toxicity and treatment. *Curr Treat Options Neurol.* 2005;7:91-98. **4.** Data on file. Columbia, MD: Meridian Medical Technologies™, Inc.

DuoDote™ AUTO-INJECTOR
(atropine and pralidoxime chloride injection)

Rx Only
Atropine 2.1 mg/0.7 mL
Pralidoxime Chloride 600 mg/2 mL

Sterile solutions for intramuscular use only

FOR USE IN NERVE AGENT AND INSECTICIDE POISONING ONLY

THE DUODOTE™ AUTO-INJECTOR SHOULD BE ADMINISTERED BY EMERGENCY MEDICAL SERVICES PERSONNEL WHO HAVE HAD ADEQUATE TRAINING IN THE RECOGNITION AND TREATMENT OF NERVE AGENT OR INSECTICIDE INTOXICATION.

INDICATIONS AND USAGE

DuoDote™ Auto-Injector is indicated for the treatment of poisoning by organophosphorus nerve agents as well as organophosphorus insecticides.

DuoDote™ Auto-Injector should be administered by emergency medical services personnel who have had adequate training in the recognition and treatment of nerve agent or insecticide intoxication.

DuoDote™ Auto-Injector is intended as an initial treatment of the symptoms of organophosphorus insecticide or nerve agent poisonings; definitive medical care should be sought immediately.

DuoDote™ Auto-Injector should be administered as soon as symptoms of organophosphorus poisoning appear (eg, usually tearing, excessive oral secretions, sneezing, muscle fasciculations).

CONTRAINDICATIONS

In the presence of life-threatening poisoning by organophosphorus nerve agents or insecticides, there are no absolute contraindications to the use of DuoDote™ Auto-Injector.

WARNINGS

CAUTION! INDIVIDUALS SHOULD NOT RELY SOLELY UPON ATROPINE AND PRALIDOXIME TO PROVIDE COMPLETE PROTECTION FROM CHEMICAL NERVE AGENTS AND INSECTICIDE POISONING.

PRIMARY PROTECTION AGAINST EXPOSURE TO CHEMICAL NERVE AGENTS AND INSECTICIDE POISONING IS THE WEARING OF PROTECTIVE GARMENTS INCLUDING MASKS DESIGNED SPECIFICALLY FOR THIS USE.

EVACUATION AND DECONTAMINATION PROCEDURES SHOULD BE UNDERTAKEN AS SOON AS POSSIBLE. MEDICAL PERSONNEL ASSISTING EVACUATED VICTIMS OF NERVE AGENT POISONING SHOULD AVOID CONTAMINATING THEMSELVES BY EXPOSURE TO THE VICTIM'S CLOTHING.

When symptoms of poisoning are not severe, DuoDote™ Auto-Injector should be used with extreme caution in people with heart disease, arrhythmias, recent myocardial infarction, severe narrow angle glaucoma, pyloric stenosis, prostatic hypertrophy, significant renal insufficiency, chronic pulmonary disease, or hypersensitivity to any component of the product. Organophosphorus nerve agent poisoning often causes bradycardia but can be associated with a heart rate in the low, high, or normal range. Atropine increases heart rate and alleviates the bradycardia. In patients with a recent myocardial infarction and/or severe coronary artery disease, there is a possibility that atropine-induced tachycardia may cause ischemia, extend or initiate myocardial infarcts, and stimulate ventricular ectopy and fibrillation. In patients without cardiac disease, atropine administration is associated with the rare occurrence of ventricular ectopy or ventricular tachycardia. Conventional systemic doses may precipitate acute glaucoma in susceptible individuals, convert partial pyloric stenosis into complete pyloric obstruction, precipitate urinary retention in individuals with prostatic hypertrophy, or cause inspiration of bronchial secretions and formation of dangerous viscid plugs in individuals with chronic lung disease.

More than 1 dose of DuoDote™ Auto-Injector, to a maximum of 3 doses, may be necessary initially when symptoms are severe. **No more than 3 doses should be administered unless definitive medical care (eg, hospitalization, respiratory support) is available.**

Severe difficulty in breathing after organophosphorus poisoning requires artificial respiration in addition to the use of DuoDote™ Auto-Injector.

A potential hazardous effect of atropine is inhibition of sweating, which in a warm environment or with exercise, can lead to hyperthermia and heat injury.

The elderly and children may be more susceptible to the effects of atropine.

PRECAUTIONS

General: The desperate condition of the organophosphorus-poisoned individual will generally mask such minor signs and symptoms of atropine and pralidoxime treatment as have been noted in normal subjects.

Because pralidoxime is excreted in the urine, a decrease in renal function will result in increased blood levels of the drug.

DuoDote™ Auto-Injector temporarily increases blood pressure, a known effect of pralidoxime. In a study of 24 healthy young adults administered a single dose of atropine and pralidoxime auto-injector intramuscularly (approximately 9 mg/kg pralidoxime chloride), diastolic blood pressure increased from baseline by 11 ± 14 mmHg (mean ± SD), and systolic blood pressure increased by 16 ± 19 mmHg, at 15 minutes post-dose. Blood pressures remained elevated at these approximate levels through 1 hour post-dose, began to decrease at 2 hours post-dose and were near pre-dose baseline at 4 hours post-dose. Intravenous pralidoxime doses of 30-45 mg/kg can produce moderate to marked increases in diastolic and systolic blood pressure.

Laboratory Tests: If organophosphorus poisoning is known or suspected, treatment should be instituted without waiting for confirmation of the diagnosis by laboratory tests. Red blood cell and plasma cholinesterase, and urinary paranitrophenol measurements (in the case of parathion exposure) may be helpful in confirming the diagnosis and following the course of the illness. However, miosis, rhinorrhea, and/or airway symptoms due to nerve agent vapor exposure may occur with normal cholinesterase levels. Also, normal red blood cell and plasma cholinesterase values vary widely by ethnic group, age, and whether the person is pregnant. A reduction in red blood cell cholinesterase concentration to below 50% of normal is strongly suggestive of organophosphorus ester poisoning.

Drug Interactions: When atropine and pralidoxime are used together, pralidoxime may potentiate the effect of atropine. When used in combination, signs of atropinization (flushing, mydriasis, tachycardia, dryness of the mouth and nose) may occur earlier than might be expected when atropine is used alone.

The following precautions should be kept in mind in the treatment of anticholinesterase poisoning, although they do not bear directly on the use of atropine and pralidoxime.

- Barbiturates are potentiated by the anticholinesterases; therefore, barbiturates should be used cautiously in the treatment of convulsions.
- Morphine, theophylline, aminophylline, succinylcholine, reserpine, and phenothiazine-type tranquilizers should be avoided in treating personnel with organophosphorus poisoning.
- Succinylcholine and mivacurium are metabolized by cholinesterases. Since pralidoxime reactivates cholinesterases, use of pralidoxime in organophosphorus poisoning may accelerate reversal of the neuromuscular blocking effects of succinylcholine and mivacurium.

Drug-drug interaction potential involving cytochrome P450 isozymes has not been studied.

Carcinogenesis, Mutagenesis, Impairment of Fertility: DuoDote™ Auto-Injector is indicated for short-term emergency use only, and no adequate studies regarding the potential of atropine or pralidoxime chloride for carcinogenesis or mutagenesis have been conducted.

Impairment of Fertility: In studies in which male rats were orally administered atropine (62.5 to 125 mg/kg) for one week prior to mating and throughout a 5-day mating period with untreated females, a dose-related decrease in fertility was observed. A no-effect dose for male reproductive toxicity was not established. The low-effect dose was 290 times (on a mg/m^2 basis) the dose of atropine in a single application of DuoDote™ Auto-Injector (2.1 mg).

Fertility studies of atropine in females or of pralidoxime in males or females have not been conducted.

Pregnancy:

Pregnancy Category C: Adequate animal reproduction studies have not been conducted with atropine, pralidoxime, or the combination. It is not known whether pralidoxime or atropine can cause fetal harm when administered to a pregnant woman or if they can affect reproductive capacity. Atropine readily crosses the placental barrier and enters the fetal circulation.

DuoDote™ Auto-Injector should be used during pregnancy only if the potential benefit justifies the potential risk to the fetus.

Nursing Mothers: Atropine has been reported to be excreted in human milk. It is not known whether pralidoxime is excreted in human milk. Because many drugs are excreted in human milk, caution should be exercised when DuoDote™ Auto-Injector is administered to a nursing woman.

Pediatric Use: Safety and effectiveness of DuoDote™ Auto-Injector in pediatric patients have not been established.

ADVERSE REACTIONS

Muscle tightness and sometimes pain may occur at the injection site.

Atropine

The most common side effects of atropine can be attributed to its antimuscarinic action. These include dryness of the mouth, blurred vision, dry eyes, photophobia, confusion, headache, dizziness, tachycardia, palpitations, flushing, urinary hesitancy or retention, constipation, abdominal pain, abdominal distention, nausea and vomiting, loss of libido, and impotence. Anhidrosis may produce heat intolerance and impairment of temperature regulation in a hot environment. Dysphagia, paralytic ileus, and acute angle closure glaucoma, maculopapular rash, petechial rash, and scarletiniform rash have also been reported.

Larger or toxic doses may produce such central effects as restlessness, tremor, fatigue, locomotor difficulties, delirium followed by hallucinations, depression, and, ultimately medullary paralysis and death. Large doses can also lead to circulatory collapse. In such cases, blood pressure declines and death due to respiratory failure may ensue following paralysis and coma.

Cardiovascular adverse events reported in the literature for atropine include, but are not limited to, sinus tachycardia, palpitations, premature ventricular contractions, atrial flutter, atrial fibrillation, ventricular flutter, ventricular fibrillation, cardiac syncope, asystole, and myocardial infarction. (See **PRECAUTIONS**.)

Hypersensitivity reactions will occasionally occur, are usually seen as skin rashes, and may progress to exfoliation. Anaphylactic reaction and laryngospasm are rare.

Pralidoxime Chloride

Pralidoxime can cause blurred vision, diplopia and impaired accommodation, dizziness, headache, drowsiness, nausea, tachycardia, increased systolic and diastolic blood pressure, muscular weakness, dry mouth, emesis, rash, dry skin, hyperventilation, decreased renal function, and decreased sweating when given parenterally to normal volunteers who have not been exposed to anticholinesterase poisons.

In several cases of organophosphorus poisoning, excitement and manic behavior have occurred immediately following recovery of consciousness, in either the presence or absence of pralidoxime administration. However, similar behavior has not been reported in subjects given pralidoxime in the absence of organophosphorus poisoning.

Elevations in SGOT and/or SGPT enzyme levels were observed in 1 of 6 normal volunteers given 1200 mg of pralidoxime intramuscularly, and in 4 of 6 volunteers given 1800 mg intramuscularly. Levels returned to normal in about 2 weeks. Transient elevations in creatine kinase were observed in all normal volunteers given the drug.

Atropine and Pralidoxime Chloride

When atropine and pralidoxime are used together, the signs of atropinization may occur earlier than might be expected when atropine is used alone.

OVERDOSAGE

Symptoms:

Atropine

Manifestations of atropine overdose are dose-related and include flushing, dry skin and mucous membranes, tachycardia, widely dilated pupils that are poorly responsive to light, blurred vision, and fever (which can sometimes be dangerously elevated). Locomotor difficulties, disorientation, hallucinations, delirium, confusion, agitation, coma, and central depression can occur and may last 48 hours or longer. In instances of severe atropine intoxication, respiratory depression, coma, circulatory collapse, and death may occur.

The fatal dose of atropine is unknown. In the treatment of organophosphorus poisoning, doses as high as 1000 mg have been given. The few deaths in adults reported in the literature were generally seen using typical clinical doses of atropine often in the setting of bradycardia associated with an acute myocardial infarction, or with larger doses, due to overheating in a setting of vigorous physical activity in a hot environment.

Pralidoxime

It may be difficult to differentiate some of the side effects due to pralidoxime from those due to organophosphorus poisoning. Symptoms of pralidoxime overdose may include: dizziness, blurred vision, diplopia, headache, impaired accommodation, nausea, and slight tachycardia. Transient hypertension due to pralidoxime may last several hours.

Treatment: For atropine overdose, supportive treatment should be administered. If respiration is depressed, artificial respiration with oxygen is necessary. Ice bags, a hypothermia blanket, or other methods of cooling may be required to reduce atropine-induced fever, especially in children. Catheterization may be necessary if urinary retention occurs. Since atropine elimination takes place through the kidney, urinary output must be maintained and increased if possible; intravenous fluids may be indicated. Because of atropine-induced photophobia, the room should be darkened.

A short-acting barbiturate or diazepam may be needed to control marked excitement and convulsions. However, large doses for sedation should be avoided because central depressant action may coincide with the depression occurring late in severe atropine poisoning. Central stimulants are not recommended.

Physostigmine, given as an atropine antidote by slow intravenous injection of 1 to 4 mg (0.5 to 1.0 mg in children) rapidly abolishes delirium and coma caused by large doses of atropine. Since physostigmine has a short duration of action, the patient may again lapse into coma after 1 or 2 hours, and require repeated doses. Neostigmine, pilocarpine, and methacholine are of little benefit, since they do not penetrate the blood-brain barrier.

Pralidoxime-induced hypertension has been treated by administering phentolamine 5 mg intravenously, repeated if necessary due to phentolamine's short duration of action. In the absence of substantial clinical data regarding use of phentolamine to treat pralidoxime-induced hypertension, consider slow infusion to avoid precipitous corrections in blood pressure.

MERIDIAN MEDICAL TECHNOLOGIES™

Manufactured by: Meridian Medical Technologies™, Inc.
Columbia, MD 21046

MMT 5173 11/07

Battlefield Forensics: Rebirth of an Ancient Science

By Neil C. Livingstone, Viewpoint

On July 17, authorities in Afghanistan captured a Pakistani woman named Aafia Siddiqui. She had first come to the attention of U.S. officials in late 2003 or early 2004, and they were deeply concerned by her links to al Qaeda, particularly in view of her extensive education in biology and the neurosciences. She had been educated at M.I.T. and Brandeis, and it was feared that she had the ability to actually produce weapons of mass destruction (chemical, biological, radiological). As part of the ongoing investigation of Siddiqui, U.S. investigators reportedly have taken hair and saliva samples from her, as well as fingernail scrapings, to ascertain whether or not she has been in recent proximity to various substances that could be used in WMD production.

Welcome to the new world of battlefield forensics.

Battlefield forensics was traditionally the purview of archaeologists and historians. They typically visited old battlefields – and analyzed old battles – focusing on such arcane (to the layman) matters as terrain analysis, the placement of fortifications, and an examination of cartridges, bones, and other debris to determine "what really happened" and to test theories, for example, about why one side was victorious over the other.

Recently, battlefield forensics has undergone a major revolution, and the focus today is no longer exclusively on the past but on contemporary fields of conflict as well. Utilizing the forensic tools developed by law-enforcement agencies and the criminal justice system, a new breed of specialists is using modern forensic techniques in the war on terrorism in combat theaters such as Afghanistan and Iraq. According to U.S. Navy researcher Anh N. Duong, the purpose is to "rapidly process battlefield evidence in-situ to support judicial, tactical, and strategic operations."

Members of the U.S. military are today being taught to collect, analyze, and preserve an array of information acquired on battlefields ranging from the tarmacs of airports to the mountains of Afghanistan and the roadways of Iraq. This information includes latent fingerprints recovered from explosive devices and safe houses, hair and blood samples, firearms (for clues as to their origin and use), and papers, identity cards, software, and computer data captured in engagements with terrorists or seized from their bases and safe houses. According to a report published in *USA Today*, Sgt. 1st Class Carlos Tyson, a member of a weapons intelligence team, investigated a roadside bombing in Iraq. Tyson found various "pieces" of the suicide bomber, including a hand. "We got a hand," Tyson told the reporter, "so we could fingerprint it."

Members of the 203rd Military Intelligence Battalion, which became known as "CSI Baghdad," are credited with pioneering the process of "fingerprinting, bagging, and tagging evidence and sending it back to the rear." Now the techniques and procedures developed by the 203rd and other bomb and weapons intel teams are being disseminated throughout the U.S. military, and the U.S. Department of Defense (DOD) has deployed portable forensic analysis units to a number of locations.

Valuable Information – And Potential Evidence

All of the information gathered has major intelligence applications, of course, but it also is important in making criminal cases against terrorist suspects captured by the military. This kind of evidence can definitively place a suspect at the scene of a terrorist attack or a terrorist training facility. It can trace an explosive device to a particular bomb maker or designer. Biometric evidence obtained on the battlefield also can be used to place terrorist fugitives on various watch lists.

Bombs are examined to learn about their design, construction, and, ultimately, for insights on how to defeat them. In view of the fact that seventy percent of U.S. military deaths in Iraq are caused by improvised explosive devices (IEDs), explosives forensics has become one of DOD's most important priorities. In large part for that reason, the department has established its own Terrorist Explosives Device Analytical Center (TEDAC). The Bureau of Alcohol, Tobacco, Firearms and Explosives has assisted in the training of forensic bomb technicians in Iraq, as have British police units.

In the future, DNA material will be collected from dead enemy combatants as well as those captured by U.S. military forces. This material can be stored in databases that military commanders, investigators, and intelligence officers can access in connection with ongoing investigations and/or to verify identity. DNA has been collected, for example, from members of the bin Laden family for comparison to fluids, residues, or body parts that might be recovered after a firefight or bombing raid to ascertain whether or not they belong to Osama bin Laden. It will be critically important that a positive I.D. be made before any public statement is released or the hunt for the al Qaeda leader is called off.

This use of DNA evidence would be strictly a bonus factor, though. It is clear that the new emphasis on battlefield forensics has been driven primarily by *warfighter* needs, and will be a key element in the global effort to defeat terrorism.

Dr. Neil C. Livingstone, chairman and CEO of Executive Action LLC and an internationally respected expert in terrorism and counterterrorism, homeland defense, foreign policy, and national security, has written nine books and more than 200 articles in those fields. He was the founder and, prior to assuming his present post, CEO of GlobalOptions Inc., which went public in 2005 and currently has sales of more than $80 million.

Standards for Sharing Intelligence and Information

By Diana Hopkins, Standards

When individual professionals, government agencies and other organizations, and the private sector join forces to develop consensus standards – i.e., standards approved by a consensus of stakeholders – the success of the process depends a great deal on all of those stakeholders sharing the same level of information and intelligence. Largely for that reason, the creation and success of information-sharing standards themselves require not only the harmonization of software and hardware but also the standardization of processes and procedures and, of even greater importance, the standardization of governance, particularly with regard to the safeguarding of sensitive information. Most importantly of all, perhaps, it involves the development of trust between and among the numerous stakeholders involved.

The challenges involved in information- and intelligence-sharing go far beyond the routine problems of information-sharing at the stakeholders table, where some agency stakeholders still distrust a system in which industry shares equally in consensus decision making; and in which at least some industry representatives are still not comfortable communicating in a forum that includes their competitors. There is a greater underlying challenge that affects all levels of government and industry in the homeland-security and national-defense communities, however, and it includes and reaches far beyond just those of standards development. What all levels of government, and the private sector, have learned from the terrorist attacks against the United States on 11 September 2001 is that the inability to work and plan together, combined with the inability, and/or unwillingness, to share information, can increase both individual and collective vulnerabilities.

Even before the 2001 attacks, though, the difficulty involved in the sharing of information and intelligence was considered a major challenge to the nation's successes in emergency management. After the attacks that difficulty was identified (in the 9-11 Commission's Report) as a key contributor to the federal government's failure to prevent the attacks. As the Commission Report suggested, the resistance to sharing information and intelligence probably is a carryover of the Cold War mindset that has been embedded in the thinking and behavior of the U.S. defense and intelligence communities for decades, during an era when it was clearly understood that intelligence leaks and data sharing could easily lead to catastrophe. The situation has changed considerably since the end of the Cold War, though, and today – as the 9-11 Report also suggests – continued resistance to the sharing of intelligence and information is more apt to place the United States, and the American people, in harm's way.

Although it has appeared at times that getting all sectors of the government and industry to modify their previous information-sharing behavior will require a sea change in attitudes as well as in legislation, significant progress has in fact been made in both areas. (For a timeline of the actions (and links to additional information) that have been taken by the U.S. government over the past several years to create an acceptable, and useful, Information Sharing Environment (ISE), click on http://www.ise.gov/pages/archive.html.)

It is difficult, of course, to excerpt just those efforts that involve only the development of standards, because an accurate assessment would depend on how successful the government is with its overall efforts in the promotion of information sharing. Following, nonetheless – with links to additional information also included – are some of the more notable steps the United States has taken, in the years indicated, to encourage (or in some cases require) the sharing of intelligence and other information:

2002 – The National Commission on Terrorist Attacks Upon the United States (also known as the 9-11 Commission – a bipartisan commission created by Congress and the President) was chartered to prepare an independent assessment of the 2001 terrorist attacks, and to develop recommendations to guard against future attacks.

2004 – The 9-11 Commission issued its Final Report, citing the lack of information/intelligence-sharing as a key factor in the nation's failure to prevent the 2001 attacks, and presenting a number of recommendations for changes in this area.

2004 – Responding to the Commission's recommendations, Congress enacted and the President signed the Intelligence Reform and Terrorism Prevention Act (IRTPA – Public Law 108-458), which specifically called for the creation of the previously mentioned Information Sharing Environment (ISE) to, among other things: (a) facilitate the sharing of information (e.g., about terrorism, weapons of mass destruction, and homeland security); and (b) to rationalize, standardize, and harmonize the policies, business processes, architectures, standards, and systems used by both the government and the private sector to share information. (For additional information about the Intelligence Reform and Terrorism Prevention Act, click on: http://www.ise.gov/docs/guidance/irtpa.pdf.)

Note: The IRTPA also called for the appointment of a program manager

OUR MISSION YOUR SAFETY

MSA
The Safety Company

TRIPLE RESPONSE

With MSA's NEW FireHawk® M7 Responder Air Masks

1. Use FireHawk M7 CBRN SCBA for firefighting and rescue
2. Switch to FireHawk CBRN Gas Mask *(air-purifying respirator)* for scene management, after low hazard level is assessed
3. Convert to FireHawk CBRN PAPR *(powered air-purifying respirator)* for long-term comfort and use

Each mode meets/exceeds the latest requirements of NFPA & NIOSH standards.

RESPOND NOW!

***Call your MSA fire service distributor or go to* MSAFIRE.com.**

| SCBA | APR/PAPR | FIRE HELMETS | GAS DETECTION | THERMAL IMAGING CAMERAS |

1.877.MSA.1001 | www.msapoliceline.com/domprep.html

(PM) for the ISE and the creation of an Information Sharing Council (ISC). On 15 March 2006, Ambassador Thomas E. McNamara was appointed to fill the PM post within the office of the Director of National Intelligence (DNI). (For ISE contact information, contact: Program Manager, Information Sharing Environment, Office of the Director of National Intelligence, Attn: Program Manager, Information Sharing Environment, Washington D.C., 20511; or call (202) 331-2490.)

2004 – The President established the National Counterterrorism Center (NCTC), a multi-agency facility dedicated to eliminating terrorist threats to U.S. interests at home and abroad. The NCTC was directed to serve as the primary federal organization for integrating and analyzing all intelligence pertaining to terrorism and counterterrorism, and to conduct strategic operational planning by integrating all relevant U.S. resources in this area. In December 2004 the NCTC was placed in the Office of the Director of National Intelligence.

2005 – A National Information Exchange Model (NIEM) was created by the U.S. Department of Homeland Security (DHS) and the U.S. Department of Justice (DOJ) to serve both as a foundation for and as a common standard for national inter-agency information-sharing and data exchange in the areas of justice, emergency management, and intelligence. One of the NIEM's more remarkable capabilities is that it not only automates information sharing, and thus makes information easily accessible in a universal namespace – but also can compartmentalize information for different levels of sharing. NIEM also is designed to allow the modification and growth of standards as new data components are harmonized and/or added. The nation's private-sector technology community has responded well to creation of the NIEM. (To contact NIEM, click on nisshelp@ijis.org or information@niem.gov; or call 1-877-333-5111 or 1-703-726-1919.)

2005 – A presidential memorandum was directed to the heads of executive departments on *"The Guidelines and Requirements in Support of the Information Sharing Environment,"* which provides five ISE priority areas for their attention and follow-through: (1) Defining common standards for how information is acquired, accessed, shared, and used within the ISE; (2) Developing a common framework for the sharing of information between and among executive-branch agencies and state, local, and tribal (SLT) governments; (3) Standardizing procedures for "sensitive but unclassified" (SBU) information; (4) Facilitating information-sharing between executive agencies and foreign partners; and (5) Protecting information privacy and other legal rights of Americans.

All levels of government have learned that the inability to work together, combined with the inability, and/or unwillingness, to share information, can increase both individual and collective vulnerabilities

2006 – The ISE Implementation Plan was created to provide a trusted one-voice partnership of all levels of the U.S. government, the private sector, and foreign partners that would help them: (a) share information in a multi-dimensional fashion; and (b) work together to build new core systems to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism. To further allay the concerns of many with regard to the quality and management of shared information, the Plan emphasizes that the information provided not only will be timely, validated, protected, and actionable, but also supported by education, training, and awareness programs. (For further information about the ISE Implementation Plan, click on: http://www.ise.gov/docs/reports/ise-impplan-200611.pdf.)

2006 – ISE privacy guidelines and implementation procedures were released by the PM-ISE, and an ISE Privacy Guidelines Committee (PGC) was formed to assist agencies in implementation. The ISE Privacy Guidelines (http://www.ise.gov/docs/privacy/privacyguidelines20061204.pdf) focus on existing privacy protections, and from that base strive to improve protections while also enhancing the sharing of information between and among all levels of government. Here it is important to note that the PGC is headed by the PM-ISE and includes the privacy officials of each ISC member. (Requests for additional information about the PGC and/or the privacy guidelines and implementation procedures should therefore be directed to the PM-ISE at the link provided above.)

2007 – The Common Terrorism Information Sharing Standards (CTISS) program was established, as a subcommittee of the ISC, to provide ongoing governance, configuration management, and both cross-agency and cross-government coordination and review of the standards developed. CTISS standards are thus performance-based "common standards" for preparing terrorism information for maximum distribution and access within the ISE.

2007 – The National Strategy for Information Standards (NSIS) was created: (a) to integrate all prior terrorism-related information-sharing policies, directives, plans, and recommendations; and (b) to provide a national framework against which to implement the ISE. The NSIS requires

that the ISE support the inclusion of locally generated information because such information is often extremely important to the development of statewide and national assessments of terrorist threats. The CTISS program also embraces the Federal Enterprise Architecture's Data Reference Model, a standards-based model designed to optimize data architectures for improved cross-agency information sharing. The first version of an enterprise architecture framework for the ISE was published earlier this year.

2007 – Under the CTISS program, a multi-agency partnership started, converging information exchange standards of NIEM, and the Department of Defense/ Intelligence Committee's Universal Core or UCORE. The purpose of the NIEM-UCORE partnership is to share information at critical times through the entire justice, public safety, emergency- and disaster-management, intelligence, and homeland security communities.

2008 – NIEM released a common format (in January) for law-enforcement data, LEXS, creating another important linkage in the NIEM-UCORE partnership, as well as an important linkage for state, local, and tribal partners. Three months later, the Department of Defense (DOD) and the Intelligence Committee (IC) issued a formal announcement on the status of UCORE, describing it as a standard that links many DOD and IC systems into common information components, basically of a geospatial nature.

2008 – The PM-ISE issued the first CTISS functional standard – i.e., one that provides the data and information-sharing foundation for operational information-sharing of Suspicious Activity Reports (SARs) in the ISE and supports demonstrations to include the SAR Evaluation. (The DOJ and Federal Bureau of Investigation (FBI) are working with fusion centers to adopt and implement the SAR functional standard both at the federal level and at selected fusion centers. The Department of State also has plans underway to apply the standard to its SAR database.)

2008 – A presidential memorandum was issued (on 9 May) to the heads of executive-branch departments and agencies on the designation and sharing of "Controlled Unclassified Information" (CUI) – implementing the recommendations of an interagency coordinating committee – i.e., that a common framework will streamline the designation, marking, safeguarding, and dissemination of CUI within the ISE.

2008 – Marking a significant change in the information-sharing culture, the FBI sponsored the creation of National Joint Terrorism Task Forces (NJTTFs) to combine federal and SLT units dedicated to combating terrorism in specific geographical areas. As of early August, more than 80 JTTFs had been created. The NJTTF effort includes a fusion operation, which means that threat intelligence and information are instantly shared vertically from FBI headquarters to all JTTFs and across NJTTF agencies. There are a number of state and major urban area fusion centers already working with local JTTFs. Creation of the NJTTFs represents a huge cultural change in regard to information-sharing because it demonstrates development of the awareness that different levels of government need, both to trust one another and to forge the agreements needed to quickly share detailed information in order to be effective. It also contributed to the Law Enforcement Information-Sharing Program (LEISP) Exchange Specification (LEXS) – a subset of the NIEM. (For information about local JTTFs, click on: http://www.fbi.gov/contact/fo/fo.htm.)

2008 – The President and Congress directed establishment of an Interagency Threat Assessment and Coordination Group (ITACG), integrated into the NCTC to improve the sharing of information with SLT and private-sector representatives. The creation of the ITACG is considered another major step forward toward the dissemination of federal data at the state, local, and tribal levels of government, and to the private sector as well, focusing on threat alerts, situational awareness reports, and strategic assessments of risks and threats. By integrating with the NCTC efforts, the ITACG has the added benefit of accessing information and experts of the FBI-sponsored NJTTFs, and that capability facilitates the production of federally coordinated terrorism-related information products intended for dissemination to SLT officials and private-sector partners. Considerable progress also has been achieved by the ITACG and the NJTTG in their efforts to develop a national network of state and major urban area fusion centers.

It is obvious that over the past several years the federal government has put considerable effort into promoting a new culture of information-sharing, and in making it understood that this is not just a good idea whose time has come, but an entirely new behavior pattern that is both recommended and mandatory. In short, although it took longer than anticipated after the 2001 terrorist attacks to surmount its previous problems with information sharing, the federal government has made significant progress on this front, particularly over the past year. Moreover, it is expected that the PM-ISE will be issuing a training module in the near future both to guide agency representatives toward an even greater shared awareness of the ISE and also to guide them in promoting information-sharing on their staff through the judicious use of performance evaluations and incentives.

Diana Hopkins is the creator of the consulting firm "Solutions for Standards." She is a 12-year veteran of AOAC INTERNATIONAL and former senior director of AOAC Standards Development. Most of her work since the 2001 terrorist attacks has focused on standards development in the fields of homeland security and national defense.

IDGA
Institute for Defense and Government Advancement

presents a training conference:

Register with code DOMPREP and SAVE $200 off the standard price!

4th Annual BORDER MANAGEMENT™ SUMMIT

October 14 – 17, 2008 • Bethesda North Marriott Hotel & Conference Center, MD

New track dedicated to maritime security!

This event is your passport to achieving interoperable border security operations:

- Learn interoperability policies and solutions you need for today's challenges
- Gain insight into the future of law enforcement strategies from the CBP
- Obtain a "boots-on-the-ground" perspective by hearing directly from the United States Coast Guard
- Discover the latest surveillance and communication technologies

Hear case studies, lessons learned and the way forward from speakers including:

Al Martinez-Fonts
Assistant Secretary, Private Sector Office, DHS

Kenneth Ritchhart
Assistant Commissioner/CIO, Office of Information Technology (OIT), CBP

Gregory Giddens
Executive Director
Secure Border Initiative

Robert Mocny
Director, US-VISIT Program

Maj Gen Michael Kostelnik, USAF (Ret),
Assistant Commissioner,
Office of CBP Air & Marine

And many more!

Sponsored by:

BAE SYSTEMS · safeports · FNH USA · Microsoft · TERADATA Raising Intelligence · TELEPHONICS A Griffon Company

www.BorderManagementSummit.com

Local Emergency Management: The CFATS Challenge

By Joseph W. Trindal, Law Enforcement

Chemical facilities have always been a concern for local first responders. Most major chemical accidents rapidly overwhelm the community emergency-services capabilities. Until the terrorist attacks of 11 September 2001, U.S. emergency-services agencies viewed chemical incidents as accidental events – and the tragic Bhopal (India) toxic chemical release in 1984 had already alerted emergency-services agencies worldwide as to the devastating consequences posed by chemical accidents. In the Bhopal accident, over 7,000 fatalities occurred within days of the accident; long-term casualty estimates later escalated the total to more than 100,000 victims.

The 9/11 attacks, coupled with intelligence reports of other attack plans, showed that many terrorists are willing to exploit the hazardous nature of chemical sites to further their aim of creating an atmosphere of fear and intimidation in a target population. For that reason alone, local emergency-services agencies with chemical facilities in their jurisdictions must now consider preparation for chemical-related events that are intentional as well as accidental. While there are few distinctions between managing an accidental as opposed to an intentional chemical event, the attractiveness of chemical sites as a terrorist target poses major challenges for all emergency-services disciplines.

In 2006, the federal government established the foundation for chemical-security regulations that are currently in the implementation phase. The Chemical Facility Anti-Terrorism Standards (CFATS) create uniform security standards for high-risk chemical sites throughout the United States. The CFATS regulations, administered by the Department of Homeland Security (DHS), are designed to ensure that consistent performance-based security standards are effectively applied to all chemical sites possessing certain quantities of 322 so-called "chemicals of interest."

In order to identify high-risk chemical sites, DHS conducted a massive screening effort of nearly 40,000 producers, users, distributors, and holders of the chemicals of interest. After analyzing the data developed by the screening, the department determined that about 7,000 sites should be subject to CFATS regulations. The same data provided DHS the information needed to establish a risk ranking of the 7,000 facilities, which are grouped in four "tiers" – with Tier 1 being the highest-risk facility. The tier ratings are based on the quantity and types of chemical(s) on site, coupled with the site's proximity to U.S. population centers.

The CFATS regulations affect local emergency-service agencies in a number of ways. First, the local emergency-services community must be aware of the DHS high-risk sites in its jurisdiction and understand what security standards apply to each site. Second, emergency-services agencies must address the information-sharing challenges posed by CFATS. Lastly, the emergency-services community needs to embrace the private chemical sector in an all-hazards approach to emergency preparedness.

Local CFATS Awareness Mandatory

At the core of the CFATS regulations are 18 Risk-Based Performance Standards (RBPSs) related to security needs. The CFATS security criteria are performance-based rather than proscriptive. This provides the opportunity for chemical sites to determine the most cost-effective way to meet CFATS regulatory performance expectations. In addition to the 18 RBPSs, DHS reserves the right to establish additional security requirements as situations or actionable intelligence may dictate.

Integrating the CFATS-regulated site and its local emergency-service providers is a major performance standard. Regulated chemical sites must, depending on their tier rankings, establish their security standards with consideration of local law-enforcement response capabilities. They also must conduct emergency preparedness exercises with local emergency-services agencies in order to validate site security plans and ensure effective local integration.

In most jurisdictions, local fire departments already have established working relationships with the chemical sites in their communities. These relationships provide an excellent springboard for developing and strengthening emergency preparedness collaboration under CFATS. The local fire department is well positioned to host interdisciplinary working groups that focus on CFATS-regulated facilities in the local jurisdiction. The DHS Office of Infrastructure Protection and the state Homeland Security Advisor's office are excellent resources for collaboration.

CFATS Challenges To Information Sharing

CFATS provides compliance standards for information sharing. The information collected under CFATS is protected as Chemical-Terrorism Vulnerability Information (CVI), a subset of the "Sensitive but Unclassified" (SBU) information security designation. CVI provisions treat certain information as if it were *Secret*, though, to safeguard it from terrorist plotting and intelligence efforts.

A key element governing CVI access is the "need-to-know" guideline. DHS recognizes that certain disciplines of the local emergency-services community have a clear need to know certain CVI material. For that reason, the department has established procedures, in cooperation with state Homeland Security Advisors' offices, to provide local emergency-service agencies access to such information. These procedures include a vetting process of each person nominated to be granted access as well as a short web-based training program that must be completed by that person before access is granted. Even regulated chemical sites are prohibited from disclosing CVI-designated information to unauthorized personnel.

It is vital that local emergency-services agencies determine who within their organizations has the need to know and therefore should be granted access to CVI data. These personnel decisions should take into account a need for redundancy – balanced, though, against the equally compelling need for narrow access controls. Each agency is required to establish protocols for managing its own CVI material. (This requirement is similar to but procedurally different from the requirements for managing Protected Critical Infrastructure Information (PCII) or Sensitive Secure Information (SSI) under other DHS-administered programs.)

With the CVI clearances completed, the local emergency-services community can substantively engage in broad emergency planning, working in close cooperation with representatives of the CFATS-regulated sites. Because the local CFATS-regulated chemical sites are, by DHS definition, high-risk facilities, the integrated emergency planning efforts should concentrate primarily on those sites.

DHS determines the attack scenarios that are considered to be most applicable to the chemicals of interest held at each site. Many regulated sites are already applying those attack scenarios to their respective sites and chemicals as part of what are called site-vulnerability assessments (SVAs).

The same attack scenarios, when applied to the regulated sites within a local jurisdiction, provide an ideal starting point for integrated planning. Representatives of the regulated chemical sites are the subject-matter experts on how the attack-scenario consequences are likely to unfold, taking into consideration the chemical characteristics, attack characteristics, and the site-mitigation capabilities available. Local emergency-service agencies are the subject-matter experts on local response capabilities and community-based consequence-management capabilities. The CFATS-regulated sites are required to develop site security plans (SSPs) as part of the CFATS compliance efforts. The local emergency-services community should be engaged at various points in the development of the SSPs.

Integrated Emergency Management with CFATS Focus

The inclusion of CFATS-regulated sites in local- and state-focused emergency-preparedness exercises is an important aspect of integrated planning. Exercises are a vital tool for testing and validating internal stakeholder plans as well as the interagency cohesion across disciplines and stakeholders. A critical incident involving a CFATS-regulated site changes the traditional list of stakeholders involved in that event. At the national level, each CFATS-regulated site is inherently a high-risk and potentially high-consequence site.

The integrated emergency planning required has to be carried to the next level. CFATS regulations apply to defeating or mitigating acts of terrorism. However, sound and comprehensive emergency preparedness considers cascading impacts and compounding events from an all-hazards perspective. Government and CFATS-regulated site officials should therefore examine and prepare for non-terrorist events that also might produce vulnerabilities that could be exploited by terrorists. A natural disaster typical to a particular local community – e.g., wildfires in California, hurricanes in Florida – might well diminish the security integrity at a CFATS-regulated site, leaving it more vulnerable to terrorist attack or exploitation. Since the 9/11 attacks, state, local, and tribal jurisdictions throughout the United States have greatly improved the natural-disaster preparedness capabilities of their own communities. With the CFATS regulations in place, there are new opportunities to economize on emergency preparedness efforts – e.g., by including CFATS-regulated sites in natural-disaster planning and exercises.

To summarize: CFATS was established to provide uniformity in the rules and regulations securing the nation's hazardous-chemical sites from terrorist attacks. Chemical security standards are essential in protecting U.S. communities from malicious threats of the 21st century. Effective security requires a community effort that is inclusive of CFATS while extending beyond regulated sites to involve all local stakeholders and reasonable incident scenarios that might occur. Critical incidents and disaster events are local in nature; for that reason, the optimal solutions are almost always community-based. In short, CFATS presents regulated sites and local first-responder communities new opportunities for inclusive and focused emergency planning.

Joseph W. Trindal recently retired as chief of the Inspections & Enforcement Branch of DHS's Infrastructure Security Compliance Division. That branch is responsible for administering and enforcing the Chemical Facility Anti-Terrorism Standards. A career federal law-enforcement investigator and executive, Trindal served with the U.S. Marshals Service for 20 years before accepting the position of director for the National Capital Region, Federal Protective Service, DHS.

ADVANCED CAPABILITIES FOR CRITICAL ASSET PROTECTION

ICx Technologies is a leader in the development and integration of advanced detection technologies for all the CBRNE segments. Our sensors are compact, portable and simple to use. These network ready CBRNE detection instruments are ultra sensitive, accurate and have low false alarm rates. Our ruggedized products deliver the situational awareness and actionable intelligence necessary for facility and checkpoint monitoring such as at the Statue of Liberty and Ellis Island in New York.

www.icxt.com/detection

NEW THREATS.
NEW THINKING.™

icx™ technologies

Indiana, California, South Carolina, and Virginia

By Adam McLaughlin, State Homeland News

Indiana Conducts Biohazard Drill with the U.S. Postal Service

Emergency personnel worked to contain an anthrax contamination and deal with injuries, crowd control, and even a woman in labor during a 30 July training exercise at the main U.S. post office in Lafayette, located in western Indiana.

Emergency responders, firefighters, police officers, post office personnel, healthcare workers, and American Red Cross volunteers spent much of the afternoon simulating their individual and collective responses to a biohazard emergency and the complications that could ensue. "If this [a real major disaster] ever happens, it is going to be considered as a WMD [weapon of mass destruction] attack," said Kimberly Yates, customer relations' coordinator for the U.S. Post Office. "We have to be prepared."

Timothy Batta, deputy director of the Tippecanoe County Emergency Management Agency, pointed out that there are numerous factors involved in a response of the scale planned, and going through the whole drill from start to finish "helps work out the kinks." When the representatives of the numerous agencies involved go back later to critique the exercise, he said, everyone will be able to see different aspects of the response where improvements can be made.

James Eagy of Lafayette, a mail handler at the post office, volunteered to be one of the "victims" evacuated by emergency teams and put through the decontamination process. He had to go through a shower system that washed him down head to toe, which was not an altogether unpleasant experience during last week's hot weather. Other evacuees who needed decontamination were run through wash stations. In addition, emergency personnel simulated the washing down of people suffering from simulated injuries of various types, and also practiced the processing of uninjured people through a truck shower system. The cleansers used, Batta said, were everyday household products: Dawn dish detergent and liquid Tide, both of which are commonly used in hazmat response operations.

> ***The quake served as a helpful reminder of the seismic dangers always lurking not too far below the state's sprawling freeways and numerous subdivisions***

The post office also uses a biohazard detection system to continuously test loose particles in the mail, officials said. An alarm would go off in the case of biohazard detection, and calls would go out to local 911 dispatchers. Contaminated clothes also would be collected, along with the water used to rinse off the victims. A private contractor would dispose of the materials after a real emergency.

Yates said there is no increased concern about anthrax threats, but drills are nonetheless carried out routinely at various post office locations to ensure a broad level of preparedness throughout the country. Two Washington, D.C., postal workers died from anthrax exposure in 2001 not long after the 9/11 terrorist attacks.

California Moderate Earthquake An Unscheduled Drill For "The Big One"

Despite shaking a large swath of Southern California, last week's magnitude-5.4 earthquake was not "The Big One" that scientists, and that state's residents, have long feared. Still, it rattled nerves, causing many Californians – and both state and local responder agencies – to move faster to step up their emergency-response preparations.

The quake, which rocked the region from Los Angeles to San Diego last Tuesday (July 29), caused some property damage and a number of minor injuries, but also served as a helpful reminder of the seismic dangers always lurking not too far below the state's sprawling freeways and numerous subdivisions.

The temblor's epicenter was determined to be just outside Chino Hills, 29 miles southeast of downtown Los Angeles in San Bernardino County, and was felt as far east as Las Vegas. Dozens of aftershocks followed, the largest a magnitude-3.8. "We were really fortunate this time," said Capt. Jeremy Ault of the Chino Valley Independent Fire District. "It's a good opportunity to remember that we live in earthquake country. This is part of living in Southern California, and we need to make sure we're prepared."

Chino Hills was incorporated in 1991, so much of the construction in that area is not only newer but also built to more stringent safety standards, city spokeswoman Denise Cattern pointed out. There were no reports of any major

problems in the city of 80,000, she said, although cell phone service in the area was briefly disrupted. "We have all the latest building standards and that probably made a difference," Cattern said.

The magnitude-5.9 Whittier Narrows quake in 1987 was the last big shake centered in the region. Scientists are trying to determine which fault ruptured to cause the latest quake, but they believe it is part of the same system of faults. The 1987 earthquake heavily damaged older buildings and houses in a number of communities east of Los Angeles.

Minor structural damage was reported throughout Los Angeles itself, though, along with five minor injuries and a few instances of passengers stuck in elevators, according to City Councilwoman Wendy Greuel, serving as acting mayor. She said there also was flooding in one department store.

The jolt caused a fire but no injuries at a Southern California Edison electrical substation in La Habra, about 12 miles southwest of the epicenter, said spokesman Paul Klein. Damage there and to other equipment led to some power outages in Chino Hills, Chino, Diamond Bar, and Pomona, he said.

To prepare even more thoroughly for "The Big One," scientists and emergency planners have scheduled for this fall what is being described as the largest earthquake exercise in the country – it will be based on a hypothetical magnitude-7.8 temblor. Earlier this year, scientists calculated that California faces a 99.7 percent chance of a magnitude-6.7 quake or larger sometime within the next 30 years.

South Carolina
Interagency Port Security Initiative Serves as National Model

A pilot program established in 2003 as a long-term response to terrorism, Project SeaHawk puts federal, state, and local law-enforcement personnel together – in the operations center, at weekly briefings, and aboard boats and other small craft.

Rows of seats face a panel of flat screens in the Charleston, S.C., operations center. Some of the screens show global positioning systems on dispatched SeaHawk vehicles and boats. Others play real-time footage from around the port and/or on key roadways. One shows the portal, a virtually collaborative website specifically established for Project SeaHawk officials. The individual viewer can click on any ship logged into the portal to see the vessel history and the potential threat it poses, where the ship's crew is from, and how each SeaHawk-affiliated agency is expected to check it out as it traverses local waters.

Before the SeaHawk technology became available, law-enforcement agencies at the port sometimes repeated one another's chores – and occasionally overlooked a few of those chores. SeaHawk also boasts an arsenal of detection tools, ranging from an ion scanner designed to detect the presence of drugs and/or explosives to so-called "currency canines" assigned to the Charleston County Sheriff's Office.

SeaHawk dwells in discretion. The project does not advertise its location, and a green film covers each window at the operations center to deflect and deter spy cameras. But, despite its secrecy, SeaHawk now wants to share some of its accomplishments, because its coffers are almost empty and its future has therefore become uncertain. Both in South Carolina and in Washington, D.C., emergency-management officials are wondering what will happen to the program, the first of its kind funded by Congress to fill in potentially deadly security gaps on the maritime front.

Project SeaHawk operates under the U.S. Department of Justice, with the U.S. Attorney's Office managing its finances. By next fall, however, the $46 million in funds originally allocated to the program will run out, and the project will be transferred to the custody of the Department of Homeland Security, an agency that did not exist when SeaHawk was launched.

There is one question that SeaHawk officials can answer quickly and directly, because it comes up often: Of all the ports throughout the United States, why Charleston?

Residents know that Charleston boasts an active commercial waterfront. As a seaport, it ranks sixth in the nation in container throughput, handling the equivalent of 1.8 million 20-foot-long steel boxes a year.

The state's economy and the nation's security roost here. For that reason alone, representatives from 47 law-enforcement agencies meet at SeaHawk headquarters every Wednesday for half an hour or so, during which time they share intelligence both about international terrorism and about the local crime situation.

A number of other ports around the country have followed Charleston's model, and some of the Project SeaHawk technology is expected to become nationally streamlined under the SAFE Port Act. The port of Savannah, Georgia, for example, started a SeaHawk spin-off called the Maritime Interagency Center of Operations last year and, although without its own funding, uses some of the technology already developed in Charleston.

Virginia
University Conducts Computer-Simulated Study On Pandemic Flu Impact

The federal government would have to quarantine infected households and ban most if not quite all public gatherings to contain pandemic flu, according to a computer simulation study conducted by researchers from Virginia Tech and discussed in the *Proceedings of the National Academy of Sciences* March 2008 issue.

"You would not go out to the movies. You would not congregate with people," said researcher Stephen Eubank. "You would pretty much be staying home with the doors and windows battened down."

The consensus among health experts is that a pandemic, or global epidemic, of influenza is inevitable at some time in the not-too-distant future. The last such pandemic, in 1918, killed between 40 and 100 million people. (The exact number will never be known, in large part because the gathering of statistics was at that time both more difficult and much less precise than in recent years.)

Because of the belief that a pandemic cannot be avoided, researchers are instead looking into ways to limit its effects. In the Virginia Tech study, researchers used a computer to model the hypothetical spread of a flu pandemic in the city of Chicago under various containment scenarios. They found that a vigorous early response could reduce the infection rate by 80 percent. "Depending on how fast it [the flu] is spreading, it seems as though you really need to throw everything you can at it," Eubank said.

Under the containment scenario, those infected with or exposed to the disease would be confined to their homes, and schools and day-care centers would be shut down – as would be other public-gathering places such as bars, restaurants, and theaters. Offices and factories probably would remain open, but because of quarantines would usually operate at reduced capacity.

The extreme measures postulated would have to continue for months, until a reliable and effective vaccine could be developed and distributed. "We are not talking about simply shutting things down for a day or two like a snow day," Eubank said. "It … [would be] a sustained period lasting weeks or months." The computer model assumed widespread compliance with the response plan, but Eubank said he does not anticipate that that would be a problem. "In the context of a very infectious disease that is killing a large number of people," he said, "I think that large fractions of the population will not have a problem with [accepting] these recommendations."

Adam McLaughlin is with the Port Authority of NY & NJ, and is the Preparedness Manager of Training and Exercises, Operations & Emergency Management, where he develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs.