

Chemical Preparedness Progress and Pitfalls



A U.S. Responder's View of
Israeli Security and Preparedness

By Glen Rudner, Fire/HazMat

"By Far the Greatest Threat to U.S. Civil Aviation"

By Neil Livingstone, Ph.D., Transportation

The PPE & Other Basic Needs of Tactical Officers

By Richard Schoeberl, Law Enforcement

ICD - Shorthand for a Potentially Ubiquitous Threat

By Joseph Cahill, EMS

DomPrep Survey

Your Thoughts Compared with DomPrep40's
National Experts on...The Chemical Threat
& the State Of Chemical Preparedness

Prepared by Major General Stephen V. Reeves

USA (Ret.); Summarized by John F. Morton, DP40

Surgically Implanted Death

Human IEDs vs. Full-Body Scanning

By Joseph Trindal, Law Enforcement

Responding to CBRNE Attacks: A Quick Primer

By J.L. Smither, Viewpoint

Haiti 2010

When Disaster Is Compounded

By Chaos and Confusion

By Theodore (Ted) Tully, Public Health

Department of Defense Focuses on IT Innovation

By Thomas Payne, Director, ITT's

Information Integration Systems, Case Study

The Need for

Situational Awareness in a CBRNE Attack

By Jordan Nelms, Viewpoint

Partners in Preparedness

Close to 2000 Attendees

At Public Health Preparedness Summit

By Jack Herrmann, Public Health

The Security Checkpoints of Tomorrow

By Peter Kant, Vice President

Rapiscan Systems Government Affairs, Case Study

Keeping It Simple - And the Need for Pre-Planning

By William (Jeremy) Magers, Fire/HazMat

Critical Infrastructure Protection:

Another Role for NIMS+ICS

By Steven Grainer, CIP-R

Massachusetts, Arizona, North Dakota & Nevada

By Adam McLaughlin, State Homeland News

smiths detection

bringing technology to life

bioterrorism is a real threat

NEW **Bio-Seeq™ PLUS**
Portable Anthrax, Tularemia,
Plague and Pan-Orthopox
detector and identifier

- LATE PCR technology produces lab quality results in the field
- Detects trace levels of organisms through DNA replication
- Used by emergency responders with little to no biological testing experience
- High accuracy of distinguishing between harmful and benign material

For more information:
call toll-free **1 888 473 6747**
or **1 203 207 9700**
email [GMR.Americas@smithsdetection.com](mailto:GMER.Americas@smithsdetection.com)



Bio-Seeq™ PLUS



www.smithsdetection.com

Bio-Seeq™ PLUS is a trademark of Smiths Detection Group Ltd.

Editor's Notes

By James D. Hessman, Editor in Chief



The U.S. and Israeli aviation security systems; personal protective equipment and other personal/operational needs of tactical officers; the U.S. medical response to the earthquake in Haiti; protection of the U.S. critical infrastructure; a “quick primer” on how to respond to CBRNE attacks; the U.S. Department of Defense’s renewed interest in some creative IT (information technology) upgrades; and an easy-to-follow roadmap to reading gas spectrometers and other complicated meters, measuring devices, and similar equipment.

All of those topics, and more, are covered by world-class experts – in each of the subject areas named – in this month’s printable edition of DPJ – which also includes: (a) advance notice of an alarming new type of terrorist threat – surgically implanted IEDs (improvised explosive devices) deep inside the body cavities of volunteer martyrs willing to sacrifice their lives by attacking Americans; (b) a bullish report on the recently concluded and highly successful Public Health Preparedness Summit in Atlanta; (c) a timely preview of the upgraded and highly sophisticated – but simpler in several important ways – aviation security checkpoints of the future; (d) situational updates on recent domestic-preparedness advances and improvements in the great states of Arizona, Massachusetts, Nevada, and North Dakota; and (e) Last but by no means least, the just announced results of the latest DomPrep40 Survey (on U.S. Chemical Preparedness as well as a number of glaring deficiencies in that area).

The Chemical Preparedness survey, prepared by Maj. Gen. Steven V. Reeves, USA (Ret.) and summarized by John F. Morton, compares the views, in this immensely important subject area, of the DomPrep40 members with the considered opinions of *DPJ* readers and finds, not surprisingly, that both groups believe that U.S. preparedness to cope with a chemical-warfare attack is woefully deficient in numerous ways and that the present *lack of preparedness* amounts, in effect, to a mass-casualty incident waiting to happen.

Meanwhile, earlier, and continuing, deficiencies in U.S. airport security are discussed in related articles by Glen Rudner and Neil Livingstone, both of whom recommend that the United States take a long look at the simpler but much more effective Israeli aviation-security system; Dr. Livingstone provides an additional list of changes, upgrades, and improvements that, if fully implemented, would make the skies above as well as the airports below much safer and more secure for all Americans. A companion “Case Study” article by Rapiscan’s Peter Kant provides the preview look, mentioned above, of the security “Checkpoints of Tomorrow.”

A second Case Study, by ITT’s Thomas Payne, discusses the heightened DOD interest in, and operational use of, several recent advances in IT technology. JL Smither of LLIS authored the quick primer on how to cope with CBRNE attacks (quickly, but also very carefully, and always according to “the book”). Jack Herrmann’s roundup report on the 2010 Public Health Preparedness Summit – keynoted by HHS Secretary Kathleen Sebelius – should guarantee even greater attendance next year. But Joseph Trindal’s discussion of the use of “Human IEDs” to down more U.S. passenger aircraft shows that those who hate America also know how to learn from experience.

Rounding out the issue are articles by: (1) Richard Schoeberl (on the equipment and PPE needs of tactical officers); (2) Theodore (Ted) Tully (on how New York City’s Mount Sinai Hospital helped the long-suffering Haitian people in their hour of greatest need); (3) William (Jeremy) Magers (on the common-sense “simplicities” and easy-to-understand basics of preparedness training); (4) Steven Grainer (on the mutual benefits that can be achieved by fusing, so to speak, the NIMS and ICS guidelines), and (5) Adam McLaughlin, whose news digest on recent advances and upgrades in the four states named above shows that not all is gloom and doom, that much good work already has been done, and that the responder guidelines must still and always be Forward, Onward, and Ever Upward.

About the Cover: Collage, by Susan Collins, of two iStockphotos (the smoke, and the making of a homemade chemical bomb) and one U.S. Army photo (by Benjamin Faske) of an Army hazmat specialist calling headquarters to report his status during the 8 November 2009 Operation Vibrant Response, a CBRNE training exercise, at the Muscatatuck Urban Training Center in Butlerville, Indiana.

Business Office

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

Staff

Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Catherine Feinman
Account Executive
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

AVON Protection
Bruker Detection
Disaster Response & Recover Expo
DuoDote (Meridian Medical Technologies)
Environics USA
ICx Technologies
Idaho Technology Inc.
IDGA Border Security Southwest Conference
International Hazardous Materials Response
Teams Conference 2010
ITT
PROENGIN Inc.
Rapiscan Systems
Remploy Frontline
SE International
Smiths Detection
SMI Cyber Defense Conference
Tex-Shield

© Copyright 2010, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

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

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



Dangerous threats are everywhere. So we make it our mission to address and minimize them. At ITT, we engineer, implement and maintain customized solutions that help secure our nation's borders, ports and infrastructure. By combining integrated software architecture and leading-edge technology, we provide solutions that can enhance and maintain the security of our nation. Our systems can limit the effects of disasters, detect terrorist activity and provide intelligence and warnings so that attacks can be prevented before they happen. Are you ready? For more information about ITT, please visit itt.com/security.

Today's threats are unpredictable. Our security should be anything but.



ITT

Engineered for life

Electronic Systems • Geospatial Systems • Information Systems

ITT, the Engineered Blocks logo, and ENGINEERED FOR LIFE are registered trademarks of ITT Manufacturing Enterprises, Inc., and are used under license. ©2010, ITT Corporation

Contributors

First Responders

Kay Goss
Emergency Management

Joseph Cahill
EMS

Glen Rudner
Fire/HazMat

Steven Grainer
Fire/HazMat

Rob Schnepf
Fire/HazMat

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Joseph Watson
Law Enforcement

Medical Response

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Bruce Clements
Public Health

Theodore (Ted) Tully
Health Systems

Adam Montella
Health Systems

Government

Corey Ranslem
Coast Guard

Dennis Schrader
DRS International LLC

Adam McLaughlin
State Homeland News

Infrastructure

Neil Livingstone
ExecutiveAction

Industry

Diana Hopkins
Standards

A U.S. Responder's View Of Israeli Security & Preparedness

By Glen Rudner, Fire/HazMat



While the United States continues to suffer under the weight of yet another change in security protocols, several questions remain unanswered as to why the U.S. government has not put into effect a security system similar in most if not quite all ways to the one the Israelis have been using – with remarkable success – for many years.

The most obvious, and most important – but perhaps not truly answerable – question is this: How can the United States make American society more like Israel's, which has dealt with far greater terror threats for many years, and with far less inconvenience? During a recent trip to Israel, a group of U.S. responders [including the author of this article] observed how the Israelis cope with terrorist threats on a daily basis.

Valuable lessons were learned by the American responders on each and every day of the trip as different aspects of the Israeli culture were observed. It quickly became evident, for example, that the everyday life of Israeli citizens is seldom disturbed by the constant threat of an outside attack – primarily, it seemed, because a mindset of safety and security is deeply imbedded within the Israeli people, and that mindset has become part of the everyday national lifestyle. The Israelis have learned to be, and are, concerned about terrorism – but they do not allow it to ruin their lives; instead, they have learned to be personally and collectively observant and to rely on a security force that is in many but not quite all ways transparent – to visitors as well as to the Israelis themselves.

The Israeli security force is composed of all of the nation's emergency services including EOD (explosive ordnance disposal), fire, police, and medical-response teams, as well as internal security agencies – all members of which are trusted members of the community. Collectively, and as individual citizens, these teams, agencies, and organizations not only protect but also educate their neighbors and friends by their own constant vigilance and awareness.

Visibility, Simplicity, Common Sense, Transparency

While traveling throughout the State of Israel, which covers a land mass slightly smaller than the state of New Jersey, the American observers also noted that the Israeli security process is not only visible but also, in many respects, transparent. There are both uniformed and non-uniformed security officers and responders at malls, shopping centers, office buildings, even walking the streets – but they are blended into and have become part of the environment. There are a number of locations, of course – government buildings, and military posts, for example – where visibility is important because it acts as a deterrent. But the visibility of security personnel is seldom if ever threatening to the general public.

The most amazing aspect of such transparent security, perhaps, is that every man, woman, and child (except very young children) living in Israel is part of it. An unattended bag, a person acting suspiciously, and aberrant behavior of any type is almost always quickly reported – and just as quickly acted upon, even if the action taken is simply a law-enforcement officer asking a question or two. One obvious example of this is evident to visitors arriving at the entrance to Ben Gurion Airport, which is the hub of travel for all of Israel. As visitors enter the airport property they must go through a security checkpoint where a law enforcement officer asks a few simple questions – for example, “Who are you?”, “Where are you going?”, and “How long have you been in Israel?”

It quickly becomes obvious that the security officers not only are looking for incendiary or explosive materials – grenades, guns, and bombs, for example – but also, and of much greater importance, are seeking to detect any of various human factors (nervousness, hesitant and/or confusing answers, etc.) that indicate there may be a problem. From this point forward the security system is observing people on a continuing basis from the time they exit their transportation vehicle until they board their aircraft.

Here it is important to note that there are several rings of security at Ben Gurion that must be crossed to travel from the entrance of the airport to the boarding gate. In short, it is a simply amazing system that combines technological capabilities with common sense, due diligence, and a close to national mindset. The way the Israelis carry out their “profiling” of visitors includes a significant difference (from the American way) that is worth emphasizing – namely, that the Israelis profile *everyone*. History has shown that the Israeli system works – exceptionally well – and the observers’ trip through the airport provided an excellent example of how and why it works.

Human Factors: The Most Important Component

What is perhaps even more important is that the Israeli security system works with minimum interference with

the everyday pursuits of the individual citizen. From the arrival at the first checkpoint to the gate to board an aircraft, for example, it took less than 40 minutes for the American visitors to pass through all of the security checkpoints involved.

This same level of security, which is demonstrated daily throughout the country, provides an interesting perspective to a first responder from another part of the world where security is taken for granted. During the past 12 months there have been two examples of U.S. security breaches that – most if not all U.S. (and outside) security experts agree – would not have occurred if changes had been implemented through which the United States had been able to use the Israeli methodology of security. Both of those incidents – the Fort Hood shootings and the attempted Christmas Day bombing of a passenger aircraft bound for Detroit – probably could have been prevented if U.S. security agencies had used the “human factors” approach to security that the Israelis have used so well for so many years – and that have become that nation’s front line of homeland defense.

There is a need to learn from Israel, and from other U.S. allies throughout the world, much more about the human facets of front line security. The nation’s first-responder community, which already has become an important tool in the global war on terrorism, must be encouraged to take the golden opportunity now available to educate themselves to be much better prepared than they now are in observing, and acting upon, the human factors which, all evidence shows, may well be the most important component of an effective homeland-defense policy.

It quickly became evident that the everyday life of Israeli citizens is seldom disturbed by the constant threat of an outside attack – primarily, it seemed, because a mindset of safety and security is deeply imbedded within the Israeli people, and that mindset has become part of the everyday national lifestyle

Glen D. Rudner is a project manager for CRA-USA, where he works with senior management executives on major corporate issues; he is currently assigned to management of the Target Capabilities List project for the U.S. Department of Homeland Security. A recently retired Northern Virginia Regional Hazardous Materials Officer, he has been heavily involved during the past 32 years in the development, management, and delivery of numerous local, state, federal, and international programs for such organizations as the National Fire Academy, the FBI, and the Defense Threat Reduction Agency. A widely published author on public safety issues, he also is a voting member of both the National Fire Protection Association’s Hazardous Materials Subcommittee and the International Association of Fire Chiefs’ Hazardous Materials Committee as well as the co-vice chair of the Ethanol Emergency Response Coalition.

“By Far the Greatest Threat to U.S. Civil Aviation”

By Neil C. Livingstone, Ph.D., *Transportation*



“The system worked,” said DHS (Department of Homeland Security) Secretary Janet Napolitano on the Sunday talk shows following apprehension of the so-called “Underwear Bomber,” Umar Farouk Abdulmutullab, on Christmas Day 2009.

Abdulmutullab had attempted to detonate a PETN-based explosive device, hidden in his underwear, while flying from Amsterdam to Detroit on Northwest Airlines Flight 253. The device had fizzled, however, and Abdulmutullab was subdued by other passengers until after the plane landed in Detroit.

In tests conducted for the BBC using a similar device holding the same amount of explosive, researchers concluded that it was unlikely that Flight 253 would have gone down if the device had worked properly. Nevertheless, Abdulmutullab and whoever was sitting next to him would probably have died in the blast – and the incident once again underscores the vulnerability of the U.S. civil aviation system to terrorists.

Moreover, Napolitano’s assertion that “the system worked” would have been true only if the passengers who stopped Abdulmutullab were considered part of “the system.” That also was the case in the 2001 incident involving Richard Reid, when the other passengers had to deal with the situation on board after failure of the explosive device concealed in Reid’s shoes to detonate completely.

For Abdulmutullab to come as close as he did to exploding a lethal device aboard an aircraft there had to be, and were, several failures throughout the U.S. aviation security system. It is evident in retrospect, for example, that he should have been caught before he ever boarded the aircraft (an Airbus A330). Also, he had paid cash for a one-way ticket to the United States and held an apparently valid U.S. visa – despite the fact that his United Kingdom visa had been cancelled a year earlier. Either of these suspicious circumstances should have alerted security inspectors that something was amiss.

Moreover, Abdulmutullab’s own father had actually warned the U.S. embassy in Nigeria that his son was a dangerous jihadist – nonetheless, the younger Abdulmutullab was not on the U.S. no-fly list or even on the so-called “secondary” screening list. Last but not least, he had passed through security in Amsterdam with no difficulty and was not given any special attention.

All of the preceding was in rather sharp contrast to the flight Richard Reid took on El Al in 2001. He and every item in his possession were thoroughly screened, and an undercover air marshal was assigned to an adjacent seat on the same plane. Because Reid seemed to be “just testing” El Al security, did not have any explosives or weapons with him, and had not manifested any unusual behavior, he was permitted to reach his destination without incident; but he was being carefully monitored every step of the way.

Profile & Interview: A Powerful Combination

Many people point to the Israeli aviation security system as a model for what the U.S. system *should* be. Others say that this is a bogus comparison because Israel operates only 43 planes serving 48 destinations. U.S. air carriers, in contrast, complete an average of about 28,000 flights per day. Nonetheless, there are still a number of helpful lessons that the United States can learn from the Israelis.

The backbone of the Israeli system is the profiling the Israelis use of each passenger. The profiling is accompanied by an interview during which a well trained security agent carefully questions the passenger, inquiring about such matters as to why he or she is traveling to Israel, where he/she is staying while in Israel, and who does he or she know in the country.

It was this patient methodology that unmasked the pregnant Irish woman with a bomb who attempted to board an El Al flight in London in 1986. The father of the unborn child was a Jordanian named Nizar Hindawi, who had told the woman that he wanted her to come to Israel to meet his family before they were married. He was not traveling with her – but it was he who had packed her bag. Sewn in the lining of the bag was an expertly crafted bomb packed with Czech-made Semtex explosive. The bag had been x-rayed several times, and nothing suspicious had been detected – but the security agent at the gate was nonetheless convinced, from her interview with Anne Mary Murphy, that there was something wrong. It was not until the security agent cut the lining of the bag open that the explosives were discovered.

The Israeli focus is less on guns and explosives than it is on people. As reporter Jeff Jacoby observed (in a 23 August 2006 article in *The Boston Globe*), the Israelis believe that “*things* don’t hijack planes, terrorists do, and ... the best way to detect

terrorists is to focus on intercepting not bad things, but bad people.” Hence, the Israeli emphasis on profiling and the interviewing of passengers. Indeed, the Israelis learned long ago that not all passengers should be accorded the same amount of screening. The real key to effective airport security, in their view, is reducing to a minimum the size of the pool of people being more than perfunctorily screened, and then spending whatever time is necessary on those individuals who fit the terrorist profile and/or fail the initial screening process.

The Egalitarian Triumph Over Common Sense

In contrast, the U.S. aviation security system is far more egalitarian – primarily because of political correctness, it seems obvious – than the Israeli system is, which means in practice that everyone receives more or less the same treatment. If a Muslim is pulled out of line for secondary screening, one observer commented, TSA (the U.S. Transportation Security Administration) employees will then select a dozen or more blonde women and/or harmless senior citizens for secondary screening so that no one can complain that he or she had been singled out by profiling or that the system is prejudiced against Muslim males in a certain age group.

Any objective analysis of the statistics developed over the last 10-15 years shows, though, that Muslim males between the ages of 17 and 35 – and from any of a short list of countries – represent by far the greatest threat to U.S. civil aviation. They should, therefore, be accorded most of the attention at airport checkpoints.

But the U.S. system does not work that way, unfortunately. This is not to say that the U.S. screening system should not be on continuing alert for the occasional aberration – and/or for the person who does not fit the profile. It already is well known that al Qaeda is attempting to recruit women, and Muslim men, from both the United States and Western Europe. One terrorist plotter arrested in the United States went so far as to change his Muslim name, Abdul Rahman, to a name, James Cromite, that sounds more Anglo-Saxon. As Jacoby also noted in his insightful 2006 article, “No sensible person imagines that ethnic or religious profiling alone can stop every terrorist plot. *But it is illogical and potentially suicidal not to take account of the fact that, so far, every suicide-terrorist plotting to take down an American plane has been a radical Muslim man* [emphasis added].”

Another way of reducing the number of people who need to be carefully screened would be through implementation of a Registered or Trusted Traveler program. One of the TSA’s more

obvious failures has been its inability to develop and implement an effective trusted traveler program – through which a passenger can elect to voluntarily provide certain personal data, including biometric information, to the government in order to pass through security at airports more rapidly and efficiently.

The Obvious Need To Rethink U.S. Aviation Security

The TSA has, in fact, authorized a number of pilot programs, in partnership with the private sector, to test the feasibility of setting up a trusted traveler program. “Clear,” the largest of the trial programs, ended operations last year when its parent company went out of business. The various other U.S. programs that have been tested thus far cost participants between \$100 and \$149 per year. In contrast, the British “IRIS” program not only is highly efficient but is also operated by the U.K. government – and is free of charge.

It is estimated that airport security now costs U.S. taxpayers more than \$6 billion a year – and that total does not include the work being done in this area by U.S. intelligence agencies, the Defense Department, and numerous law-enforcement agencies across the nation. So the question arises: Are the taxpayers getting their money’s worth? The answer is a resounding “No”! Some critics have described the present U.S. airport screening process as “security theater,” contending that there is little if any hard evidence that the system has ever actually thwarted any real terrorist attacks and that it exists mainly to reassure the flying public that there will be no repeat of the 9/11 terrorist attacks. Others, including many security specialists, suggest that the only real security improvements since the 9/11 attacks have been reinforcing cockpit doors in aircraft, reinvigorating the sky marshal program, and convincing passengers that they personally might have to fight back in the event of an incident on board.

What else needs to be done? All evidence suggests that nothing less than a complete overhaul of the current U.S. aviation security system will suffice – otherwise, the nation can anticipate additional aviation disasters in the future. If anything is certain from the intelligence gleaned from jihadists it is that civil aviation, in all its facets, remains their number one target when it comes to striking out at the United States and its Western allies. A number of captured hard drives, and other materials, suggest that various jihadist cells are still working – around the clock, and on a 24/7 basis – to find existing or new vulnerabilities that can be exploited not only at civilian airports throughout the country, but also in the now unfriendly skies over the entire world.



Rapiscan Systems - the Leading Provider of Security Screening Solutions

Security. Performance. Value. When it comes to your security needs, Rapiscan Systems understands the environment in which you operate – and knows how to protect it.

With the broadest range of products for checkpoint screening, perimeter security and personnel screening, we provide comprehensive, fully-integrated security solutions.

And with over 15 years experience, global expertise and a world class service and support network, we have the proven capability to meet your most demanding requirements – on time and on budget.

To learn more or to schedule a demonstration, contact us at 1-310-978-1457.



Rapiscan Secure 1000 Single Pose



Rapiscan 620DV



Rapiscan Eagle M60

Following is a brief list of *some* of the more obvious changes senior U.S. decision makers should at least consider:

(1) Improved Leadership at DHS & TSA: When DHS Secretary Napolitano said that “the system worked” at a press briefing shortly after apprehension of the so-called “underwear bomber” who had tried to blow up Northwest Airlines Flight 253 during its descent to Detroit on Christmas Day 2009, many critics – not only political opponents but security specialists as well – said she should be fired. More than three months later, that has not happened. It still seems obvious, though, that much improved leadership is needed both at DHS and at the Transportation Security Administration (TSA).

DHS also needs to be depoliticized – by, for example, the appointment of a senior advisor, not as a political reward, but because he or she is a career professional with considerable real-world working experience in civil aviation. What makes such an appointment even more imperative is that the new TSA director, retired Major General Robert A. Harding, has a long background in intelligence and is certainly a distinguished American, but has little in his resume to suggest that he is nearly as conversant on aviation security issues.

(2) Profiling: The United States should not only use ethnicity profiling, as the Israelis do, but make it the centerpiece of its aviation security system.

(3) Better Training for TSA Employees: In 2006, a man was detained by TSA employees in Milwaukee because he had written, on a plastic bag containing his toilet articles, the words “Kip Hawley [then the head of TSA] is an idiot.” Legally, though, Ryan Bird, the man who was detained, was simply exercising his First Amendment rights – and, not incidentally, also indicating his understandable disapproval of TSA’s inadequate security procedures. The TSA employees who detained him acted in a discriminatory and wholly unprofessional manner, claiming that they had to investigate whether or not those five words constituted an actual threat.

Another problem, as far too many passengers have learned, is that many TSA employees seem to be both bored and unhelpful, and have neither the training nor the interest needed to do their jobs at a consistently high standard of performance.

Another problem, as far too many passengers have learned, is that many TSA employees seem to be both bored and unhelpful, and have neither the training nor the interest needed to do their jobs at a consistently high standard of performance

Various published sources indicate that screeners routinely fail, on average, about seventy percent of the tests conducted by undercover agents attempting to smuggle weapons components and/or explosives through security checkpoints. In private tests conducted in connection with the already ongoing 9/11 litigation, to cite but one example, box cutters were regularly overlooked by TSA screeners unless the cutters had been laid flat on their sides in the hand luggage carried by the agents.

(4) A Trusted Traveler Program: For the reasons previously noted, top priority should be given to the creation and implementation of a “Trusted Traveler” program at all U.S. airports.

Even former TSA chief Kip Hawley strongly supported the idea. According to Hawley, “We believe that a nationwide Registered Traveler program can provide expedited screening for many travelers, and enhance aviation security as well.”

(5) Hardened Aircraft: The cargo and baggage holds, especially the former, of most U.S. carriers are perhaps the most vulnerable sections of any aircraft. The Israelis have hardened the baggage holds of their planes so that the force of an explosive device can at least be mitigated, thanks to the bullet-resistant materials used to absorb the blast effects and shrapnel, and to carefully designed “blast plugs” that release the pressure in the hold. Another option is to

use containers made of bullet-resistant materials. One study indicated that, although bullet-proof containers cost three times as much as current containers, they last four times as long.

(6) Improved “No Fly,” “Secondary Screening,” and “Terrorism Watch” Lists: It is estimated that, since their inception, the cost of compiling and maintaining these passenger-aviation lists has exceeded \$1 billion. However, Abdulmutallab, the underwear bomber, was not on the “no fly” list, or even on the secondary screening list – despite intelligence information suggesting that he might be a dangerous jihadist. The number of horror stories involving so-called “false positives,” or cases of mistaken identity, are legion. Comedienne Joan Rivers, whose name and face are easy to recognize, recently missed her flight from Costa Rica back to the United States because her passport lists her as “Joan Rosenberg AKA Joan Rivers” – an identification that apparently was more than the security screeners could process. Moreover, even the late Senator Theodore M. (Ted)

Kennedy was frequently stopped, despite the fact that he had one of the most recognizable faces in America, until he protested to the Secretary of DHS – and even then it still took three weeks for the issue to be resolved.

Among many others who were similarly detained or delayed have been U.S. soldiers returning from Iraq or Afghanistan, children under the age of five, members of Congress, actors, journalists, and just plain everyday citizens with no connection whatsoever to terrorism. One would think that, for an investment of more than \$1 billion, the various watch lists could be properly assembled and maintained – especially since the “no fly” list at the time of Abdulmutallab’s capture contained only about 3,400 names and the “secondary screening” list an estimated 16,000 or so.

Another area that needs reform is the State Department’s role in issuing visas. Abdulmutallab should never have been issued a visa to begin with, and after his radical views were identified his visa should have been cancelled. The State Department has a poor track record in general when it comes to issuing visas to terrorists. The so-called “Blind

Sheikh,” Omar Abdel-Rahman – who was linked to many violent attacks, including the Sadat assassination and the first bombing (in 1993) of the World Trade Center – was issued a tourist visa to the United States despite being on the terrorism watch list. The State Department later said that an error had been made in the transliteration of his name. However, he was not expelled from the United States even after he issued a fatwa, or religious decree, in this country saying that it is permissible to kill Jews and even rob banks.

(7) New Technologies: New technologies are not a panacea in themselves, of course, in terms of airport security. Yes, full body scanners *might* have discovered the bomb inside Abdulmutallab’s underpants, but it seems unlikely. Nonetheless, as so-called “sniffers” and other bomb-detection technologies become ever more sophisticated, they can and should be introduced at U.S. airports. But they represent only one facet of what should be a seamless overall security system, involving everything from profiling to watch lists, better visa controls, stronger aircraft, trusted traveler programs, and improved intelligence.

USA MADE RADIATION DETECTORS ✨ SURVEYING THE WORLD WITH QUALITY



Inspector EXP+

The Radiation Alert® Inspector EXP+ is designed for the requirements of emergency response personnel. It has the same valuable features, small size, and high quality of the Inspector, but with an external probe and settable alert.

The carrying case provides a full view of the readout and access to the switches, as well as a convenient belt loop for carrying the instrument. The unique design of the carrying case allows one-handed operation and a small check source pocket.

SENTRY

The Radiation Alert® Sentry is a Personal Alarming Dosimeter / Ratemeter designed to ensure the safety of personnel that work in occupations with potential x-ray or gamma exposure.

The pocket size unit has built in memory for tracking accumulated exposure. The optional software enables you to easily set the vibrating and audio dose/dose rate alarms and generates incident reconstruction for analysis.



SE INTERNATIONAL, INC

RADIATION A • L • E • R • T



S.E. International, Inc.

P.O. Box 39, 436 Farm Rd. Summertown, TN 38483

1-800-293-5759 | Fax: 931-964-3564

www.seintl.com | radiationinfo@seintl.com



(8) Improved Intelligence Collection and Sharing: As with the intelligence failures associated with the 9/11 attacks, the failure of the U.S. intelligence community to anticipate and identify Abdulmutallab represents a major embarrassment, especially since the United States spends an estimated \$75 billion a year on the sixteen intelligence agencies that constitute the U.S. intelligence community as a whole. Once again, there were charges of not being able to “connect the dots,” and even today it seems clear that intelligence sharing between and among federal agencies falls far short of optimal.

(9) Improved International Cooperation: The international civil aviation system is only as strong as its weakest link. This writer witnessed security screening in a West African nation where all hand luggage was placed on a moving belt – but was not actually screened because: (a) the x-ray machine had not been turned on; and (b) both of the “security agents” present were sitting on nearby chairs, smoking whatever it was they had in their pipes. What made that situation worse is that anyone who passed through security in that country was automatically inside the *international* civil aviation system, because one of the departing flights went to Charles de Gaulle airport outside of Paris, where passengers were not screened again and therefore could easily have boarded other flights – to other European destinations or even the United States – with little trouble.

What makes this problem even more difficult is that not all nations follow the same uniform screening practices – the Israelis, for example, do not make passengers remove their shoes. Moreover, both the “shoe bomber” and the “underwear bomber” were on flights originating in Europe – and neither of them was discovered to be carrying explosive devices before boarding. Considerably more effort must be expended, obviously, both in developing uniform procedures and by adopting common technologies to screen passengers. There also should be better and more streamlined intelligence sharing, and the international community should give careful consideration to requiring both Airbus and Boeing to harden all of their new aircraft in accordance with new uniform specifications. In addition: (a) Aviation terrorists should be dealt with severely by all countries; and (b) All nations must be required to comply with all extradition requests in matters involving aviation-related crimes.

(10) Speedy Trials and Executions: A vast majority of Americans agree that it was a serious mistake to “Mirandize” Abdulmutallab and many of the other terrorists apprehended

in connection with plots against U.S. civil aviation. A key component of the Miranda warning is informing the suspect that he or she has the right “to remain silent” – but in real-life situations it is vitally important that a suspected terrorist be interrogated both quickly and effectively. Unless they are American citizens, therefore, terrorists should be regarded as “enemies of all mankind” – just as pirates were, under British admiralty law, beginning in the 18th century. Moreover, because of the heinous nature of piracy, it was understood to be a crime that, under the concept of universal jurisdiction, *any* nation could punish, usually summarily and with a considerable degree of finality. It should be the same in terms of how the United States and other nations deal with aviation pirates and bombers. In short, they should be tried, very quickly, before military tribunals, and if found guilty should be executed as soon as possible.

In the final analysis, the current U.S. civil aviation security system needs to be upgraded and improved at almost every level. The present system, according to one observer, catches only “the sloppy and the stupid.” However, a well-conceived and well-executed terrorist operation aimed at dozens of airports and/or flights around the world could potentially kill many more people than the 3,000 who died on 9/11 – and quite possibly might even shut down international travel and commerce for several weeks, or even months, thereby plunging the world into an even deeper and more far-reaching recession, perhaps even a depression.

Al Qaeda recognized long before 9/11 that the chief source of U.S. military and political power is the nation’s economic power – and that was what the organization was targeting in the attacks against the World Trade Center towers in 2001. Should the U.S. economy seriously falter, the United States would be unable to support U.S. (and allied) military and naval forces around the globe, especially those in the relatively moderate regimes in the Middle East that produce so much of the world’s oil. The United States should not, and *must* not, let that happen.

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. A gifted speaker as well as writer, he has made more than 1300 television appearances, delivered over 500 speeches both in the United States and overseas, and testified before Congress on numerous occasions. He holds three Masters Degrees as well as a Ph.D. from the Fletcher School of Law and Diplomacy. 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.

They Expect You To Be More Than 80%* Prepared for a Biological Threat



Now You Can Be with the New **RAZOR™ EX**



RAZOR EX

Field Portable BioHazard Detection System

Less than 1% error rate

Screen ten targets in a single run with The 10™ Target Kit

Used by Military, Hazmat, and First Responders

The 10™ Target Screen Kit:

Anthrax	<i>E. coli</i> O157	<i>Salmonella</i>
<i>Brucella</i> spp.	Tularemia	Smallpox
Botulism	Ricin	Plague
<i>Coxiella</i>		



Call **1.800.735.8544** or visit www.idahotech.com to discover how you can reliably protect those you serve.

*Most other field biohazard detectors have a 20% error rate.



390 Wakara Way, Salt Lake City, UT, 84108, USA | 1-800-735-6544 | www.idahotech.com

The PPE & Other Basic Needs of Tactical Officers

By Richard Schoeberl, Law Enforcement



Law enforcement faces a myriad of challenges when responding to hazardous situations. In the wake of intelligence that al Qaeda is relentlessly pursuing the development or purchase of WMDs (weapons of mass destruction) – coupled with the fact that the United States has received a failing grade in the preparedness to respond to a WMD threat – it is more important than ever before to have “Hazmat-Ready” tactical teams across the country.

Recently, a bipartisan panel – i.e., *The Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism* – was established by Congress for the sole purpose of addressing the threat a WMD attack poses to the United States. The panel issued a failing grade to the nation as a whole on its lack of preparedness to handle a biological, nuclear, or chemical weapon attack. More specifically, the report, released on 2 January 2010, states that, “Of 17 grades, the report card includes three failing ‘F’ grades on: (a) rapid and effective response to bioterrorism; (b) Congressional oversight of homeland security and intelligence; and (c) national security workforce recruitment.”

The study is almost surreal in some respects, primarily because it comes almost a full decade after both the terrorist attacks of 11 September 2001 that killed close to 3,000 U.S. citizens and the anthrax attacks, shortly thereafter, that left several more Americans dead and a number of others infected when letters were mailed to U.S. Senators and several media offices. If the Commission’s study is accurate, it is in agreement with other assessments that the government is not progressing in the right direction and, furthermore, failing to take the countermeasures needed to shelter the nation from the horrendous threats posed by a WMD attack.

One of the panel members, former U.S. Senator Bob Graham (D-Fla.), pointed out that “. . . we no longer have the luxury of a slow learning curve when we know al Qaeda is interested in bioweapons. In a time where we already sit on guard awaiting al Qaeda’s next attempted attack, we still find ourselves playing catch-up in an effort to get ahead of the curve. If we sit idle and unprepared, we will find ourselves reacting to another attack instead of being proactive.”

The Rapid Growth of an Ancient Threat

Terrorism has been in existence for thousands of years, and the progressive growth, particularly in recent years, of the means

to terrorize has evolved immeasurably. Looming in the wake of intelligence that al Qaeda has been attempting to obtain biological weapons, it is difficult to believe that the United States is still not prepared to respond effectively to the threats posed by modern terrorism. Moreover, despite the fact that al Qaeda’s efforts to terrorize the United States and U.S. allies continue, the nation’s law-enforcement community is still not prepared to handle, much less respond effectively to, an attack using biological, nuclear, or chemical weapons.

What is perhaps even more unsettling is that, despite spending billions of dollars on equipment and training, the United States is still far behind in developing, and practicing, the countermeasures needed to respond to and combat a WMD attack. When, not if, another attack occurs it will almost assuredly be delivered in such a way that the first responders to arrive on-scene would have to have been tactically trained in order to effectively neutralize the threat they encounter.

Since the inception – in Los Angeles, in 1968 – of the first SWAT (Special Weapons And Tactics) team, thousands of law-enforcement agencies and organizations throughout the world have developed similar units of their own. The tests facing SWAT teams today vary greatly, of course, from response to response and from one nation to another. Typically faced with a barricaded subject – e.g., in a narcotics raid or bank robbery – the training needed and the responses recommended for SWAT teams drastically changed in the wake of the 9/11 attacks against the United States.

Moreover, knowing that al-Qaeda is actively seeking to obtain chemical and/or biological weapons, SWAT members are now faced with the problem of responding to terrorist incidents while outfitted in special gear. Although WMD attacks are not yet a common threat, SWAT members know they must be diligent in their training so long as al Qaeda continues its efforts to acquire WMDs.

The Dilemma: How to Respond to a Changing Scenario

In short – and there should be no mistake about it: The threat posed by WMDs is real – some would say imminent – and the efforts by terrorist groups to acquire nuclear, biological, and/or chemical weapons or devices have increased dramatically in recent years. For that reason alone, tactical officers throughout

the country must not only be in position to respond to assailants using WMDs, they also must be prepared to operate and work in an environment contaminated by a possible dirty bomb or a biological or chemical weapon.

Preparing to respond to a nuclear, chemical, or biological crime scene has become a new and immensely serious undertaking for tactical officers – partly because, until recently, the response to WMD “incidents” was usually left up to technicians who were both equipped and trained to handle the dangers associated with a situation involving hazardous materials. In recent years, however, because of issues over and beyond response – the task of clearing and securing the incident scene, for example, and the preservation and collection of evidence – law-enforcement agencies have been required to train, and use, tactical officers outfitted with various types of protective gear, specifically including personal protective equipment (PPE).

Today, however, when responding to a WMD incident, traditional first responders such as firefighters and EMTs (emergency medical technicians) cannot be expected to also carry out the duties of tactical law-enforcement officers. In the current more rigorous operational climate, therefore, law-enforcement officers must themselves be prepared to meet the challenges associated with a WMD threat – and those who are not tactically trained when arriving at the scene will not be prepared to address the full situation and, in all likelihood, will ultimately be added to the rapidly growing list of casualties.

Greater Danger, Plus an Escalating List of Tasks

Because tactical officers generally tend to receive more training time than most other first responders, they also would be better suited at responding to a WMD situation and would be able to contain the scene more rapidly than their colleagues in other disciplines could. The first responders on the scene not only must be prepared to handle the dangers presented by the hazardous material itself, but also should be equally prepared to carry out that important task – while at the same time coping with a chemical or biological agent, apprehending the perpetrator (if and when possible), securing the scene, and preserving evidence. A typical hazmat unit is very seldom prepared or equipped to carry out any of these tasks.

A typical scenario that might be faced: Smoke and poisonous gas bellow out from a crowded shopping mall as patrons mass-exit into the streets. Local police and fire departments respond to the scene in an effort to neutralize the situation – only to learn that an undetermined number of men are inside, some of

them armed with guns, and others strapped with bombs and/or quick-release gas canisters containing an unknown but presumably lethal type of powder. Police learn that the men inside also have several hostages with them.

Traditionally, the first responders responding to this scenario would be patrol officers and firemen. However, faced with the realization that armed men are concealed within a shopping mall, holding an unknown number of hostages as well as an unidentified biological weapon, timing is obviously of the essence. Whether law enforcement is faced with a lone-wolf scenario in a shopping mall or a credible attack from al Qaeda operatives possessing WMDs, rapid response and deliberately violent action from a prepared and well trained tactical team can make all the difference between a mass-casualty outcome and a safely contained scene.

Too Many Complications, Not Enough Time

In accordance with Presidential Decision Directive 39, the Federal Bureau of Investigation is the lead federal agency assigned to coordinate all aspects of the federal response to a WMD incident. Each of the FBI’s 56 field offices is assigned a WMD coordinator – who has established relationships with his or her regional, state, and local counterparts. Should an incident happen – or if there is a reasonable suspicion of an incident happening – it would be the WMD coordinator’s responsibility to find out what exactly is going on, with the information provided, in most cases, via radio or other communications with his or her counterparts.

After the communications connection has been established, the coordinator alerts the WMD Directorate at FBI headquarters about the incident and a conference call is arranged between the local field office and the senior-level decision makers at FBI headquarters. It is then determined what federal resources, if any, should be deployed to the scene of the incident.

Timing is critical when one is talking about the spread of contamination and/or containment of the incident scene. In the wake of new intelligence, the time it takes to coordinate a response from an FBI field office to FBI headquarters and back is frequently not acceptable. “Rapid deployment” means precisely that: *rapid* deployment. There simply would not be enough time, in many plausible scenarios, to discuss and debate various options through the chain of command and/or determine who should make the key decisions when the immediate concern is containing the WMD scene itself. In other words, in many if not quite all situations the most important as well as immediate

objective is neutralizing and containing the threat as quickly and as efficiently as possible.

The Capabilities and Responsibilities Of Local & State Agencies

Local and state agencies also do not have time to linger when responding and neutralizing the scene. It is crucial, therefore, that they also be prepared to secure the scene – even prior to the federal government’s response.

Local and state resources obviously should work in close cooperation with federal agencies, though, particularly on such important matters as responding to and containing a WMD incident. Another factor to consider is that federal agencies simply do not have the luxury of rapid-response capability that local and state agencies (already on or closer to the scene) usually possess. Moreover, there is no doubt that the fallout effects of a WMD event will almost always overwhelm local resources – for at least three reasons: (a) the massive number of casualties likely; (b) the nature of those casualties; and (c) the decontamination efforts needed. However, by combining resources through properly coordinated efforts an efficient and usually acceptable end result can be effectively achieved.

In their efforts to prepare for a WMD attack many members of tactical units across the globe have been training for that unfortunate day that they hope never comes. It is training, moreover – repeated, thorough, and effective training – for a WMD catastrophe that is the most crucial aspect of a truly effective response. An additional major problem, though, is that most tactical teams are currently outfitted with obsolescent military equipment, possess inadequate levels of protection, and are limited to only a few days a year in which to train and prepare for a WMD attack. (In contrast, sports franchises do not expect the professional athletes who work and play for them to train for only a few days a year and then perform without mistakes.)

The bottom line is that tactical officers and other responders should not be expected to don their protective equipment for only a few days each year in order to respond, quickly and effectively, to a life-threatening WMD incident that might not only result in mass casualties but also cause the destruction of critical infrastructure. Proper training not only allows these officers the ability, and opportunity, to adjust in and adapt to a toxic environment, but also enables them to make educated decisions based on the hard-earned experience developed in training.

Protecting the Protectors: A Few Guidelines

Respiratory protection is probably the single most important piece of chemical-agent equipment needed by most SWAT officers. It is as important as the weapons they are carrying and/or the Kevlar vests they are wearing. Operators should be outfitted with PPE (personal protective equipment) that meets OSHA (Occupational Safety and Health Administration) standards and still allows the operator to be fully functional – without compromising his or her stealth movement. One of the greatest complaints voiced by many operators is that PPE slows down movement, and for that reason the effectiveness of some operators deteriorates after three hours or so of operation, and their judgment is sometimes impeded as well.

Ideally, therefore: (1) PPE should be so carefully designed and fitted that it enables the operator to deploy immediately without wasting too much time getting dressed; (2) PPE also should be “comprehensive” in the sense that it allows the wearer to be protected from *all* toxic agents – whether chemical, biological, or radioactive; and (3) The PPE worn should complement rather than impede the other equipment that operators will initially be wearing or carrying.

To briefly summarize: SWAT or tactical officers are called to the scene not only to mitigate a threat but also to contain, preserve, and secure the incident scene. No matter where the threat comes from, foreign or domestic, each team must face its own set of unique circumstances and, usually, possess at least the minimal abilities needed to equalize the situation. It is therefore increasingly important to understand, particularly in an era when the highest threat level in U.S. history is a frequent occurrence, that the nation: (a) equip and outfit its most critical resources – the first responders themselves – with the best possible training and equipment available; and (b) give them the time needed to train both thoroughly and effectively. Moreover, during a period when it seems entirely possible that more terrorism-related cases may well be tried in civil court, it becomes even more important for responses to be carried out with tactical officers factored into the equation.

For additional information on the Commission study mentioned above, refer to: The Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism, 2010.

Richard Schoeberl has over 15 years of counterintelligence, terrorism, and security management experience, most of it gleaned from his career with the Federal Bureau of Investigation, where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the National Counterterrorism Center. During most of his FBI career he served in the Bureau’s Counterterrorism Division, providing oversight to the FBI’s international counterterrorism effort.

To hell and back home again.

"My job involves risks. But no risk is worth taking if I don't get back home to my family. That's why I carry DuoDote."¹



DuoDote has replaced the Mark I™ Kit using advanced dual-delivery technology¹

- Optimizes response to chemical nerve agents^{2,3} by delivering both atropine and pralidoxime chloride in a single auto-injector
- Counteracts the life-threatening effects of a wide range of organophosphorus nerve agents and organophosphorus insecticides¹
- Offers the same advanced technology used by the U.S. military and allied nations worldwide⁴

Please visit www.DuoDote.com or call 1-800-638-8093 for more information.

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

Preparing for the unexpected.



MERIDIAN
MEDICAL TECHNOLOGIES

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.

© 2007 Meridian Medical Technologies™, Inc., a subsidiary of King Pharmaceuticals®, Inc. DuoDote™ Auto-Injector, Mark I™ Kit, and the DuoDote Logo are trademarks of Meridian Medical Technologies™, Inc. MMT 5173 11/07

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/MMGL/mmgl166.html>. Accessed February 21, 2007. 3. Holstoge CP, Dotzeimer SG. Nerve agent toxicity and treatment. *Curr Treat Options Neurol.* 2005;7:91-98. 4. Data on file. Columbia, MD: Meridian Medical Technologies™, Inc.



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.

EVAUATION AND DECONTAMINATION PROCEDURES SHOULD BE UNDERTAKEN AS SOON AS POSSIBLE. MEDICAL PERSONNEL ASSISTING EVAUATED 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 \pm 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 parathionophenol 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/m² 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 scarlatiniform 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, or 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™

© 2007 Meridian Medical Technologies™, Inc., a subsidiary of King Pharmaceuticals®, Inc.
Manufactured by: Meridian Medical Technologies™, Inc.
Columbia, MD 21046
DuoDote™ Auto-Injector and the DuoDote Logo are trademarks of Meridian Medical Technologies™, Inc.
MMT 5173 11/07

ICD – Shorthand for a Potentially Ubiquitous Threat

By Joseph Cahill, EMS



The acronym CBRNE stands for chemical, biological, radiological, nuclear, and explosive – and is used by responders as shorthand for what also are called weapons of mass destruction (WMDs).

Because there have been so many CBRNE incidents in Iraq and Afghanistan in recent years the phrase improvised explosive device, or IED, also has become part of the modern American military lexicon. The term “dirty bomb” usually refers to a radiological weapon or device – another very real threat in the age of terrorism – and is now part of the common vocabulary as well. So far, though, the threat posed by an improvised *chemical* device, or ICD, is not quite so well known.

That could change in the very near future. The destructive potential of an ICD, placed covertly by a terrorist organization, has been recognized by first-responder agencies for over a decade. The ICD threat is not only substantial but also ubiquitous and relatively low in cost. The reason is simple: Like IEDs, ICDs can be made primarily from materials commonly available in most communities throughout the country. Those communities include numerous small towns and literally hundreds of rural hamlets and villages throughout the United States, where chemicals toxic enough to be a significant hazard are usually available for purchase. Other common chemicals, available for over-the-counter purchase at local grocery stores, can also, when mixed properly, produce a toxic cloud of poison gas.

As with IEDs, ICDs can range in size from a small localized device that affects only those in a specific building, or a small room or compartment – e.g., in a subway station or delivery truck – to a rail car-sized attack that could cripple and contaminate a major section of a large city.

EMTs (emergency medical technicians) and their leaders must be much more aware of chemical hazards and threats in the future than they have been in the past. Fortunately, there are five operational principles to follow that can and should be easily remembered: (1) a 10-second scene survey; (2) scene demarcation and control; (3) decontamination; (4) affirmative treatment; and (5) communications across silos.

Close Observation, Common Sense & Reliable Communications

In the microcosm of the individual ambulance or EMT, the first and best defense against an ICD attack is a combination of close observation and common sense. Every responder should perform a 10-second scene survey – which means, in everyday language, taking a quick look at the scene of an incident, checking for any hazards that might be evident, before the ambulance pulls in to the

curb. Any EMS unit that arrives on scene, for example, and sees a number of people on the ground without an obvious cause, should and would be super-cautious. The same principle holds true when responding to a report of an explosion or an unusual smell. These and other common-sense clues should be warning enough to put on the brakes and look before leaping. In short, just a 10-second look should be enough to give the responders the opportunity to personally survive to carry out their mission of saving the lives of the victims of the incident.

Fire and hazmat staff also should quickly establish the edges of the contaminated – i.e., “hot” – area and mark it off (the “scene demarcation and control” task mentioned previously) to prevent accidental exposure after their arrival. Law-enforcement personnel also may assist by maintaining the boundary from the clean (cold) side. The warm zone usually can serve as a buffer between the cold and hot zones in which responders can clean or decontaminate the victims. It also is in this area that EMTs can, if properly trained and equipped, start evaluating patients and providing non-invasive care.

The macrocosm of the EMS system requires that EMTs and other responders – as well as emergency managers and other decision makers – must continue to pursue better detection and treatment options. Being astute enough to pull back from a hazard is acceptable only until backup personnel with appropriate skills and equipment arrive at the scene.

A constant feature of after-action reports – derived from drills and training exercises, as well as from real events – is the need to improve communications. Here there should be not only inter-unit communications connecting unit to unit but also inter-agency and system-wide communications so that, when one agency or jurisdiction is aware of a threat, that same threat also is on the radar of all of the other parties potentially affected.

To briefly summarize: The ICD threat is not only one of the most obvious nightmare scenarios confronting the EMS community today but also, in all likelihood, the one with the greatest growth potential – because the materials needed to make an ICD are readily at hand in the community. Fortunately, most of the resources needed to respond to the ICD threat are locally available as well.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS.

DomPrep Survey

Your Thoughts Compared with DomPrep40's National Experts on...The Chemical Threat & the State of Chemical Preparedness

Prepared by Major General Stephen V. Reeves, USA (Ret.); Summarized by John F. Morton, DP40



This DomPrep survey on U.S. chemical preparedness (and the steps needed to improve it) finds DomPrep members very much in synch with the views of the DomPrep40. Both groups are highly attuned to the chemical threat and what it might mean for local emergency managers. Moreover, although local jurisdictions may consider a chemical warfare agent or TIC/TIM (toxic industrial chemical/toxic industrial material) event as high-consequence/low-probability, they do not necessarily have the time, talent, and financial resources needed to apply to increasing local preparedness for such events.

The chemical threat is real; [U.S.] chemical preparedness is inadequate – what is most needed now are government standards for chemical detection equipment and an “approved products list” for DHS (Department of Homeland Security) grant funds

“Much more can be done in policy and process at the national level to help local emergency managers be better prepared,” says DomPrep40 member Major General Stephen V. Reeves, USA (Ret.), the Pentagon’s former Joint Program Executive Officer for Chemical and Biological Defense, who prepared the survey. Citing the use of chemical detectors as an example, General Reeves comments that, “We can’t leave most local emergency managers on their own to determine what an acceptable standard is. This survey was an attempt to arrive at a consensus on the policy and process holes which – if filled – can help a local emergency manager make better decisions and be better prepared.”

Key Findings: DomPrep members validated the sharply defined consensus view of the DomPrep40. The chemical threat is *real*. Chemical preparedness is *inadequate*. What is most needed now are government standards for chemical detection equipment and an “approved products list” for DHS (Department of Homeland Security) grant funds.

The DomPrep40

The DomPrep40 is an interactive advisory board of insider practitioners and opinion leaders who have been asked to offer advice and recommendations on pertinent issues of the day. Focusing primarily on all-hazard preparedness as well as response and recovery operations, they will be challenged to provide quantifiable feedback that will be shared with the DomPrep audience.

DomPrep40 Members

John Morton

Strategic Advisor

James Augustine

Chair, EMS & Emergency Department Physician

William Austin

Chief, West Hartford Fire Department (West Hartford, CT)

Ann Beauchesne

Vice President, National Security & Emergency Preparedness Department, U.S. Chamber of Commerce

Joseph Becker

Senior Vice President, Disaster Services, American Red Cross

Bruce Clements

Public Health Preparedness Director, Texas Department of State Health Services

John Contestabile

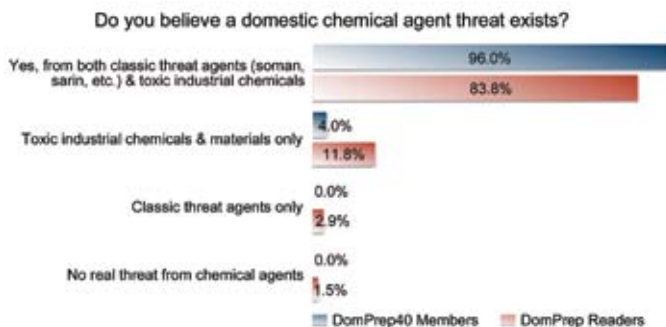
Former Director, Engineering & Emergency Services, Maryland Department of Transportation

Craig DeAtley

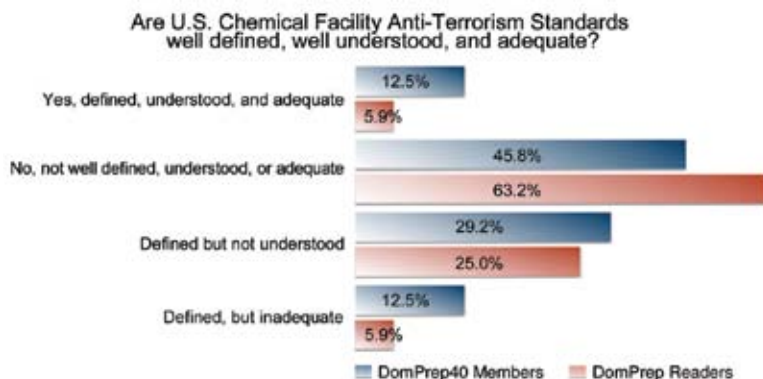
Director for Institute for Public Health Emergency Readiness

Following are the survey results

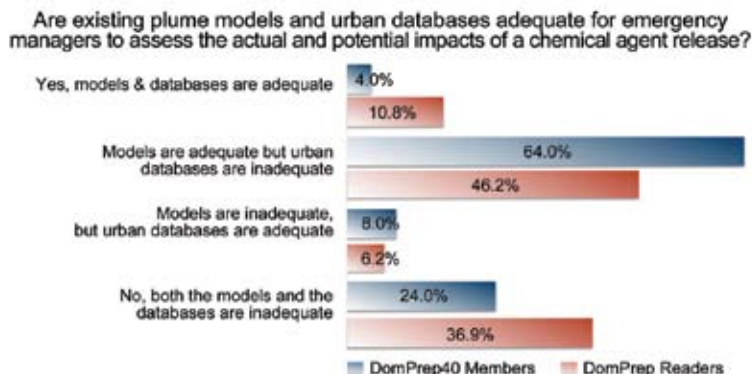
DomPrep members agreed very conclusively – at almost 84 percent – with the DomPrep40 opinion that a domestic chemical agent threat already exists.



An extremely low percentage of members – just under six percent – say that current Chemical Facility Anti-Terrorism Standards (CFATS) are well defined, well understood, and adequate. But well over 90 percent disagree with that hopeful assessment, so Yes, there is much more work that must be done in this area.



Members also support the DomPrep40 view that greater attention is needed, on primarily urban databases, on the potential impact of a chemical release.



DomPrep40 Members

Nancy Dragani

Former President, National Emergency Management Agency (NEMA), Executive Director, Ohio Emergency Management Agency

Warren Edwards

Major General USA (Ret.), Director, Community & Regional Resilience Institute (CARRI)

Katherine Fuchs

Deputy Chief FDNY Emergency Medical Services Command

Ellen Gordon

Member, Homeland Security Advisory Council and Naval Postgraduate School Center for Homeland Defense Security

Kay Goss

Former Associate Director, National Preparedness Training & Exercises, FEMA

Steven Grainer

Chief, IMS Programs, Virginia Department of Fire Programs

Jack Herrmann

Senior Advisor, Public Health Preparedness, NACCHO

Cathlene Hockert

Continuity of Government Planning Director, State of Minnesota

James Hull

Vice Admiral USCG (Ret.), former Commander, Atlantic Area

Harvey Johnson, Jr.

Vice Admiral USCG (Ret.), former Deputy Administrator & Chief Operating Officer, FEMA

Dennis Jones, RN, BSN

Executive Consultant, Collaborative Fusion Inc.

Robert Kadlec

Former Special Assistant to the President for Homeland Security and Senior Director for Biological Defense Policy

The table below represents a combination of the DomPrep40 and DomPrep Readers responses to other questions asked in the survey. Several additional conclusions, based on the answers indicated in the table, become evident, including the following: (a) somewhere between two-thirds and three-quarters say that the United States currently lacks a reliable means of attribution; (b) over three-quarters say that DHS should change its policy on regulating chemicals of interest; (c) only about 12 percent are satisfied with the detection tactics, techniques, and procedures (TTPs) used by the Environmental Protection Agency (EPA) for chemical incident decontamination (again, there is much work to do); (d) with only one out of five believing there are adequate training programs that use live chemical agents, members are less confident than their DomPrep40 colleagues are about this key area; and (e) finally, there is agreement here – with members and the DomPrep40 both registering four out of five in their opinions – that the Chemical Safety Board should require industry to report all chemical incidents.

	Yes		No		Unsure	
	DomPrep40 Members	DomPrep Readers	DomPrep40 Members	DomPrep Readers	DomPrep40 Members	DomPrep Readers
Are adequate systems and processes in place addressing attribution as a means of identifying the nature and source of materials, the perpetrators, and the methods of chemical attacks?	4.0%	13.2%	72.0%	61.8%	24.0%	25.0%
The U.S. Department of Homeland Security (DHS) does not currently plan to regulate railroad facilities that are used to store, in rail cars, large quantities of chemicals or materials on the DHS "chemicals of interest" list. Should DHS change its current policy and undertake such regulation?	76.0%	79.1%	16.0%	13.4%	8.0%	7.5%
Has the Environmental Protection Agency developed adequate detection technologies, plans, and protocols - including the development of risk-based clean-up goals - to decontaminate following a chemical incident?	12.0%	11.9%	48.0%	55.2%	40.0%	32.8%
Should the Federal Government set standards and require independent testing and validation of commercial chemical-detection equipment?	76.0%	83.3%	12.0%	10.6%	12.0%	6.1%
Should the Department of Homeland Security establish an "approved products list" for the use of DHS grant funds?	60.0%	64.5%	28.0%	16.9%	12.0%	18.5%
Is there sufficient scientific research on low-level exposure to toxic chemicals and materials on civilian populations?	4.0%	9.1%	56.0%	72.7%	40.0%	18.2%
Are there adequate training facilities - using live chemical agents - for first responders and emergency managers?	24.0%	20.9%	68.0%	74.6%	8.0%	4.5%
Is the United States sufficiently engaged with Canada & Mexico to prevent chemical incidents in either of those countries from crossing U.S. borders?	0.0%	3.0%	72.0%	71.6%	28.0%	25.4%
Should the Chemical Safety Board require industry to report all chemical incidents?	80.0%	77.6%	20.0%	11.9%	0.0%	10.4%

In short, the chemical preparedness survey provides a compelling consistency across and between the DomPrep40 and DomPrep members. DHS therefore may want to take note: This quantitative sampling of opinion among homeland security professionals indicates that U.S. chemical preparedness must still be considered, at best, a work in progress. But the same survey also suggests several specific remedies in such areas as standards, regulations, training, and scientific research.

DomPrep40 Members

Neil Livingstone

Chairman & CEO, Executive Action

James Loy

Admiral USCG (Ret.), former Deputy Secretary, DHS

Adam McLaughlin

Preparedness Manager, Port Authority of NY & NJ (PATH)

Vayl Oxford

Former Director, Department of Homeland Security's Domestic Nuclear Detection Office (DNDO)

Joseph Pennington

Senior Police Officer, Houston Police Department

Stephen Reeves

Major General USA (Ret.), former Joint Program Executive Officer for Chemical & Biological Defense, DOD

Richard Schoeberl

Former Executive, Federal Bureau of Investigation & the National Counterterrorism Center

Dennis Schrader

Former Deputy Administrator, National Preparedness Directorate (NPD), FEMA

Robert Stephan

Former Assistant Secretary of Homeland Security for Infrastructure Protection

Joseph Trindal

Former Director, National Capital Region, Federal Protective Service, Immigration & Customs Enforcement (ICE)

Theodore Tully

Director, Trauma & Emergency Services, Westchester Medical Center (Westchester County NY)

Craig Vanderwagen

Former Assistant Secretary for Preparedness & Response, U.S. Department of Health & Human Services



SARATOGA®
Unparalleled Protection.

The **ONLY** chemical protective overgarments approved by DoD for all US Joint Forces.

**THE MOST TESTED AND TRUSTED
TECHNOLOGY IN THE WORLD.**



TEXSHIELD
CBRN PROTECTION



(202) 973-2858
info@tex-shield.com

Surgically Implanted Death

Human IEDs vs. Full-Body Scanning

By Joseph Trindal, Law Enforcement



Terrorist patterns of adaptation continue to present challenges for the emergency services community worldwide. In the 1980s the number of terrorist suicide/homicide bombings was rapidly increasing and spreading. Terrorist tactics almost exclusively involved person-borne and vehicle-borne delivery of improvised explosive devices (IEDs). Some terrorist groups led the way toward adaptation, and most others followed. Death tolls escalated and the tactics spread on a global scale.

The reason this is relevant now is that the United Kingdom's Secret Service (MI-5) recently released intelligence-based warnings that Islamic jihadists – many of them trained in Western colleges and universities as medical professionals (surgeons, for example) – may soon play a major role in preparing and launching the next wave of terrorist attacks against the West.

Similarly, hijackings for the use of commercial aircraft as weapons against a target population were a relatively new tactic nearly a decade ago. Today, though, the use of either privately owned or commercial aircraft is but one of many “delivery” options available to terrorists and/or mentally disturbed persons alike. Even an angry taxpayer may be willing to resort to airborne suicide attack – as recently proved by the attack on the U.S. Internal Revenue Service offices in Austin, Texas.

Reid's Shoes & Christmas Day Underwear

Another example of how terrorists learn from experience: The “shoe bombing” tactic used by Richard Reid and his support network in the failed 2001 attack was unique at the time. Even though U.S. airport security was on high alert – it was still only a few months after the 9/11 attacks against the World Trade Center towers and the Pentagon – Reid was able to pass through screening at Charles De Gaulle Airport in Paris with explosives concealed in his shoes, which were built to circumvent metallic detection devices – and which were then very seldom checked by security inspectors.

About four years ago, adapting to Israeli's advanced security inspection techniques, the Hamas and Hezbollah terrorist groups came up with the idea of using “underwear bombs.”

Countering this terrorist adaptation, Israel developed counter-measures to more easily thwart this still emerging tactic. In an urban application of martyrdom-delivered explosives, the size of a main charge sufficient to inflict mass casualties poses a challenge to underwear concealment methods.

However, combining the construction of non-metallic explosive devices with underwear concealment methods apparently was Umar Farouk Abdulmutallab's intended tactic of choice in his failed Christmas 2009 attempt to bring down Northwest Airlines Flight 253 over Detroit, Michigan. The construction of the device, coupled with the concealment method used, is yet another example of how terrorist groups continue to adapt their tactics to circumvent improved security measures.

A few months earlier (in August 2009), al Qaeda adapted the smuggling techniques used by drug traffickers in Abdullah Asieri's assassination attempt against Prince Mohammed Bin Nayef, Saudi Arabia's chief of counterterrorism operations. Armed with an estimated 2kg of explosives secreted in his body cavity, Asieri, a wanted terrorist, failed operationally – but strategically raised the bar another notch for counterterrorism security officials.

The United States and many other countries are now accelerating the installation and use of body scanners in the nation's airports to counter additional Abdulmutallab-style attacks. The recent MI-5 warning strongly suggests, though, that the next step in terrorist circumvention techniques may be the surgical implantation of explosives deep inside the bomber's body.

A Deadly Game of Chess – With No End in Sight

The possibility that the jihadist recruiting of Western-trained surgeons adhering to radical ideology may be to use their specialized skills to surgically implant high-impact explosives into the body of a suicide attacker should not be dismissed as improbable or unlikely. Dr. Stuart Linder, a noted Beverly Hills plastic surgeon, said in a recent ABC News interview that it is medically possible to implant a large enough charge of explosives into the human body to create an effective bomb. Such a concealment method would be very difficult to detect, according to several security experts, even with the new “full body” scanning devices now being installed at many U.S. airports.

If nothing else, U.S. screeners should at least be made fully aware of the emerging threat involving medically implanted IEDs – as well as all other forms of anatomical-based concealment. Terrorist attack operations have repeatedly demonstrated the alarming ability of terrorists to circumvent new screening technologies. Nonetheless, no terrorist group has successfully eluded Israel’s airport screening in recent years. The behavioral assessment techniques used by the Israelis, in conjunction with advanced technology, provide another important layer in the screening process. Screeners should be provided additional training on behavioral assessment techniques – as well as directions on how to actively engage people in targeted conversations as an added layer of screening.

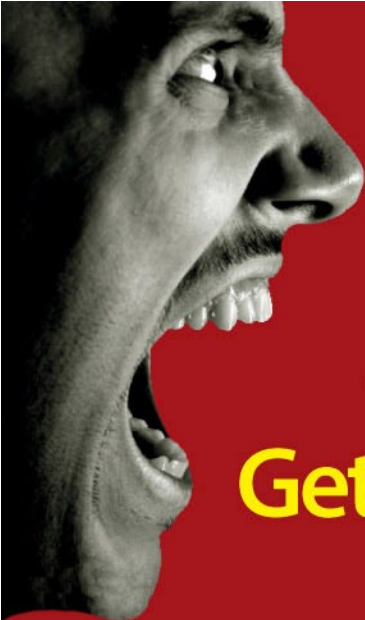
Large, high-risk security screening operations, such as those typically used at most U.S. airports, may decide to station and use medical professionals – emergency medical technicians, for example, and/or paramedics – on-site to carry out closer and more comprehensive medical examinations, and use those examinations in conjunction with improved patient-assessment techniques to detect suspicious people – particularly those who have apparently had recent surgeries.

One cautionary note, though: EMS (emergency medical services) personnel are already a key provider of the emergency services capability at most of the nation’s larger airports, but they are not currently expected to carry out a security screening function in addition to their usual medical-response tasks.

Nonetheless, with terrorist tactics frequently evolving into new and even more dangerous methods for circumventing evolving security procedures, the recognition of newly emerging threats is essential to developing – and constantly upgrading – effective countermeasures. Total reliance on advanced technology is of course an insufficient guarantor of public safety. To detect and thwart the use of medically implanted IEDs, an interdisciplinary approach – involving

sophisticated behavioral assessments, used in conjunction with new advances in screening technology – may be what is needed to effectively counter the still evolving threat posed by the new “human IEDs” of the early 21st century.


Joseph Trindal is the Managing Director at KeyPoint Government Solutions Inc., where he is in charge of the company’s Infrastructure Protection Services. He also serves on the Board of Directors at InfraGard Nation’s Capital Member Alliance. Trindal retired in 2008 from the U.S. Department of Homeland Security, where he had served as Director for the National Capital Region, Federal Protective Service, Immigration & Customs Enforcement.



If This Is Your Crisis Plan For Chemical & Bio Hazards? Get A Better Plan!

The AP4C Handheld Chemical Detector

- ▶ Fast Start-Up
- ▶ No Shelf Cost
- ▶ Easy to Use



Contact Us Now, Before It’s Too Late...

PROENGINEER

Responding to CBRNE Attacks: A Quick Primer

By JL Smither, Viewpoint

With terrorists becoming more sophisticated and the homegrown terrorist threat becoming more real, jurisdictions throughout the United States must prepare for possible attacks using chemical, biological, radiological, nuclear, or explosive (CBRNE) weapons or devices. Many jurisdictions and agencies have already held exercises to test their plans and responses to CBRNE attacks, and a number of them have shared – through *Lessons Learned Information Sharing* (www.llis.gov) – the lessons they have learned, or are learning, with other agencies and organizations throughout the country.

In 2006, the U.S. Department of Homeland Security’s Domestic Nuclear Detection Office sponsored what was called the Southeast Transportation Corridor Pilot Technology Demonstration exercise. The participants included representatives from a number of federal departments and several southeastern states. The objective of the exercise was to test screening technology and procedures by using both fixed and portable radiation detection equipment to screen commercial trucks and cargo containers at port security facilities and vehicle weigh stations.

The participants were expected to proceed, after discovering what seemed to be radiological material, as they would during a real-world incident. However, after detecting a potentially dangerous radiological source in a commercial truck, emergency officials did *not* close the weigh station; nor did they clear the surrounding parking lot. In fact, traffic was allowed to continue through the station while the potentially harmful truck was parked in the nearby parking lot, where many other vehicles also had stopped after being weighed and inspected.

The lack of proper action by emergency officials significantly increased the risk of exposure and contamination throughout a much larger area than just the weigh station itself. The lesson here, of course, was that, after detecting what seems to be a contamination source, law enforcement officials and other emergency responders should immediately secure the surrounding area.

Moreover, after closing down the area, emergency officials should then clearly label and control the contaminated zones. During a functional exercise in Oregon’s Hood River County, agencies practiced and tested their response to the detonation of a radiological IED (improvised explosive device). The simulated blast created a large and potentially contaminated debris field. Not only were some residents “contaminated” by the initial blast, but others also were contaminated when they rushed to help.

During the exercise response activities, the safety officer did not clearly demarcate the boundaries of the control zone. Without realizing it, some responders and victims walked freely, and repeatedly,

from contaminated areas into “cold zones” and back again. These actions put the uncontaminated individuals, equipment, and areas at risk of cross-contamination. Here the lesson is that safety officers should demarcate contaminated areas, clearly, with colored cones, police tape, and/or other visible markers so that responders and victims can avoid cross-contamination.

The NCR Reads, Heeds, and Promulgates

Learning from those exercises, the Metropolitan Washington, D.C., Council of Governments also urges caution when approaching the blast site of any CBRNE device. In a plan designed to ensure that all emergency responders within the National Capitol Region (NCR) follow the same basic operational guidelines, the Council has recommended that the first responders to the site of a potential CBRNE incident stop and evaluate the situation from 300 feet *outside* the debris field. That distance should be enough to minimize the risk of responders being unnecessarily exposed to contamination and/or accidentally detonating a secondary device hidden among the initial blast debris. By evaluating the situation from a safe distance, responders on foot or in vehicles will be unlikely to cross-contaminate cold zones inadvertently.

The Council’s plan also instructs emergency officials to stop rescue vehicles that are outside the blast perimeter. The staging officer on-site should arrange parking for such vehicles in a manner that allows for rapid egress. For that reason, emergency vehicles should be instructed to back into the area without blocking each others’ paths. Adherence to that procedure not only allows victims to be quickly and easily removed from the scene, but also helps vehicles avoid secondary and sudden dangers, such as another explosion or a building collapse.

Today, jurisdictions at all levels of government must prepare to meet the threat posed by a possible CBRNE attack. The first moments immediately following such an attack are critical to the success of the response. Emergency officials will in all probability have to rescue, treat, and decontaminate victims while at the same time containing the contamination and avoiding actions that cause additional harm. As jurisdictions and agencies continue to train on these and other responses, they will develop even more lessons to share.

For additional information on CBRNE responses and other lessons learned, visit *Lessons Learned Information Sharing* at www.llis.gov.

Jennifer L. Smither is the outreach and partnerships manager for Lessons Learned Information Sharing (LLIS.gov), the Department of Homeland Security/Federal Emergency Management Agency’s national online network of lessons learned, best-practices, and innovative ideas for the U.S. homeland-security and emergency-response communities. She received her bachelor’s degree in English from Florida State University.

After detecting a potentially dangerous radiological source in a commercial truck, emergency officials did not close the weigh station; nor did they clear the surrounding parking lot – in fact, traffic was allowed to continue through the station while the truck was parked in the nearby parking lot

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



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

USA Tel: +1 866 803 5956 (Toll Free)

Email: frontline@remploy.com

UK Tel: +44 (0)845 241 2990

Email: frontline@remploy.co.uk

www.rememployfrontline.com

SO DO OUR SUITS

Remploy Frontline

SURVIVAL EVOLUTION

Haiti 2010

When Disaster Is Compounded by Chaos & Confusion

By Theodore (Ted) Tully, Public Health

The “lessons learned” that are discussed in the following article were developed primarily from the relief mission to Haiti that was organized by Mount Sinai Hospital in New York City, which responded with the support and affiliation of the NGO Partners in Health. The goal of the article is to reinforce, for other organizations and individuals, lessons that can be used in future humanitarian responses carried out by private hospitals and/or teams of medical volunteers.



Less than two months ago – more specifically, on 12 January 2010 – the earth shook in Port au Prince, Haiti, and for millions of Haitians the world was forever changed, in less than a minute. The magnitude 7.1 earthquake revealed to the world not only how poor the population of Haiti was, and is, but also how tenuous the Haitian healthcare system was even before the disaster.

Relief organizations all over the world mobilized their staffs, and their members, to send help almost immediately. Numerous government agencies and organizations, as well as non-government organizations (NGOs), put together relief efforts to focus on the immediate needs of water, food, rescue, and eventually emergency health care. The health care response would have to be geared to a region that was considered, even before the quake, to be probably the poorest in the Western Hemisphere. It has been estimated that approximately 110,000 Haitian adults are living with HIV/AIDS. A host of other deadly and/or debilitating diseases – e.g., malaria, dengue fever, parasitic infections, hepatitis, typhoid fever, and rabies – were not uncommon in Haiti even prior to the quake. These facts took a back seat, though, to the immediate need for medical personnel to respond to a mass-casualty disaster of staggering dimensions.

The response by American physicians, nurses, and other medical professionals has been well documented in the U.S. news media. During the first ten days after the quake many American medical personnel and organized relief missions arrived in Port au Prince. What happened before the medical teams, and the supplies and equipment they brought with them, arrived in Haiti is still a relatively unknown story.

The Pre-Planning Stages

Even though most relief organizations started to plan immediately, because of the severe need for doctors and nurses, it was important to focus closely on the specific types of help that would do the most good for the most people. The extreme

need for surgeons, and for a well organized pre- and post-operating system, was acknowledged by several NGOs that were already on the ground in Haiti and providing healthcare even before the earthquake. Responders were able to obtain valuable information from those agencies on the specific personnel needs and the medical equipment also required – for amputations, for example, for open & closed extremity fractures, and for infections.

Aligning the response with such organizations turned out to be an invaluable help. There were, and are, numerous reports of physicians who self-deployed only to quickly become frustrated, and sometimes fearful for their lives as well, because of the support they were *not* receiving during their first 24-48 hours in-country. Many medical personnel and small groups even left Haiti with a high degree of frustration in *not* having been put to use. A key lesson learned by the Mount Sinai group from this difficult situation was the need for the volunteers themselves – individuals as well as small groups – to be as self-reliant as possible for at least the first 48 hours in-country.

The NGOs that responded, and stayed, were recognized as doing an almost unbelievable job in setting up systems for healthcare in a relative vacuum. Taking care of the responders' own needs, though – for food, water, transportation, shelter, and security, to name just a few of the more obvious requirements – was proving to be a massive task secondary only to helping the sick and injured Haitian citizens.

Volunteers from U.S. healthcare institutions were not totally naive in their response to the Haitian disaster, of course, but in retrospect it seems obvious that relying immediately, and directly, on an NGO for the everyday necessities of life was somewhat unrealistic, given the almost total lack of infrastructure in the Haitian capital (and in the areas just outside Port au Prince).

The groups that responded (this experience is based primarily on reports from the medical teams based in and around the National Hospital-HUEH) to several NGOs all seemed to experience more or less the same needs and frustrations during the initial 24-48 hour time frame. There was no reliable source of uncontaminated food and water, and shelter from the elements was minimal at best – one medical group slept in tents close to

the runway of the city's main airport, and others slept on concrete floors in the hospital itself. Perhaps the most problematic issue, though – partly because of the looting and general public disorder that followed the quake – was finding safe transport, through the devastation, to and from the hospital each day.

These and other needs were eventually responded to (successfully, for the most part) by the NGOs, and/or by the various official government organizations and agencies – specifically including units of the nation's armed services – that arrived in-country as more time passed. However, although some rescuers could and did manage to put up with the squalid, and dangerous, conditions they encountered, many others were definitely not prepared. If civil unrest had gotten worse, or if the weather conditions were poor, or if an infectious outbreak of a lethal disease had occurred and rapidly spread, the difficult task of coordination would have been much more dangerous as well for the responders and rescuers themselves.

Mount Sinai Experience Pays Off

The Mount Sinai Team response was about as well formulated as it possibly could be during the three days of pre-planning that preceded the first flight to Haiti, particularly given the meager intelligence that was available (but was frequently either outdated or incomplete or actually erroneous). A 27-member surgical team – made up primarily of surgeons, anaesthesiologists, nurses, nurse practitioners, surgical technicians, and administrative/logistical support personnel – was formed in relatively short order, and a team organization was developed with leadership roles assigned to specific physicians, nurses, administrators, and team coordinators.

The Mount Sinai Hospital Incident Command System (HICS), which had been activated to coordinate the team development, was found to be extremely valuable, particularly in such tasks as: the detailed screening of volunteers; meetings with the hospital's legal department (to get answers on liability); other meetings with representatives from human resources (to determine compensation requirements); the logistical coordination of the supplies needed and/or available; and travel information, including the determination of immunization requirements.

All volunteers were briefed on the information received from the NGOs, and from government organizations and agencies already on the ground in Haiti. However, the volunteers were given less than 24 hours to obtain the passport information they needed, the immunizations required, and the prescriptions that had to be filled prior to travel. One particularly valuable lesson learned came from recruiting team members who spoke Creole or French (Haitian volunteers were seen as a plus for many reasons; this was one of them).

Team members were asked: (a) to bring with them only one bag for their clothing and other personal items; and (b) to plan to stay for two weeks, but possibly longer. It was not known in the initial planning stages when and/or how the volunteers would return to their home communities.

A private charter flight would be the method of transport, but because of the very tight time frame that had been set the aircraft's capacity was not known until 24 hours before the flight. The cargo capacities planned, in both size and weight, were estimates at best, so the supply list was developed with minimal and, as it turned out, inadequate information. More than 4,000 pounds of equipment, not counting personal baggage, was brought to the plane before it was realized that only about 3,000 pounds of supplies, including personal luggage, could be taken on the initial flight. A quick "triage" of the most important supplies and equipment was carried out at the plane itself, and each box was labelled and weighed. Nonetheless, and despite this unexpected difficulty, it was obvious that the pre-planning activities were an invaluable help in quickly loading the plane and meeting the necessarily very tight landing schedule.

During the next eight days the Mount Sinai Relief Response – which included volunteers from other New York City Hospitals (Elmhurst, Queens General, Mount Sinai Queens, Beth Israel, and Maimonides) – developed a functional operating suite where the volunteers carried out and/or assisted in over 120 surgeries, organized equipment/sterilization processes, developed pre- and post-anaesthesia patient care, carried out their daily "rounds" (checking vital signs and changing bandages)

The health care response would have to be geared to a region that was considered, even before the quake, to be the poorest in the Western Hemisphere; approximately 110,000 Haitian adults are living with HIV/AIDS ... [and] a host of other deadly and/or debilitating diseases were not uncommon

on all patients presenting themselves for care, and established a logical and cohesive system for documenting the surgical care that had been provided.

Lessons Learned – And Daily Reinforced

There are hundreds of stories on how the medical mission in Haiti affected the patients and medical staff. Possibly the principal lesson – reinforced, and visible in the faces of many volunteers who were in Haiti during the first 24-48 hours – was, and is, the disorientation that exists in such a country, in such circumstances. *Becoming self-sustainable* for basic needs is very important, therefore, if only because the NGOs that volunteers may be relying on might well be busy with other tasks of higher priority. The nation's Disaster Medical Assistance Teams (DMATs) have learned, over many years of deployments, that the teams should come into a disaster scene ready to take care of themselves for at least the first few days, and possibly longer.

Developing a team approach and organization in advance was invaluable in the effort to quickly develop a medical group and ensure a successful mission. Other lessons learned focused on the importance of team meetings, the reinforcement of safety/situational awareness, and setting up teams in pairs – with easy-to-remember meeting places (where individual volunteers could go if safety issues arise). The safety issues cannot be emphasized enough, especially in countries such as Haiti, where there is little or no information available about areas of civil unrest.

The pre-planning for infection protection of volunteers who wanted to deploy also was important. Immunizations and prophylactic medicines are needed so that the volunteer staff feels both safe and protected. Certain personal medications (for malaria and HIV, for example) may have to be started before departure – and continued after the mission is over – to protect volunteers. This information needs to be strongly reinforced, particularly given the infectious-disease history of the area and especially the potential for lethal outbreaks during and after a major disaster.

Precautions related to blood and other body fluids also became very important to reinforce (Mount Sinai brought its own prophylactic HIV kits for needle stick precautions) during long operations and/or when staff became tired.

There also were a number of *mental health concerns* – caused by, among other things, the difficult emotional experiences, the strange and dangerous environment, the lack of food and/or water, or simply the fact that the volunteer is away from his

or her family, and isolated to some degree. Many such issues, with mental as well as physical causes and symptoms, should be a conscious concern of all volunteers. The use of informal debriefings during and at the end of such experiences can be of help even for those who may have served on similar missions in the past. Support at home is also important so that volunteers know their families are aware that they are safe (a nightly briefing was carried out by Mount Sinai, which sent family emails out every day).

Simple personal supplies are among the small necessities that many volunteer responders may not think of until they are actually on-scene in a disaster area. Items such as Vick's Vapor Rub (to mask the smells, which are not only unpleasant but also sometimes dangerous as well), indelible markers to write on bandages, head lamps (to work hands-free), personal flashlights (with extra batteries), and cell phone chargers (for both wall and car) – because the availability of electricity is unpredictable. Also, the importance of pairs of inexpensive point-to-point portable radios – similar to those used by families in amusement parks to stay connected – becomes evident when cell phones are useless for any number of reasons.

What Leads to the Decision to Volunteer?

Most volunteers from the Mount Sinai Team who have been interviewed, and other volunteers who already have returned from Haiti, have said they wish they could have done more and, somewhat surprisingly, perhaps, wish they could have stayed longer. The feeling that they helped in some small way is something they said would stay with them for a long time to come, and might well motivate them to volunteer again, if and when needed.

The NGOs for medical volunteers – e.g., Partners in Health, International Medical Corps, Doctors Without Borders, and others – do a superb job. If healthcare workers want to deploy and to help in situations such as what happened (and is still happening) in Haiti or other distressed areas of the world, an association with such organizations can help provide them the support and protection they definitely will need. To self-deploy without affiliating with an NGO, though, as was seen, will likely result in personal frustration from not being able to help – and for that reason alone substantiates the need of an individual, as well as an organization, to participate only as a member of a strong and meticulously detailed pre-planned mission.

Theodore (Ted) Tully, Administrative Director for Emergency Preparedness at Mount Sinai Medical Center in New York City, served as Administrative Lead for the Mount Sinai Haiti Relief Mission and helped organize the mission.

NEW

CHEMPRO

Handheld Chemical Detector **100i**

ChemPro100i is a handheld vapor detector for classification of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). The ChemPro100i adds 6 more sensors to increase the number of chemicals that it can detect and to decrease the potential for false alarms.



No maintenance costs for 5 years!

- Industry leading sensitivity
- Stores well - no regular exercise needed
- Non-threatening design
- Easy-to-use

* Contact Us for details on our standard 5-years Guaranteed Cost of Ownership (GCO) program



Environics Oy
Graanintie 5
P.O. Box 349
FI-50101 Mikkeli, Finland
tel. +358 201 430 430
fax. +358 201 430 440
www.environics.fi
sales@environics.fi

Environics USA Inc.
1308 Continental Drive, Suite J
Abingdon, MD 21009
USA
tel. +1 (410) 612-1250
fax. +1 (410) 612-1251
www.EnvironicsUSA.com
sales@EnvironicsUSA.com

Department of Defense Focuses on IT Innovation

By Thomas Payne, Director, ITT's Information Integration Systems



Some of the most important technological developments that have improved society in general have resulted directly from innovations built for military operations. Technologies developed by the Department of Defense (DOD), for example – to integrate, share, and protect information supporting large-scale military campaigns – can be adapted to advance the way that civilian agencies and organizations manage their information. To exploit the most modern technologies, therefore, private businesses and state, local, and non-DOD federal agencies should look more closely at information management tools that the military and DOD have already developed.

Consider this: To identify and understand the interconnected network of people and activities in various terrorist organizations responsible for building and planting improvised explosive devices (IEDs), an analyst would need a truly innovative, collaborative, and analytical technological framework. The information architecture and tools that enable intelligence analysts and operators to rapidly respond to warfighter requests on enemy networks, battle space conditions, ISR (intelligence, surveillance, reconnaissance) optimization, and threat trends are the same tools that can completely transform the way that civilian organizations analyze and respond to similar data. Customization of that technology not only is possible but also might well be critical to advance information management in other sectors, such as those responsible for homeland security and law enforcement.

A New Model – Centers of Analytic Excellence

In this new model, information of value is gained through tailored open architecture and secure information integration and the sharing of enterprise solutions. The goal of data integration is to transform raw data into actionable knowledge.

Like many other organizations, DOD faced several daunting issues at first: outdated storage and retrieval systems, for example, the inability to find information fast enough, inflexible sharing and searching processes, and the inability to layer and integrate information.

The new model creates “centers of analytic excellence,” as described by DHS (Department of Homeland Security) Secretary Janet Napolitano, using open architecture and best-of-breed non-proprietary hardware and software.

Among the many advantages achieved with the DOD’s solution are the following:

- Instant access to analytical-quality data;
- The use of metadata tags to speed search;
- Smart applications with built-in integration mechanisms;
- The establishment of a collaborative environment; and
- The ability to tailor various applications and tools.

Open Architecture and The Dimensional Data Model

How is this type of model created? The first step involves establishing an open-architecture framework with enough flexibility to meet both evolving needs and emerging threats. Open architecture also delivers the best structure for innovations in collaboration, intelligent search, and real-time analytics.

Within the backbone of an open architecture structure, core data environments are created based on the metadata developed. The core search environment features tools that catalogue, process, and tag the metadata. The data is then further tagged both by security “domain” level (Special Access, Top Secret, Secret, Confidential, and Unclassified) and by releasability. The data is processed by a set of entity and relationship extractors including geo-coding, name recognition, phone numbers, bank accounts, and other information facets. These facets are then captured to create a unique “dimensional data model” – one that has far-reaching implications for all organizations.

To think dimensionally about data means to approach a rich data system in such a way as to create useful and effective search and share capabilities. Organizations need this ability to respond immediately to unanticipated events, intelligently share information across divisions, obtain and receive real-time tech support, provide the continuous fusion and aggregation of data, and support federated search capabilities – while also maintaining a cost-effective budget.

Information Sharing and Protection

When sharing takes place within a single security domain, this model uses many of the same tools and methods as those used in a modern business environment. Because security domains are carefully tagged, when the level of information sensitivity increases, so does the level of its protection, resulting in increasingly rigorous controls and more limited access.

HAZMAT IDENTIFICATION. IN THE PALM OF YOUR HAND.



Ground-breaking Raman technology in an affordable, palm-size instrument for rapid identification of unknown materials.

Fido® Verdict™ provides real-time, accurate identification of unknown liquids, powders and solids for HazMat professionals. With Verdict, the capabilities of Raman technology are available in an easy to use, miniaturized system at an affordable cost. Hazardous materials identification is now within reach for the entire first responder community.

Contact ICx Technologies at 1-877-692-2120 for more information on Verdict and the Verdict HazMat-CB Responder Kit which includes enzyme-based chemical agent tests and bio-assay strips for a comprehensive chem bio solution.

www.icxt.com

NEW THREATS.
NEW THINKING.®

icx®
technologies

Sharing becomes more difficult across security domains; a challenge similar to providing safeguards for privacy, U.S. persons data, and law enforcement sensitive data. When moving from the most strictly controlled to the least, information sharing is governed by thousands of laws, policies, regulations, and rules. All of these gate-keeping measures are in place, of course, to protect the integrity of the data and to control user access. DOD has funded dozens of software and hardware solutions, however, to provide for the efficient and safe exchange of information between two or more parties operating at different security levels.

More complex situations require that information be shared among different government agencies and public/private communities as well as across different security domains. Here, data protection is achieved through user education and awareness as well as through technological means. Again, DOD is playing a leading role in this area: critical infrastructure and information protection activities, being addressed in federal policy and law, are intended to enhance the security of the public and private infrastructures that are essential to the nation's physical, cyber, and economic security.

Real Life Applications

As discussed earlier, a critical aspect of this new model is the ability to integrate disparate data and share it not only across multiple departments and organizations but also across different security levels. The following scenarios illustrate how improved capabilities can have a profound impact in real-world situations.

Case 1: A border patrol agent must make a decision on whether or not to detain an individual. In this situation, the agent needs to query information sources with a variety of raw data – e.g., passports, fingerprints, images – and to receive a timely and relevant response in return.

Solution: The agent uses a web-based secure system that allows data sharing across multiple agencies and security levels. The system possesses an “attribute-based access control” capability, which means that the agent can access data cleared to his/her appropriate security level. Information owners can aggregate and share requested data controlled to his or her level, and to the levels of other agents who might be involved. With this greater collaborative engagement capability, the agent can know immediately whether to detain that individual or let him/her go.

Case 2: An agent must respond to a domestic terrorist threat. Post-attack, this agent needs to quickly investigate and protect against further threats by accessing and integrating data in disparate silos and across all security levels in the federal, state, and local domains.

Solution: The agent uses the UDOP (User Defined Operational Picture) tool that is part of his or her database. With UDOP, the agent focuses on the specific information of value on his or her exact level of concern (federal, state, local, and/or tribal) in order to coordinate a response. This same tool – much appreciated by senior level officers – can be used to plan, brief, and monitor mission execution in one system.

Organizations outside of the military could apply the same technology to improve response times and collaboration across horizontal divisions – while also protecting the integrity of the data. Within the healthcare and medical fields, this type of robust searching and sharing could prove a priceless asset in saving lives.

What Are the Next Steps?

Instead of dealing with outdated data structures and spending money on research and development, companies and government agencies should look to the military's new model for insight and advancement. One idea is to start where the Department of Defense did – with ITT, a top-10 U.S. defense contractor and one of the largest information systems providers to the federal government. Using “centers of analytic excellence” is how ITT is helping DOD stay ahead of the curve, and customizing this new technology will prove invaluable to new critical areas.

ITT's goal, using its in-depth engineering and programmatic expertise, is to meet emerging trends and transformational needs of both government and commercial customers in the areas of information integration, protection and sharing, and services. The power in ITT's tools, as demonstrated in the scenarios above, provides organizations the capability to plan, brief, and execute with just one system.

For additional information about the ITT “toolkit,” visit: <http://www.defense.itt.com/>.

Thomas Payne is the director of ITT's Information Integration Systems Department, which delivers information integration solutions based on a proven non-proprietary open architecture that integrates best-of-breed applications. The department is part of ITT Information Systems, which has over 11,600 employees globally; its corporate headquarters is in Herndon, Virginia.

The Need for Situational Awareness in a CBRNE Attack

By Jordan Nelms, Viewpoint



Six years before the terrorist attacks on the World Trade Center and the Pentagon, and eight years before the United States went to war with Saddam Hussein for his alleged concealment of chemical and biological weapons caches, Japan's Tokyo subway was struck by one of the most vicious terror attacks in modern history.

The 1995 Sarin terrorist attack represents an important case study for post-9/11 emergency managers because it highlights the key issues first responders and public health officials face when confronted with a CBRNE (Chemical, Biological, Radiological, Nuclear, Explosive) mass-casualty attack.

The after-action reporting following the Tokyo Sarin attack noted serious deficiencies in the identification of the threat, and the escalating confusion about why so many obviously sick people were coming out of the subway station. First responders arrived on the scene quickly – but, because Sarin is an invisible gas, fire and EMS units were unaware that the scene was *hot* and did not know the nature of the threat they were facing. Although they did an effective job evacuating and getting people out of the subway station, their failure to take precautionary measures specific to a CBRNE attack caused the unnecessary contamination of hundreds of first responders themselves as well as innocent bystanders. Hospitals became a primary decontamination area by default, putting emergency room doctors and other hospital workers and patients also at risk for contamination.

Recognizing these challenges, in 1995 the U.S. Department of Energy embarked on the research and development of an Autonomous Pathogen Detection System (APDS), the purpose of which is to pre-position detection devices in high-threat environments, increasing the situational awareness of first responders and emergency managers dealing with a CBRNE incident.

PROTECTing the Responders – The First Priority

Sandia National Laboratories initiated testing, in 2000, of an APDS specifically designed to meet the need of U.S. subway systems by simultaneously detecting a number of chemicals, viruses, and toxins. Meanwhile, the Program for Response Operations and Technology Enhancements for Chemical/Biological Terrorism (PROTECT) was being piloted by the Washington Metropolitan Area Transit Authority (WMATA). In 2003, after three years of testing, PROTECT became a permanent program at WMATA, and now operates in over a dozen high-volume stations along the Authority's Metro system.

An important responsibility of an emergency manager is to protect the safety and health of first responders. Increasing the emergency managers' ability to make informed decisions in the face of a CBRNE attack not only has a critical impact on the first responders' ability to save the lives of attack victims, but also

protects them from personally becoming victims. The success of the PROTECT program has the potential to become a mainstay in the homeland security programs of other major metropolitan cities. The APDS technology is now well established, and in wide use by the Department of Defense. The PROTECT program, on the other hand, because of its relative infancy and much higher cost, faces considerable barriers before national implementation would be possible.

The fact is that, as in many other homeland security initiatives, federal funding does not match the realistic cost of capability implementation. Nor can these high technology programs be paid for from the subway operators' general funds. A key theme of the DHS (Department of Homeland Security) UASI (Urban Area Security Initiative) and Transit Security Grant programs focuses on the protection of critical infrastructure, including the nation's subway systems. Ninety-six percent of the Transportation Security Administration's Tier I funds awarded to the National Capital Region, and seventy-one percent of the funds awarded to the New York Region, were allocated to infrastructure protection projects. Those projects served as pilot programs for the rollout of many critical technology solutions – and the subway systems of both cities, according to DHS, are at the highest risk of a CBRNE attack. Associations and subway operators are continuing to lobby DHS for additional funding in this area, hoping to expand the PROTECT system beyond Washington, New York, and Boston. It is clear that operators see the benefit in such a system, and understand that the only way to procure the technology is through federal grants.

Subway operators are hopeful that, after the PROTECT program becomes standardized in its technology and implementation requirements, it will be expanded to other major metropolitan cities. At present, however – almost 15 years after the Tokyo Sarin attack, and 11 years since the inception of PROTECT – operators are increasingly anxious to know DHS's intentions for a national rollout. At present they can only hope, though, that after that happens there will be not only clear guidance provided but also the development of the technology standards required and an infusion of follow-on grant funds.

In the competitive grant environment that DHS facilitates, emergency managers, first responders, and subway patrons alike are hopeful that the department's risk-based awards are increased, and the PROTECT system be allowed to proliferate in major cities around the nation.

Jordan Nelms is the Homeland Security specialist at James Lee Witt Associates, where he has been responsible for homeland security consulting to state, county, municipal, and multi-jurisdictional clients around the country. Prior to joining Witt Associates, he worked in the Emergency Operations Center and Emergency Public Information Office of Pinellas County, Florida.

Partners in Preparedness

Close to 2000 Attendees at Public Health Preparedness Summit

By Jack Herrmann, Public Health



Almost 2,000 public health preparedness and emergency management professionals, including the nation's leading public health officials, convened in Atlanta last month for the fifth annual Public Health Preparedness Summit. The huge number of attendees was a testament to the desire and need of those participating to truly be partners in preparedness. The Summit attendees represented all facets of the nation's healthcare communities, including: local, state, and tribal public health leaders; senior leaders from federal government agencies and organizations; and a broad spectrum of working professionals from private industry, academia, and community organizations. These practitioners, who represent the spectrum of emergency preparedness and response, met to work toward the common vision of safer, healthier, and more resilient communities.

The 2010 Summit offered an impressive lineup of the nation's public health leaders and decision makers – beginning with Health and Human Services (HHS) Secretary Kathleen Sebelius. Following an introduction by Dr. Thomas Frieden, director of the Atlanta-based Centers for Disease Control and Prevention (CDC), Secretary Sebelius spoke of the valuable lessons learned by the public health community in dealing with the H1N1 influenza pandemic, which put additional pressure on a strained system that had already been reeling in the wake of budget cuts and employee layoffs. Nonetheless, Sebelius said, H1N1 “confirmed that continuing to reduce our state and local public health infrastructure is a formula for disaster.”

Despite the problems it caused, she continued, the H1N1 pandemic “brought about many innovations in our nation's response, including partnerships with the education, business, and medical industries – and with state, local, tribal, and territorial public health officials.

“... What we also saw with H1N1,” Sebelius continued, “was that these partnerships pay off. When we spoke with one voice, our message was clearer. When we responded together, our efforts were more effective.”

Lurie, Jones, and an All-Star Panel of Distinguished Speakers

Following Sebelius's opening remarks, Dr. Nicole Lurie, HHS Assistant Secretary for Preparedness and Response, moderated a line-up of distinguished panelists including Carter Mecher, director of Medical Preparedness Policy for the White House; Stephen C. Redd, director of the Influenza Coordination Unit with the

CDC; Paul Jarris, executive director of the Association of State and Territorial Health Officials; and Bruce Dart, president of the National Association of County and City Health Officials.

Reflecting on their respective organizations' responses to H1N1, the panelists shared their perspectives on the value of using humility, communications, and collaboration as tools to craft a successful response. “No one agency can work alone,” said Dart. The sharing of resources, data, and communications, he said, helped health departments at all levels of government, and in the private sector, work more closely with one another, and with federal agencies, to adjust quickly to unexpected changes and challenges during the course of the H1N1 pandemic.

The concepts of partnership and collaboration continued throughout the remainder of the 16-19 February Summit. Several sessions focused on the need to establish robust relationships among and between the numerous partners and stakeholders usually involved – at different levels, and in different ways. In addition, many speakers emphasized the importance of strengthening the collaborations that were established both before and during the H1N1 response. According to keynote speaker Ana-Marie Jones – the executive director of Collaborating Agencies Responding to Disasters – the most critical steps for a *successful* collaboration are co-existence, commitment beyond the grant, and communications, cooperation, and coordination. Among the many issues to be considered along the path to a successful collaboration, she continued, are change, costs, capacity, credibility, culture clash, comfort zones, and competition. Jones advised the Summit attendees to: (a) honor natural existing and chosen associations; (b) protect partners from bureaucracy; (c) take advantage of technology; and (d) embrace the “social media” to help the partnership efforts succeed.

In addition to the panel discussions and numerous high-level speakers participating, the 2010 Summit offered an extraordinary agenda filled with hundreds of interactive sessions, skills-building workshops, sharing sessions, poster presentations, and networking opportunities. Today, although the Summit may be over, the content remains available for review. Those who could not attend, or could not attend *all* of the sessions, should visit www.phprep.org to download session materials.

Jack Herrmann is the senior advisor for public health preparedness of the National Association of County and City Health Officials. In this role, he oversees the organization's preparedness portfolio, which is aimed at enhancing and strengthening the preparedness and response capacity of local health departments. He also is responsible for establishing the priorities for public health preparedness within the organization, and serves as NACCHO's liaison to local, state, and federal partner agencies.

WE REDUCED THE SIZE. NOT THE PROTECTION.

NIOSH
National Institute for
Occupational Safety and Health
CBRN



NHI5
ESCAPE HOOD



AVON
PROTECTION

1 888 AVON 440
www.avon-protection.com

The Security Checkpoints of Tomorrow

By Peter Kant, Vice President, Rapiscan Systems Government Affairs



With every security breach comes new challenges. The security checkpoints of the future will not only anticipate and contend with emerging threats, but also combine the best screening technologies with advanced integrated solutions to reshape the nation's first line of defense.

On 25 December 2009, on approach to Detroit, Michigan, Umar Farouk Abdulmutallab attempted to detonate plastic explosives that were sewn into his underwear on Northwest Flight 253. By reacting quickly, other passengers were able to subdue the suspect and put out the flames. In the years since the aircraft suicide attacks of 11 September 2001 (9/11), many citizens, like those on Flight 253, have joined forces with the U.S. government and the nation's security agencies to keep the U.S. homeland safe. Unfortunately, the more aware people become of the dangers surrounding them, the more creative the terrorist attempts also become – and, therefore, the more sophisticated the checkpoint security protection equipment must become as well.

When Britain's internal secret service (MI5) and police forces foiled the unprecedented liquid bomb plot in August 2006, liquid threat prevention was added to the growing list of security concerns. More recently, the MI5 discovered evidence that al Qaeda may be planning to surgically implant explosives in the bodies of suicide bombers, proving again what security professionals already knew – namely, that each new terrorist tactic adds to the complexity of necessary threat detection systems. Using equipment ranging from small hand-held metal and chemical detectors to complex full-body scanners that use backscatter technology, security personnel are able to search not only baggage, cargo, and vehicles, but people as well, at critical security checkpoints.

Among the more common sites where screening is carried out on these items – and on people – are border checkpoints, airports, shipping ports, courthouses, nuclear power plants, military bases, and various “large-venue” events. However, the need for additional security is also growing in other sites such as schools and corporate buildings. Because searches are needed for a wide variety of dangers – e.g., liquid and solid bombs and other weapons, biohazardous materials, narcotics and other illegal substances – in a wide range of locations, no single screening device is sufficient to detect all possible

dangers. For example, high-energy transmission x-rays used by ports, borders, military facilities, and other installations can penetrate up to 43 cm of steel, while backscatter x-rays used on humans penetrate to only about 10 mm. Both types of devices provide exceptional detection for their respective uses, but they are not interchangeable.

New Technology for Advanced Threat Detection

The installation of inspection and screening systems at critical security checkpoints provides an important first line of defense in protecting the country as a whole. By detecting threats early – particularly within such critical infrastructure sectors as transportation, power, federal and municipal services, and law enforcement agencies – officials are able to avoid or dissipate a more catastrophic event such as the 9/11 terrorist attacks. Threat awareness, coupled with threat detection, also will usually prevent people like Richard Reid, the 2001 shoe bomber on American Airlines Flight 63, from even boarding a plane.

Obviously, government and police investigators must be equipped with the best detection equipment available in order to combat whatever threats now exist or are likely to be developed and deployed in the foreseeable future. Newer x-ray devices measure the way the rays bounce and bend, which provides better material discrimination. The combination of multiple x-ray angles and improved threat-detection algorithms results in higher quality images, lower false alarm rates, and better capability for separating organic substances – such as explosives and narcotics – from inorganic substances such as metal. Using the resulting high-resolution image, a large cargo container can be searched for hidden contraband in less than 30 seconds, significantly reducing the need for time-consuming manual inspections. As a result, port authorities can provide additional security for the critical infrastructure by scanning more containers in less time.

Software plays an important role in supporting these inspection and screening systems. Although the systems used are becoming more complex, the training needed to use the scanners effectively does not change significantly because software upgrades now supersede equipment replacement. However, as systems become even more complex, the inspection sites and inspection training involved will undoubtedly create additional concerns.



+ Disaster Response **and** Recovery EXPO

May 11-13, 2010 • Gaylord Opryland Resort & Convention Center • Nashville, TN



Discover the Latest Disaster Response & Recovery Equipment, Technology and Services!

The Disaster Response & Recovery Exposition, co-located with the 2010 Integrated Medical, Public Health, Preparedness and Response Training Summit, is the perfect opportunity for Local, State and Federal public health and emergency preparedness practitioners and policy makers to discover the latest equipment, technologies and services available.



Co-sponsored by the U.S. Department of Health and Human Services (HHS) and the Chesapeake Health Education Program, the Training Summit brings together HHS partners including the National Disaster Medical System (NDMS), the Office of the Civilian Volunteer Medical Reserve Corps (OCVMRC), the Emergency System for Advance Registration of Volunteer Health Professionals (ESAR-VHP), and the Office of Force Readiness and Deployment (OFRD).

For more information or to become an exhibitor, contact:
DRRE Exposition Management
c/o J. Spargo & Associates, Inc.
800-564-4220 / 703-631-6200
drre@jspargo.com



DRRE is sponsored by the Chesapeake Health Education Program, Inc.

Register Today—www.drrexpo.com



Networking the inspection sites to communicate remotely to a central image viewing area will alleviate several of these concerns – for three reasons: First, having a single viewing area for multiple locations reduces the cost of installation and management at each location. Second, the use of fewer viewing areas permits the expanded use of the most highly trained inspectors. Third, remote viewing protects citizens’ privacy rights – answering a concern voiced by many citizens because the body screening images become more detailed.

Here it is worth pointing out that, when given the choice of a full-body scan or a hand search in an airport test study performed in Europe by the British Airports Authority and the Manchester Airport Group, over 93 percent of the passengers in the study chose the advanced technology body scan over the traditional search. The backscatter technology used in the new scanners produce exceptional quality images – front and back – in less than seven seconds, so less time is involved, there is no intrusive search, and the passengers’ privacy is protected even more because the viewing is carried out at a remote location. The software and networking abilities of new x-ray devices make all of this possible.

An Increased Focus on Operational Efficiency and Customer Satisfaction

One of the most important aspects of the security checkpoint of tomorrow is that it will enhance operational efficiency – e.g., checkpoint throughput and staffing requirements – even as it improves checkpoint security. And, rather than creating stress and confusion for persons going through the checkpoint, it will make people feel calmer and more secure. Leading checkpoint security designs use advanced gating and signage systems that guide persons through the checkpoint. Moreover, the new systems feature ergonomically designed divestiture and “recompose” areas as well as material handling systems that facilitate the handling and inspection of carry-on baggage. In one live airport trial, the use of these types of systems, together with advanced security screening technologies, dramatically increased customer satisfaction while at the same time reducing checkpoint manpower costs.

Integrating a variety of people, baggage, and cargo systems with software solutions provides a more comprehensive as

well as more reliable security solution. At a typical airport, for example, baggage and cargo are scanned before being loaded onto an airplane, carry-on luggage is x-rayed on a conveyor belt, people are screened with metal detectors and full-body scanning devices, and the software behind all of this transmits reports and images to a central processing location. This optimized checkpoint approach can be further enhanced through the use of third-party bin diversion. In this scenario, when a threat is detected, the bag is removed automatically and authorities are alerted, thus preventing harm to airport personnel, and any others in the vicinity, and reducing stress for the person at the checkpoint. In the near future, scanners

will use automatic threat recognition rather than images to pinpoint potential hazards. These new systems will assist operators by automatically indicating the presence of hazardous materials and contraband, including liquid explosives and/or other threats. By adding newly developed automatic bag and bin handling systems, many travelers will see a fully automated checkpoint in the near future.

Rapiscan Systems, a wholly owned subsidiary of OSI Systems, is a leader when it comes to implementing fully integrated all-inclusive security solutions. Their trusted products are now being used at airports, nuclear power plants, courthouses, ports, borders, government buildings, large venue events, and companies in over 100 countries. With both U.S. Transportation Security Administration and U.K. Department for Transport approval, Rapiscan provides superior baggage and

people screening at airports around the world through its 620XR, 620DV, 627XR, 627DV, 628XR, 632DV, 638DV, MVXR 5000, and Secure 1000 Single Pose systems. By integrating a sophisticated software platform with an energy efficient security system offering optimized throughput and the smallest footprint of all screening technology, Rapiscan Systems offers “the security checkpoint of tomorrow,” TODAY.

Here it is worth pointing out that, when given the choice of a full-body scan or a hand search in an airport test study performed in Europe by the British Airports Authority and the Manchester Airport Group, over 93 percent of the passengers in the study chose the advanced technology body scan over the traditional search

Peter Kant is Vice President of Government Affairs at Rapiscan Systems, where he manages the company’s worldwide government relations effort – which encompasses over 150 countries. He works directly with senior government officials in nations all over the world, as well as with elected leaders and their staffs, and the global security community at large to help formulate and identify policies that address security vulnerabilities while at the same time protecting privacy and the flow of commerce.

Keeping It Simple – And the Need for Pre-Planning

By William (Jeremy) Magers, Fire/HazMat



Mass-casualty weapons of mass destruction (WMDs), as well as chemical and biological warfare, are terms that create fear in the average person's mind. The relatively new "combo" word ChemBio, in fact, has become a term that in the emergency-services field makes some responders automatically think requires "Rocket Science" capabilities – and for that reason is discouraging in and of itself.

One fallout problem related to that somewhat misleading impression is that there already are many groups throughout the United States teaching emergency-services personnel, the complicated way, how to respond to a ChemBio event. Unfortunately, this is yet another reason why so many responders see the response to ChemBio as a much more complex task than it really is. The truth is, though, that training and practice on the basics of how to read meters – augmented by instruction on the signs, symptoms, and decontamination processes required, along with knowing what federal and/or local agencies to call if a positive meter reading is displayed – are the major steps to follow in developing a proficient response team. In short, it is time to slow down, get back to the basics, and steer team members in the right direction.

Ion mobility spectrometry, gamma ray spectroscopy, and raman spectroscopy are just a few of the advanced technologies used in today's meters. Understanding what those technologies are, and the sometimes intricate but usually rather simple details of how they work, is important both to the people maintaining the meters and to those interested in knowing much more about them. However, that same level of understanding is not required for the average responder using a meter at the scene of an incident. For the responder, in fact, the most important rules to remember are to: (1) "keep it simple"; and (2) know the basics of how to use the meter.

A Failing Grade – To the Instructors, Not the Students

Unfortunately, there are many responders who will *not* use the meters now available because the classes they have attended focus so much attention on a complicated vocabulary and schematic diagrams that at least some students are discouraged from continuing the learning process. The more important focus, though, should be on the relatively simple basics of meters, which – if the instruction is done properly – will show students (the nation's future responders) that most meters are in fact very user-friendly.

The average meter is provided, in fact, with visible step-by-step directions that walk the responder through the correct steps – shown on a display screen – to take in responding to a potential ChemBio incident. Without training responders the correct way to use this important tool of the trade, though, the meter cannot be operated effectively. However, by focusing on the fundamental basics of meter readings, responders will quickly, and without too much difficulty, not only become comfortable with using the meters but also, as a secondary bonus, soon realize that that task is not as difficult as it sometimes seems to be.

Arriving at the scene of an incident and finding multiple casualties – many of them suffering from watery eyes, excessive sweating, vomiting, and rapid breathing – is a typical scenario that most first responders can face without flinching. Nonetheless, such a situation is chaotic enough at that point that the responder should not have to waste additional time determining what meter to use, what protective clothing to wear, what decontamination system to use, what evacuation plan to follow, and what specific toxic agent has been dispersed. Pre-planning all of these tasks, and others, *prior* to such an incident or event will allow the responder team to be much better prepared. Proper and relatively simple training – combined with the preparation and use of pre-planned check lists – will allow the team to arrive on-scene with a workable plan of action.

A Quick & Easy Inventory of Pre-Planning Essentials

ChemBio "Pre-Plans" put responders ahead of the game prior to arriving at the scene of an incident. Research is the key element leading to a successful response. Although the initial setup can and will take time and personnel to accomplish, the benefits far outweigh the efforts needed. The key, again, is to keep it simple. The average responder can set up an Incident Management System free of un-needed complications. To achieve that goal, though, the pre-plan sheets should include at least the following:

- The types of meters that should be used: Photo Ionization Devices (PIDs), Advanced Portable Detectors (APDs), Carbon Monoxide, Oxygen, Acid and Base Paper, Drager Tubes and Chips.
- Specific decontamination systems and solutions: Two-Stage, Three-Stage.
- The personal protective equipment (PPE) needed: Level A, Level B, or Level C.

- Agent characteristics, signs, and symptoms: Vapor Pressure (VP), Vapor Density (VD), Short-Term Exposure Limits (STELs), and Time Weighted Averages (TWAs).
- Support agency contact information: Federal Bureau of Investigation (FBI), Weapons of Mass Destruction Civil Support Teams (WMD CSTs), and Federal Fire Service Hazardous Material Teams.
- Any other information – e.g., Population, Geographic, Facilities, etc. – relevant to the response area and/or to the responders themselves.

Those responsible for developing and promulgating the pre-plans should organize these sheets to fit the team's needs by using research boards in units, pre-plan files, or whatever else works. Here it is worth pointing out that there are many response teams that have already developed pre-plans (on the top ten ChemBio Agents, for example), so establishing the networks needed to exchange such information is one of the most effective ways to help ensure a successful response. By pre-planning all of the information needed – or at least as much of it that can be reasonably available within a

given time frame – a response team can effectively train all of its members by using the information previously compiled by others and arrive on location with an effective plan of action.

To repeat: It is time to get back to the basics and to develop the guidelines for ChemBio response operations in a more common-sense way. By pre-planning the response prior to the incident, a team can be much more confident, and rightly so, in its response efforts. With appropriate and effective training, combined with having all relevant and necessary information available *prior* to a mass-casualty event or incident, the team will not only be less apprehensive about the potential dangers and difficulties involved in a ChemBio incident but also less likely to become overwhelmed and/or discouraged by their own response efforts. In short, let the technology of today make the job of responding to ChemBio events easier, simply by understanding the specific technologies involved and using the operating tools provided both wisely and correctly.

William "Jeremy" Magers is a Captain on Truck 45 at the Fort Meade (Md.) Fire and Emergency Services Center. He affiliated with the fire service following graduation from college in 1999 with a degree in Science. He also works as a consultant, and specializes in preparedness for both manmade and natural disasters.

Cyber Defence
National Security in a Borderless World
 17th & 18th May 2010, Swissôtel Tallinn, Estonia

In partnership with:

 ESTONIAN MINISTRY OF DEFENCE

PLUS A POST-CONFERENCE INTERACTIVE WORKSHOP:
The Cyber Warfare Battlefield
 Led by
 19th May 2010, Tallinn, Estonia

This year's exceptional speaker line-up includes:

- **Minister Jaak Aaviksoo**, Defence Minister, **Ministry of Defence, Estonia**
- **Wing Commander Tom Parkhouse**, Cyber Security Staff Officer, **Ministry of Defence, UK**
- **Rain Ottis**, Scientist, **Cooperative Cyber Defence (CCD) Centre of Excellence (COE), Estonia**
- **Robert Siciliano**, CEO, **IDTheftSecurity.com**
- **Jeffrey Troy**, Chief, **Cyber Criminal Section, FBI**
- **Timothy L Thomas**, Analyst, **Foreign Military Studies Office, USA**

Sponsored by

Supported by

www.cyber-defence.com
 +44 (0) 20 7827 6162 tarri@smi-online.co.uk **SMi**
 LINKING BUSINESS with INFORMATION



Bruker Detection Corporation



**Early Detection
is the First Step
in Protection**



E²M GC/MS System

- Identifies and quantifies organic substance in soil, air, water and from surfaces
- Mobile, compact, fast and reliable
- Software includes all standard MS acquisition methods
- Use internally purified air as carrier gas – no helium, hydrogen, or nitrogen required



HAWK FR Stand Off Detection

- Detects chemical vapors up to one mile line of sight
- Detects CWAs and many industrial chemicals
- Scan large areas in seconds
- Stand-alone or can be integrated into a network



M-IR Mobile FT-IR

- Wear-free ROCKSOLID™ interferometer for industry leading performance and reliability in harsh environments
- Rugged, portable, self contained solids and liquids analyzer
- Bearing mechanism is space qualified and virtually free from wear
- Easy-to-use graphical user interface; assistant guided operation

(978) 663-3660 x1308 ■ nbc-sales@bdal.com ■ www.bruker.com/detection

think forward

CBRN Detection

Critical Infrastructure Protection: Another Role for NIMS+ICS

By Steven Grainer, CIP-R



Homeland Security Presidential Directive Seven (HSPD-7, issued in December 2003), established the national requirement to protect critical infrastructure. By definition, Critical Infrastructure consists of “People, assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacity or destruction will have a debilitating impact on security, the nation’s economy, public health or safety, or a combination of those matters.”

Also by definition, Critical Infrastructure *Protection*, or CIP, consists of “the proactive activities [needed] to protect the indispensable people, physical assets, and communications/cyber systems from any degradation or destruction caused by all hazards.” In February 2003 – prior to the issuance of HSPD-7, it should be noted – HSPD-5 was published. Its purpose: “To enhance the ability of the United States to manage domestic incidents by establishing a single comprehensive national incident management system [NIMS].”

Although there is a direct relationship between NIMS, established by HSPD-5, and CIP, established by HSPD-7, the potential synergistic benefits of combining NIMS and CIP are sometimes overlooked. In some instances, integration of the NIMS principles – particularly as they relate to the basic elements of the Incident Command System (ICS) – with CIP is not fully recognized. Indeed, the principal NIMS components do contribute to the effectiveness of critical infrastructure protection, but the ways in which the NIMS/CIP relationship can be fostered are sometimes not recognized and/or fully understood.

For example, the Incident Command System has historically been considered to be an operational tool for use during emergency situations. As such, it sometimes is overlooked that many of the processes and systems employed in an ICS capacity are equally applicable even when there is no immediate emergency. However, those processes and systems are, in fact, fundamental steps useful for management in any context. For the reader who recalls lessons in ICS-300 in which the so-called “Planning P” is emphasized, the student is provided a planning model that captures all of the steps in an orderly planning process. That same model can readily be adapted for use in a CIP setting.

A Context of Fundamental Importance

A primary purpose of ICS, as outlined in the “Command and Management” component of NIMS, is to ensure the effective and efficient use of resources – which, it is not always recognized, is not solely a function of designating certain resources for specific purposes and establishing a clear chain of command. It *is* that, of course. But it also is a system encompassing processes designed both to: (a) identify resource shortcomings; and (b) provide a means to amend and/or alter incident objectives when the specific resources needed are not readily available.

In that context, a fundamental ICS process can be applied to CIP operations. The basic steps in what is called the P-O-S-T process can be incorporated, for example, in the CIP Process Methodology and used to assist in determining the direction of certain clearly defined CIP initiatives. For those not familiar with the P-O-S-T process – which identifies the essential requirements needed to establish an organization and framework for the incident-command structure – it includes four operating principles: P – identifying *Priorities*; O – determining *Objectives*; S – developing *Strategies*; and T – implementing *Tactics* (or *Tasks*) relative to the situation being confronted.

Because they are similar in many ways to an emergency-incident management challenge, Critical Infrastructure Protective measures are basically a management challenge as well. The management of either or both challenges is more readily achieved through use of an orderly and systematic process. Fortunately, the P-O-S-T process can be used in much the same manner to meet both types of challenges.

Life Safety – The Priority of “Paramount Importance”

In ICS, as in many other operational areas in the field of homeland security, there are several important (but sometimes competing) priorities that must be taken into consideration: Life Safety; Incident Stabilization; and Property Preservation (or protection). These three priorities are generally stated in that order – i.e., Life Safety is of paramount importance. (Not incidentally, the acronym L-I-P is often used to remind ICS personnel of the order of priorities – Life Safety, Incident Stabilization, Property Preservation.)

International Hazardous Materials Response Teams Conference

2010

Beyond the
classroom,
attend hands-on
training, unique
field trips, and
RIT exercises.

SESSIONS INCLUDE:

- First Responders and Terrorist Attacks
- Hands-On in the Hot Zone
- DuPont Experimental Station Field Trip

May 19 – 23, 2010
Exhibits: May 21 – 22, 2010

NEW LOCATION!

Baltimore Marriott Waterfront
Baltimore, MD

REGISTER NOW AT www.iafc.org/hazmat



Although these three core priorities form the basis for almost all decision making, they often can be expanded (or sub-categorized, so to speak) to establish priorities within priorities. For example, recognizing that funds, personnel, and other resources are limited, decision-makers may have to determine, within the *major* priority of Property Preservation, whether it is more important to implement preservation and/or protective initiatives for either: (1) a major highway that has been determined to be vulnerable during a natural-hazard scenario; or (2) a public-safety facility – e.g., a fire station – vulnerable to the same hazard. After considering the potential impact of the loss of either the highway or the fire station, the decision-makers (managers, or “commanders”) would then have to resolve the question as to which one is *more* important to the community, and which one might safely be postponed or by-passed.

It is in that context that the priority within a priority decisions are determined. Both possibilities involve property protection, but one possibility might be judged to be *more* critical, given the specific constraints involved. Perhaps the rationale used would be that damage to the highway would have greater long-term disruptive effects, whereas fire apparatus and personnel may be only temporarily displaced – and with adequate advance notice could be relocated and therefore not totally and permanently “lost.”

After the priorities are placed in order, the next step in this orderly process is to determine objectives. Using the above example, if the priority selected is to protect the highway from flooding, the objective might be to implement flood-control measures – which, not incidentally, might also protect the fire station as a secondary beneficial outcome.

After the specific objective has been determined, a strategy (or sometimes multiple strategies) for achieving the objective must be formulated. Several different strategies, of course, may be reviewed and evaluated. In some instances the most attractive strategies in terms of outcome may be constrained by the lack of available resources – i.e., the funds required to use the tactics needed and/or accomplish the tasks that have been agreed upon. In an ICS setting, the decisions made are generally determined during a “Tactics Meeting” in which the key players discuss both the available resources, and the *needed* resources, to determine if a particular course of action can be effectively undertaken.

A Focus on Simplicity and Objectivity

In the tactics meeting a basic ICS form (ICS 215) is customarily used to clearly, and in one and the same document, capture all of the relevant information needed – including but not necessarily limited to the anticipated tactical action (or task), the resources on hand, and the resources needed. Using simple addition and/or subtraction, the command staff can and should be able to determine whether the tactic/task specified should be undertaken. Based on the discussion that follows, an objective decision can then be made as to whether the effort can be supported with a reasonable expectation of success.

In the P-O-S-T process – as also shown in the previously mentioned “Planning P” – there must be an ongoing assessment which ensures that specific tactics/tasks either can be accomplished with the resources already available or that the resources needed can and probably would be acquired. In ICS, as used for emergencies, there is typically a continuous dialogue between the Incident Commander (who establishes overall objectives), the Operations Section Chief (who generally selects specific ad hoc objectives), and other members of the General and Command Staff – i.e., those responsible for Planning, Logistics, Finance/Administration, Safety, Liaison, and Public Information from start to finish. All of those involved in the dialogue, of course, should possess the situational awareness needed to carry out the P-O-S-T process. The same fundamental process will work in Critical Infrastructure Protection.

The preceding represents neither the first nor the last example of the many ways in which fundamental management challenges and decision-making can be improved using the basic principles incorporated in the concepts and applications spelled out in ICS guidelines. In short, the sometimes daunting task of implementing Critical Infrastructure Protection may be simplified considerably by using the P-O-S-T process to assist both in determining direction and in making important decisions.

*For additional information on the definitions set forth at the beginning of the preceding article see *The Critical Infrastructure Protection Process Job Aid (FA-313, 2nd Edition, August 2007)*.*

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

Massachusetts, Arizona, North Dakota, and Nevada

By Adam McLaughlin, State Homeland News



Massachusetts Logan Airport Is First With Full-Body Scanners

Last week, U.S. Department of Homeland Security (DHS) officials announced that the first of 150 full-body scanners planned for use at U.S. airports will be installed in Boston's Logan International Airport. The DHS plan is to install the first three of the new scanners at Logan International, and another machine two weeks later at Chicago's O'Hare International.

The remaining machines, funded at a cost of \$25 million from the 2009 stimulus plan, are expected to be installed in other airports throughout the country by the end of June, according to DHS spokesperson Amy Kudwa.

Use of the scanners in the nation's airports is a key component of the Obama administration's plans to improve airport security. Full-body scanners, which have the ability to show objects hidden on, or even within, the human body, have been available for years, but their deployment has been slowed by objections from privacy advocates.

After a Nigerian man – the so-called “underwear bomber” – allegedly attempted to blow up a Detroit-bound airliner on Christmas Day 2009, Obama called for purchasing hundreds more of the machines in addition to the 150 announced last year. Several other countries – including Nigeria and the Netherlands, where the final leg of the man's flight originated – have also signed on to use the technology.

The passenger allegedly hid the explosives in his underwear, and the materials went undetected as he went through screening in Nigeria and Amsterdam. Several experts have said that the full-body screeners would not have picked up the suspect's hidden explosives.

The machines show the body's contours on a computer located in a private room removed from the security checkpoints. The face of the person being scanned is never shown and the person's identity is supposedly not known to the screener reviewing the computer images. Nonetheless, the American Civil Liberties Union and other organizations have denounced use of the full-body machines as a “virtual strip search.”

The new scanners have not been available since the Obama administration announced last February that it would provide \$1 billion for airport screening as part of the stimulus plan.

In May, the administration spelled out how that money – including \$25 million for the new scanners – would be spent. Between May and September, DHS asked contractors to provide proposals for building the scanners. A number of competing models were tested over the summer, and DHS awarded the contract to California-based Rapiscan at the end of September.

Arizona U.S./Mexican Border Serves As Testing Site for Failing High-Tech Fence

An ambitious multibillion-dollar project to “hot-wire” the new Southwest border fence between the United States and

Mexico with high-tech radar, cameras, and satellite-signal equipment has been plagued with serious system failures and repeated delays and probably will not be completed for another seven years – if it is finished at all.

The system, originally intended to be completed in 2011, languishes in the testing phase in two remote locations in Arizona along a 50-mile stretch of the U.S./Mexican border. There, the supposedly state-of-the-art system combining sensor towers, communication relay systems, and unattended ground sensors has been bogged down with radar clutter, blurred imagery on computer screens, and satellite time lapses

Full-body scanners, which have the ability to show objects hidden on, or even within, the human body, have been available for years, but their deployment has been slowed by objections from privacy advocates

that, government officials candidly admit, often permit drug smugglers and undocumented workers to slip past U.S. law-enforcement agents.

“It was a great idea, but it did not work,” said Mark Borkowski, executive director of the electronic fence program at the U.S. Department of Homeland Security. “One of the issues was that these radars had too many problems with clutter,” Borkowski said. “Wind moving a tree shows up on the radar. And if you have too much of that, how do you find the person in the clutter? The same problem exists with the cameras. The image is blurry.”

The problems have prompted Homeland Security Secretary Janet Napolitano to order a department-wide assessment of the high-tech project, which once was billed as the capstone to the controversial 2,000-mile combined physical and electronic border fence.

Borkowski acknowledged in an interview that the government and its main contractor, the Boeing Company, had encountered a number of unforeseen problems since announcing the plan, in 2005, to build sensor towers and radar scans alongside the new border fence.

Although the administration, and Boeing, remain hopeful that the problems can be fixed, he cautioned that the technology ultimately might not cover the entire border. “It turned out to be a harder technological problem than we ever anticipated,” Borkowski said. “We thought it would be very easy, and it was not.”

Timothy Peters, vice president of Boeing Global Security Systems, which is handling the project, said that the company remains dedicated to correcting the problems. He acknowledged, though, that “our customer’s and our expectations” for the Arizona testing sites “were not initially met.”

North Dakota **Hospitals & Care Centers** **Focus on Flooding Concerns**

Hospitals and nursing homes in the Fargo-Moorhead area are well along in drafting contingency plans in the event that major flooding strikes again this spring – as seems possible this weekend, according to recent weather reports. Hospital administrators said they are better prepared than in 2009 if high river levels force evacuations, as they did last year. In fact, because of the longer lead time and experience gained from the 2009 floods, some administrators have said it is less likely that evacuations will in fact be necessary this year.

“I think there is greater confidence we are not going anywhere,” said Kris Olson, a vice president at Innovis Health, which even last year did not have to evacuate. “We have the added benefit of time and experience.” Moreover, because the Innovis facility is on relatively high ground, evacuation is less likely there than at other facilities in lower-lying areas. Innovis’s greater concern, Olson said, is the possibility that the public may not be able to reach the hospital.

Because the Innovis facility is on relatively high ground, evacuation is less likely there than at other facilities in lower-lying areas; Innovis’s greater concern is the possibility that the public may not be able to reach the hospital

Protection against floodwaters is not the only concern at the state’s healthcare facilities, which also need water, sanitation, and electrical services on a continuing basis to serve their patients and residents. MeritCare, which had to evacuate hospital patients last year, has stockpiled extra medical supplies, food, and generator fuel, a spokesman said. “We have covered, I think, just about every item that allows us to operate in an emergency mode,” said Dennis Millirons, president of the MeritCare Medical Center.

A Red River level of 40 feet is always dangerous. Last year’s record crest was 40.84 feet, but an even higher level, according to some forecasts, could occur this weekend – and, if it does, would trigger some mandatory decisions at the center, Millirons said. “If it [the water level] does get above

40 feet, we have critical decisions to make about the potential for an evacuation,” he said. “We would be watching very, very closely.”

The Veterans Affairs Medical Center in Fargo is protected by a floodwall that goes to 45 feet on the Red River, but areas relatively close to the medical complex are not as well protected. Around-the-clock dike-watch patrols start at 38 feet. Last year, the VA evacuated patients to St. Cloud and Minneapolis, and treated outpatients at two mobile units parked outside Innovis.

Villa Maria, a 140-bed nursing home on South University Drive in Fargo, is prepared to function without city services, if required, for about 6-8 days. In the event an evacuation becomes necessary, it has made arrangements with sister facilities around North Dakota to help out, president Michael Pfeifer said.

Infrastructure improvements since last year mean the evacuation level at Eventide Retirement Living in Moorhead has increased from 37 to 39 feet on the Red River, said president John Riewer. Last year, most residents who had been evacuated from Eventide were taken to comparable facilities in Minnesota, within 100 miles of Moorhead, Riewer said – but Eventide will do everything possible, he added, to avoid another evacuation this year.

Nevada Emergency Teams Develop “Large-Scale” Contingency Plans

If there is a nuclear attack by terrorists against Reno or Las Vegas, or a similar large-scale incident, those cities, and others throughout the state, will be ready for it, said Frank Siracusa of the Nevada Division of Emergency Management. Although hoping that such an attack never happens, he said, his staff is planning for a worst-case scenario.

There is no evidence to date, Siracusa emphasized, that any such attack is being planned, or perhaps even possible at this point. But the state must plan for such a large-scale incident, he pointed out, in order to be ready if any incident that serious in nature ever does happen.

“We need to be prepared to move to protect life and property,” he said during a press conference last week on the state’s emergency planning.

Nevada Governor James A. (Jim) Gibbons, who also met with the press, said “It is not that we know or believe an incident is going to occur – Nevada is just leading the way in planning.” Gibbons said that Nevada, working with federal agencies, is developing a model (plan) that other states can build on. Nevada officials are in general agreement with outside experts that the Las Vegas Strip is the most likely target in the state – and potentially one of the top five targets in the entire country. According to those same experts, a 10-kiloton nuclear device exploded on “the Strip” would kill up to 150,000 people at ground zero and another 50,000 within a one-mile radius. More than 40,000 other residents, and visitors, would be injured. A similar attack in Reno would produce an estimated one-third to one-half the same number of casualties.

The planning now under way should provide guidance in handling the entire event from the first indications of an actual threat to the immediate response to the blast to and through the recovery stage of the incident. Nevada’s Division of Emergency Management is planning to develop guidelines for all aspects of a large-scale incident – including but not limited to a major surge in medical needs, the handling of a large number of dead or disabled citizens, and the no-notice provision of major stocks of medicine, food, and other supplies. Other planning guidelines will address such important needs as shelter, decontamination, rescue operations, and the security and restoration of critical infrastructure – including communications, water, and power facilities.

Nevada is the nation’s first state, Siracusa said, to begin developing a model plan for this type of disaster. The draft plan is expected to be rolled out in May, he said, then tested in exercises – scheduled for sometime in July – and finalized sometime in September.

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. He designs and facilitates emergency response drills/exercises for agency responders, state and federal partners, and senior Port Authority executives.



DomPrep Journal readers receive an
exclusive **20% discount off**
the standard fee for all
3 days of the event with
special code
IUS_DB14 #107
when
registering!



BORDER MANAGEMENT™

May 24 - 26, 2010
Tucson, AZ



Securing our Borders with Tactical Strategies and Technologies

Meet key decision-makers and hear from a distinguished speaker faculty that includes:

Bernd McConnell, SES,
Interagency Coordination
Directorate, NORAD and
NORTHCOM

Randy Hill, Chief Patrol
Agent, US Border Patrol,
Del Rio TX Sector, DHS

Matthew C. Allen,
Special Agent in
Charge, US Immigration
and Customs
Enforcement, Office of
Investigations, Arizona

Mark Kraft, Deputy Director,
The National Gang Targeting,
Enforcement & Coordination
Center

Martin Vaughan, Regional
Director, Southwest Border
Operations, Office of Air and
Marine, US Customs and
Border Protection

Terry Azbill, Director,
Southwest Border, HIDTA
- Arizona Region

Don't miss in-depth sessions on effective border management from experts in the field. This is the place for:

- Improving interagency coordination, partnerships and interoperability
- Current capabilities and future initiatives
- Strategies to counter cross border trafficking
- Drug interdiction challenges and operations



Sponsor:



Media Partners:



www.BorderManagementSummit.com/DP