domestic preparedness .com

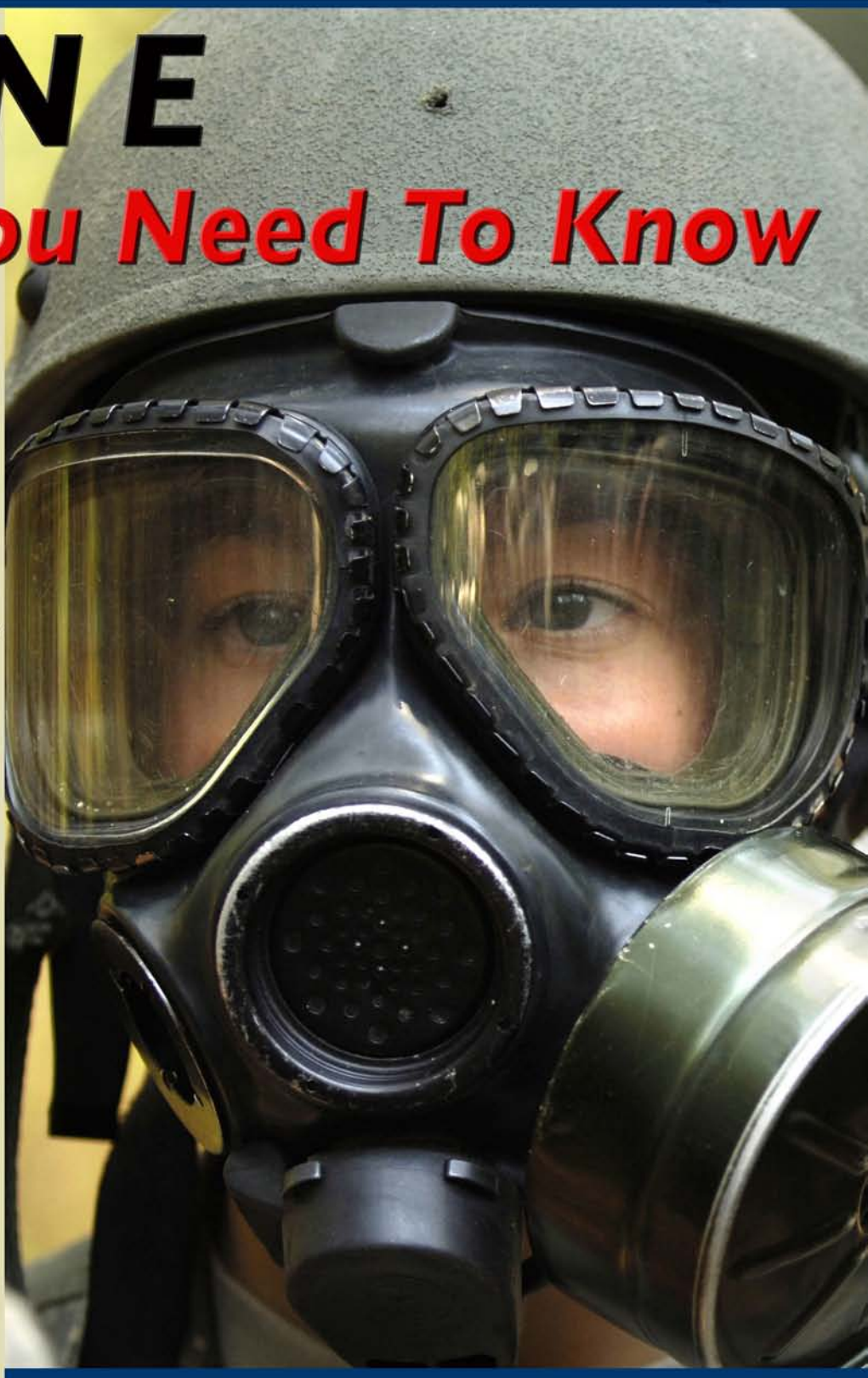
DomPrep Journal

Monthly Edition

US $100 Annual | Volume II, Issue 14 | November 2006

CBRNE

What You Need To Know



Audio Interviews
Dr. Michael Kurilla, NIAID Associate Director
CDR Melissa Sanders, HRSA Branch Chief

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

Arriving first on the scene means you never know what you're going to encounter.

Today that could include life-threatening chemical nerve agents which may be lethal in seconds.

Immediate evacuation and wearing PPE is essential, as is being equipped with auto-injectors that are designed to administer antidotes in emergency situations such as these. Unlike a syringe which can be cumbersome and time-consuming, auto-injectors provide a quick and portable drug delivery in just two steps.

Hope for the best. Prepare for the worst.

You can't rely solely on antidotes for protection, but you can be better prepared for the worst. **Call today—Meridian can help you prepare.**

MERIDIAN
MEDICAL TECHNOLOGIES™

Protecting Those who Protect Us™

www.meridianmeds.com
800.638.8093

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

Staff
Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Managing Editor & Interviews
jmorton@domprep.com

Susan Collins
Subscription Mgr. & Layout/Design
subcriber@domprep.com

Sharon Stovall
Web Content Coordinator
sstovall@domprep.com

Carole Parker
Database Management
cparker@domprep.com

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

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

IMR GROUP

EDITOR'S NOTES

By James D. Hessman, Editor-in-Chief

Slightly more than half of the articles in this "omnibus" printable issue of *DomPrep Journal* deal with various aspects of the lethal, portable, and increasingly mobile threat posed by CBRNE weapons. That useful albeit inelegant-sounding term stands for chemical, biological, radiological, nuclear, explosive weapons, previously lumped together under the acronym WMD (weapons of mass destruction).

Americans have been reading and hearing about WMDs and CBRNE weapons for quite a few years – mostly in the international news sections of newspapers and magazines, and on the "world news" segments of prime-time television. In the not-too-distant future the same type of stories are likely to be considered local news – as in Oklahoma City when the Murrah Federal Building was destroyed by home-grown American terrorists.

The terrorist bombings in Mumbai, Bali, Madrid, and London also were local news – but the psychological and emotional fallout spread around the world with the speed of summer lightning. Presidents, premiers, and prime ministers all knew, as did the proverbial man in the street, that "if it could happen there, it also could happen here." Some of the more prudent of those national leaders, and a handful of the major nations on the terrorists' most-hated list, took meaningful action to detect, prevent (if possible), and/or deal with the cataclysmic consequences of CBRNE attacks on their own major cities.

The most common reaction, though, was to put the CBRNE problem into the too-hard basket – right next to the avian-flu problem, another of those global dangers that seem to most citizens impossible to prevent, too costly to deal with even in the planning stages, and perhaps – a very prayerful perhaps, of course – not likely to happen in any case. Not here, at least, and not in the near future.

That overly optimistic, a polite way of saying foolhardy, view may be understandable in some respects when it comes to avian flu – and hurricanes, tsunamis, and other so-called "natural" disasters. But CBRNE attacks are manmade disasters, and at least some of them can be prevented – by greater investments in intelligence, for example, and improvements in technology, particularly sensor and detection systems of all types.

Additional and probably greater investments will be required to deal with the consequence-management phases of attacks that are *not* prevented. More and better personal-protection equipment for policemen, firemen, and EMS technicians logically should be first on the priority list. Repeated training, and individual skill drills of all types ranging from tabletop exercises to full-scale simulated attacks affecting an entire state, come next – along with more and better healthcare facilities and equipment, more and better training for healthcare professionals, and meticulously detailed advance planning for mass-casualty scenarios. None of this comes free.

The point made earlier about the unusual number of CBRNE-related articles in this issue deserves amplification. Each of those articles is different. They are not about the same subject, but about widely differing aspects of the same subject: CBRNE attacks – which are now a clear and present danger to the United States and its allies throughout the world. Dealing with such attacks requires planning, the setting of standards, the development of a common vocabulary, and cooperation between and among all components of the domestic-preparedness community. But there probably is no universal standard available, no one-size-fits-all solution. There are, though, many large and small partial solutions. The fitting together of those partial solutions into a cohesive whole is perhaps the most important challenge facing the nation's leaders today, and for the foreseeable future.

Individual citizens can and must help. Not just firefighters and policemen, healthcare professionals and Border Patrol agents, but all American citizens. The sound of millions of voices *will* be heard, and a collective call for action by all of the American people *will* be heeded.

Cover Photo: An Army recruit prepares to enter the gas chamber during their nine-week basic training program at Fort Jackson, S.C. This photo appeared on www.army.mil

WWW.PHPREP.ORG

CONFERENCE DETAILS REGISTRATION HOTEL INFORMATION PROGRAM

Public Health Preparedness Summit 07

action-oriented, practice-based models to improve your community's safety and preparedness

PARTNERING for *Preparedness:* **Strategies & Solutions**

February 19-23, 2007 The Hilton Washington Washington, DC

CBRNE Incidents – The Role of the Firefighter

By Theodore L. (Ted) Jarboe, Fire/HazMat

Five years have passed since the terrorist attacks of 11 September 2001. Although there have been no additional attacks in the United States during those years, most experts agree that there will be future attacks and that the question is "not if, but when." Terrorists have time on their side. They can plan, wait, and launch their attack when and where *they* want.

The specific details are classified, but it is known that the ongoing efforts of the FBI and other law-enforcement agencies, within and outside the United States, already have foiled many would-be terrorist attacks. However, this does not guarantee that terrorists will not be successful in the future – which should be reason enough for the nation's first responders to further improve their operational readiness.

Among the various first-responder units most likely to show up in the earliest stages of a terrorist event involving the release of a chemical or biological agent, or the actuation of a radiological or nuclear device, or the detonation of explosives – CBRNE attacks, in other words – will be local firefighters, police and other law-enforcement personnel, and EMS (emergency medical services) technicians. However, in the event of a covert biological attack, local and state health departments, working in close cooperation with the U. S. Centers for Disease Control and Prevention (CDC) and the FBI, usually will be among the highest-priority responders at the scene as well.

Unless they receive intelligence of an impending attack from local law-enforcement agencies, the FBI, or perhaps a regional JTTF (Joint Terrorist Task Force), firefighters responding to a CBRNE event will not have the initial information they need to alert them that the incident they are responding to may be terrorist-related. Instead, they will have to rely on their own previous CBRNE training, combined with their current on-scene observations, to gather clues as to whether the incident was deliberate. Certain signs and symptoms of casualties may indicate that a chemical agent was used in the attack, for example. In addition, the presence of radiation readings above normal background levels at the scene of an undetermined explosion could be an indicator of a radiological (i.e., "dirty bomb") release.

Self-Protection – The Most Important Priority

Probably the single most important item of a firefighter's personal protection equipment against exposure to a dispersed chemical or biological agent, or to radioactive/nuclear materials (CBRN), is what is called the self-contained breathing apparatus (SCBA) – which, among other things, prevents contaminants from entering the wearer's body through the respiratory tract and/or eyes.

The National Institute for Occupational Safety and Health (NIOSH) is testing and certifying various SCBA systems and other equipment items used by emergency responders working in CBRN environments. To determine if a specific SCBA has been tested, *and certified*, by NIOSH for use by emergency responders in CBRN environments, officials say, inspectors should inspect the system to see if a CBRN agent-approval label is on the respirator. If an SCBA has, in fact, been CBRN-approved by NIOSH, it will always carry such a label.

On the other hand, if a CBRN agent-approval label is *not* on the SCBA, the garment probably has *not* been approved by NIOSH for use by emergency responders working in CBRN environments. (The approval number for an SCBA approved for CBRN environments always includes a CBRN suffix – e.g., TC-1F-XXXXCBRN.)

Properly worn turnout gear (i.e., helmet, hood, coat, gloves, turnout pants, and boots) provides some limited protection against CBRN contaminants entering the body through the skin. However, it does not provide protection against exposure to gamma radiation.

Although ordinary firefighter protective clothing offers some protection against CBRN components, it is not a suitable substitute for the NFPA (National Fire Protection Association) Standard on Protective Ensembles for First Responders to CBRN Terrorism Incidents, also known as NFPA 1994-compliant protective ensembles. NFPA 1994 establishes the minimum requirements for the design, performance, testing, documentation, and certification of protective ensembles, and ensemble elements, designed to protect emergency first-responder personnel from chemicals, biological agents, and radiological particulate terrorism agents.

"No Community Is Immune"

Although terrorists have voiced, and demonstrated, their intention to attack large metropolises such as New York City and Washington, D.C., "any town, USA," might be a viable future target. No community is immune to a possible terrorist strike. Moreover, terrorists could unleash several simultaneous attacks.

Ten years ago, firefighters and other first responders in 120 of the nation's major metropolitan areas began participating in the Nunn-Lugar-Domeneci Domestic Preparedness Program. A principal goal of that program (which later involved some smaller metropolitan areas as well) was to enhance the preparedness of the nation's first responders to manage the consequences of potential terrorist WMD (weapons of mass destruction) incidents. The authorizing legislation designated the Department of Defense (DOD) as lead agency. Among the other major agencies participating are the Federal Emergency Management Agency (FEMA), the Federal Bureau of Investigation (FBI), the DHS (Department of Health and Human Services) Public Health Service, the Department of Energy, and the Environmental Protection Agency (EPA).

The U.S. Army Soldier and Biological Chemical Command (SBCCOM) followed up with the development of an innovative "train-the-trainer" program to build on the existing knowledge and capabilities of local first responders – fire, law enforcement, and medical personnel and hazardous materials technicians, primarily – who would deal with a WMD incident during the first hours after an attack had taken place.

Although terrorists have voiced their intention to attack large metropolises such as New York City and Washington, "any town, USA," might be a viable future target

Consequence Management And Other Priorities

That training, which started in 1997, served as a springboard from which other training programs were launched around the country. The ultimate goal was to better prepare emergency responders throughout the country to respond to and safely manage the consequences of the incident.

Depending on the particular CBRNE agent used in a terrorist event, the first arriving specialist unit probably will be a hazardous materials response team, a bomb squad, or a public health response team. Some local jurisdictions have established and are adequately funding at least some of these specialized response teams, but others have not, and therefore have no option but to rely on state, regional, and/or federal resources.

In any case, the response times of such units heavily influence how helpful they are likely to be in assisting on-scene firefighters. In general, it is safe to assume that, the longer the response time is, the greater will be the stress and challenges to the firefighters and other on-scene personnel attempting to implement their initial consequence-management measures.

Guidelines for Survival

Following are some guidelines recommended by experts to help firefighters improve and/or refresh their response capabilities and, in general, to promote the safer consequence-management phases of CBRNE events:

1. Approach the CBRNE event as if it were a hazardous-materials incident. Although most firefighters are not specialists in the management of hazmat incidents, they should know the fundamental principles applicable to the safe management of such incidents. In essence, a CBRNE event is still a hazardous-materials incident at its core – one, though, that has the potential to injure, sicken, or kill large numbers of people, cause widespread public fear, create a media-response overload, and overwhelm the on-scene resources available. For these reasons alone, on-scene conditions, combined with the perhaps limited training level of the firefighters involved, may limit their actions to a defensive posture while they await the arrival of specialist units.
2. Develop at least a fundamental understanding of the properties and potential consequences of CBRN exposure. The more knowledge that firefighters have about CBRN agents and materials, the safer and more effective they probably will be during the consequence-management phase of CBRN incidents.
3. Prepare CBRNE information and response guides. The infrequency of CBRNE events, and the daily activities of fire-service operations, easily could lead to an environment in which firefighters simply do not devote enough time to adequately address CBRNE event-related concerns.

The latter measure is a relatively inexpensive but very important way to help firefighters quickly review key information during training sessions – and even while en route to a possible CBRNE incident. Here it should be emphasized that such guides, which should be prepared beforehand, not after an incident has occurred, are meant to reinforce prior training, not substitute for it.

Practical Suggestions And Common Sense

Following are some practical suggestions that have been recommended for preparing printed guides:

- Use index stock paper (8-1/2" x 11").
- Identify and include critical CBRNE- and operations-related information and

concerns. For ease of review, keep the points brief and to the point.

- Have the document reviewed for technical accuracy and readability by a subject matter expert such as a hazmat technician, bomb technician, health physicist, and/or public health official.
- Laminate the document for durability, and use a three-hole punch to carry the guide in a binder.
- Ensure that copies of the guides are available for, and carried in, all emergency-response vehicles.
- Prepare an information bulletin about the guides and distribute it to all members of all units at all stations.
- Finally, and probably of the greatest importance, ensure that all personnel are properly trained in the operations described in the guide.

In addition to the preceding, there are other common-sense recommendations that should be standard operating guidelines for all personnel. Here are some of the more important of those guidelines:

- Wear turnout gear properly, and use a self-contained breathing apparatus – but know the limitations of each. Ordinary turnout gear is no substitute for personal protective clothing specially designed for CBR exposure (see the NFPA 1994 standard mentioned earlier).
- Always consider the possibility of a radiological "dirty bomb" and the possible presence of other explosive devices when responding to a reported explosion of unknown origin. Unless the cause of the explosion becomes readily apparent after the initial first responders arrive at the incident scene, use (or obtain) a radiological instrument to check the surrounding area for ionizing radiation. (Some fire departments carry radiation-alerting devices on their emergency response vehicles; others either install them on vehicles when the DHS National Threat Advisory System reaches a certain alert level, or simply do not have them available for use.)
- Conduct on-scene activities consistent with the local department's standard operating guidelines (SOGs) and the individual firefighter's own level of training. Untrained or improperly trained firefighters, no matter how well intentioned, could easily compromise their own safety and the safety of others.
- Develop local action guidelines consistent with the DHS National Threat Advisory System just mentioned. Some fire departments already have created their own threat advisory systems to determine, in advance (insofar as possible), what actions they should take for each of the five national threat levels (low, guarded, elevated, high, and severe) spelled out in the DHS advisory system. A local advisory system should not substitute for the national system, but it *can* enhance readiness, promote safety, improve efficiency, and reduce confusion in the aftermath of a CBRNE event that affects the local community.
- Participate fully and regularly in tabletop and full-scale exercises. Such exercises not only help participants identify the strengths and weaknesses of their own terrorism units and agencies – and perhaps discover ambiguities and/or inconsistencies in standard and local operating guidelines – but also allow them to interact with representatives of local, state, and federal agencies as well as members of the private sector.
- Review, exercise, and revise (if needed) current mass-casualty and decontamination guidelines. The nature and extent of a CBRNE event may require firefighters to triage, treat, decontaminate, and transport large numbers of contaminated casualties.

Maximum Confusion, And the Well-Prepared Mind

To summarize: A CBRNE event can result in a huge number of casualties. It might be a single event, involving one or more CBRNE materials, or several events – occurring either simultaneously or sequentially. Hazardous materials response teams, bomb squads, and public health response teams are among the principal specially trained CBRNE resources that may be (or may not be) available to respond. Nonetheless, local firefighters are likely to be on their own for at least a short time before these other important resources arrive on the scene of an incident. During that period of what might be maximum confusion, firefighters must be not only as resourceful as possible but also totally committed to doing the best they can to prevent the event from claiming more casualties.

The best indicator, perhaps, as to how well a fire department is prepared to respond to a CBRNE event is the level of training and preparedness of all of its operating members. Today, unfortunately, although many firefighters have received substantial CBRNE-related training, and also have participated in exercises testing their knowledge and operational capabilities, others are still in the process of building their knowledge base. In short, there are still too many firefighters in need of CBRNE training. However, regardless of whether they are fully prepared or not, firefighters will be almost always among the first to respond to a fire, explosion, or similar incident.

A word of advice for mayors, county executives, and other state and city officials: A casual visit to the local fire station to talk with firefighters about their domestic preparedness program for the handling of CBRNE events is an excellent way to get an idea as to how well they are (or are not) prepared. Here the important thing to remember is that the fire department's own leaders are primarily responsible for ensuring that the firefighters under their command receive the CBRNE training they need.

Good training builds both competence and confidence. Waiting until a CBRNE event occurs *before* ensuring that firefighters and other first responders are properly trained is not only irresponsible but also can lead to counterproductive decision-making and/or unsafe practices at the scene of an incident. As Louis Pasteur once commented, "Chance favors the prepared mind."

Theodore L. (Ted) Jarboe retired from the Montgomery County (Md.) Fire and Rescue Service after 40 years of career service, including 13 years as a deputy chief, and 20 years as a member of the county's Hazardous Incident Response Team. A former recipient of the National Fire Academy's Outstanding Research Award, he also served for several years as a member of the International Association of Fire Chiefs' Terrorism and Homeland Security Committee, as a guest researcher at the National Institute of Standards and Technology (NIST), and as a chairperson of the Chemical Weapons Improved Response Program of the U.S. Soldier Biological Chemical Command.

Pro and Con, Yea and Nay

Experts' Dialogue on the New HICS Guidebook

By Dr. Michael Allswede and Dr. Jerry Mothershead, Public Health

A new medical-systems guidebook published by the state of California has elicited both praise and criticism from the U.S. medical community – praise because of the wealth of useful information provided and the quality and readability of the guidebook's contents, and criticism because of several significant omissions and the alleged lack of a common-sense perspective in the development of certain comments and recommendations included in the guidebook.

The HICS Guidebook, including the command-structure organization chart referenced below, is available at www.emsa.ca.gov/hics/hics.asp

Without taking sides, DomPrep Journal asked two highly respected medical authorities, Dr. Michael Allswede and Dr. Jerry Mothershead, who hold different but not diametrically opposed views about the guidebook's usefulness, to provide a "Point/Counterpoint" discussion about the guidebook's strengths and weaknesses. Dr. Allswede leads off the discussion with his comments just below.

Dr. Michael Allswede

The state of California has recently published a 117-page "guidebook" that, among other things, provides a methodology for organizing medical systems to respond to an all-hazards problem set that conforms closely to the National Incident Management System (NIMS). Also included in the officially titled *Guidebook for Hospital Incident Command System Development* are 256 additional pages of job action sheets and 56 pages of additional forms and instructions – in other words, a grand total of 429 pages of material describing the duties and responsibilities of a notional 25-person command structure.

The HICS Guidebook also provides an abundance of assorted training materials, and 28 training scenarios to digest. The command-system material is complete and well organized, and represents an admirable effort to conform medical system decision-making to the National Incident Command System – which makes it a particularly valuable resource for the U.S. Department of Homeland Security (DHS).

While this effort is laudable and there is a clear need for such a guidebook, there also are some concerns about this one, the first and most important of which is that the entirety of life-saving personnel resources is compressed into a single box in the command structure called "Medical/Technical Specialists" – an oversized umbrella term which may or may not reflect the operational reality at every U.S. hospital. In addition to the fact that nowhere in the plan is there specific guidance for medical care per se, and/or triage guidelines to use in a variety of scenarios, there are three basic problems with the HICS approach to hospital readiness:

> ***A hospital at work is like a ship underway: Every member of the staff is on the job already or off-duty – but ready for duty on a later shift.***

1. The first is what might be called the "all things to all people" problem. Any plan designed to cover all contingencies in all circumstances may almost by definition be perhaps too large and too confusing to be truly useful in times of crisis without prior training – a lot of it.
2. The "lack of an audience" problem is next in line. The California plan seems to presume that the U.S. government's National Incident Management System is applicable to normal hospital operations and that it simply will be "someone's" job (the specific individual not identified) to provide training for and teach the material provided. The fact is, though, that most disaster training in the United States is today an unfunded responsibility assigned to most medical systems. Unless there is funding provided to train hospital personnel in accordance with the HICS guidelines, that training undoubtedly will be carried out piecemeal, not systematically.
3. The third problem is the complexity of the HICS approach. In times of crisis, personal relationships usually carry more weight than unfamiliar job titles and new and rather complicated organizational diagrams. Common sense suggests that reliance on an unfamiliar scheme with its multitude of responsibilities will fail and that the native system will dominate.

Going Back to Basics

Medical planning should begin with a clear explanation of what is needed to save lives, not on how to conform to some externally recommended structure. The HICS system does not in and of itself deliver care to victims and for that reason alone may not fit too well (if at all) with the variety of hospital administration structures present in American medicine. One of the most important problems in managing a chemical or biological incident, for example, or an infectious-disease emergency, is that a great deal of medical/technical expertise is needed – and that particular expertise is in scarce supply at most of the nation's medical facilities.

As previously mentioned, just one organizational box on the command-structure chart – 1/25 of the overall leadership structure, in other words – is used to encompass *all* of the technical/medical expertise necessary for life-saving operations and medical treatment. That is probably the inverse of what an organizational diagram *should* look like for a typical American medical facility today.

All-hazards planning for hospitals can be simplified, though, into three basic types of response situations:

- ***Trauma Disaster Plan:*** In this response mode, the rapid delivery of large numbers of traumatic casualties is a large part of the problem, and the maximum development of caregivers and the delivery of life-saving treatment in the shortest amount of time are the keys to success.
- ***HAZMAT Disaster Plan:*** In this response mode, the hospital has an ethical obligation to respond, simultaneously and effectively, to victims of a toxic exposure, ensure workplace

safety for its own employees, and preserve a safe care environment for those already admitted to and resident within the medical facility. A rapid decontamination capability, decontamination surety determinations, and the rapid administration of potentially large quantities of unfamiliar antidotal medications are the keys to success.

- ***Infectious-Disease Disaster Plan:*** In this response mode, the hospital has an ethical obligation, once again, to respond to a potentially large number of victims over a potentially protracted period of time, while also ensuring workplace safety for its own employees and a safe-care environment for patients previously admitted but not infected. Here, the segregation of contagious patients from the general hospital population and staff, the management of waste materials, and specimen collection and handling are the keys.

Operational and Fiscal Realities

Each of the plans described above requires guidelines for the individual care needed, the ability to allocate scarce resources, and the procedures to be followed to facilitate and ameliorate the delay – or, in certain cases, denial – of care to victims who either are not salvageable or, more optimistically stated, are not lethally injured. Today, most care guidelines of this type are institution-specific and represent the key capabilities that the command structure must support.

It is important to understand that most of the nation's medical systems also are "high-overhead" businesses – and, as such, must maintain a 95-100 percent bed-occupancy rate to remain financially solvent. That fiscal fact of life permits only a relatively small amount of surge capacity – which is what the HICS command structure is intended to govern. Even in a best-case (95 percent occupancy) scenario, therefore, to use but one example, a 500-bed facility serving a community of 40,000 people typically would have only 25 beds that would be available for use under the HICS command system.

It seems obvious that the current decision-making structure in most medical facilities today is probably sufficient for that task. The creation, therefore, of a NIMS-compliant 25-person command structure to decide the fate of a mere 25 beds – but provide little expertise on medical management per se – would probably not affect (i.e., improve) victim survivorship in any significant way. The medical surge capacity of 25 beds could be used for only 0.625 percent of the local population of 40,000 potential victims of a major disaster. What is clearly and much more urgently needed, it seems, is a methodology to delay, transfer, or – if necessary – deny care to victims of the stricken city.

Are Better Options Available?

Instead of developing and training an expansive (and expensive) command structure, perhaps a better and more useful endeavor would be to create training programs and allow working-level staff to gain familiarity with the equipment and medications they may be required to use in times of crisis. A hospital at work is much like a ship underway: Every member of the staff is either on the job already or off-duty – but ready to report for duty on a later shift.

Although disaster training is often described as a critical need for U.S. hospitals, the idea that a hospital drill actually "trains" the hospital – i.e., all personnel working at the hospital in different assignments and on different shifts – is probably flawed to begin with, because most disaster drills carried out at most U.S. hospitals today train only a single shift of the hospital's personnel for only about one day per year.

The development of "downtime" training and/or incorporation of disaster-management training within the existing educational programming would seem to be a much more efficient way to train the highest percentage of staff personnel – but only if job action sheets and critical medical treatment guidelines are readily accessible for immediate use, not buried somewhere in a large all-encompassing document. An organizational diagram of properly trained and equipped medical providers is clearly needed at almost every medical facility imaginable.

Once the medical-care capability is developed, an adaptable command structure would be relatively easy to create to meet the needs of a trauma, HAZMAT, or infectious-disease emergency. Putting the development of life-saving capabilities ahead of the NIMS planning concept means that the DHS guidelines in this area would, and should, be written to conform to local medical leadership structures, not the other way around.

Dr. Michael Allswede is director of the Strategic Medical Intelligence Project on ForensicEpidemiology and the creator of both the RaPiD-T Program and the Pittsburgh Matrix Program for hospital training and preparedness. He also has served on a number of expert national and international groups in the preparedness field.

Your One Source for Radiological Incident Response

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

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

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

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

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

www.canberra-hs.com

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

CANBERRA

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

Following is the Counterpoint argument provided by Dr. Jerry Mothershead

Although Dr. Allswede presents a cogent argument on the challenges inherent in changing organizational constructs during times of disasters, some of his assumptions beg to be challenged, including:

1. The assumption that healthcare operations are unique: Very few U.S. corporations or concerns are organized for crisis management on a routine basis. Even fire and police departments are administratively organized at odds with those spelled out in the National Incident Management System. The key difference is that entities that frequently respond to crises have a vested interest in rapidly transitioning to whatever organizational structure is most conducive to executing the tasks required for crisis response. Moreover, Dr. Allswede implies that other organizations that train for and practice incident-management operations do not have other duties and missions, whereas those involved with healthcare are "too busy saving lives" to be bothered with training that may be rarely if ever used. *Of course*, training and exercises are required.
2. The assumption that task management is synonymous with task execution: The HICS guidelines were neither intended nor designed to dictate triage or treatment protocols. Although triage and treatment may indeed be the "point of the spear" of healthcare operations, there is an abundance of ancillary and support requirements necessary for the spear to hit its target. In a large-scale disaster (the type that HICS *was* designed for), resource management and logistics may well play more important roles in the final results. Moreover, task management does not necessarily have to be manpower-intensive. One of the more important aspects of the incident-command concept is its inherent expandability. In a small hospital, for example, several if not all of the HICS elements could be combined under one authority – in which case, instead of a 25-person command structure, a 10-person command structure might well suffice, with many or most of those ten persons carrying out their assigned tasks or oversight responsibilities under routine operational guidelines.
3. The assumption that HICS is not a relatively simple concept: Anyone who has been assigned major administrative responsibilities within a corporation or other major organization – whether its principal product line is healthcare or facial cream – understands that the corporate world is anything but *simple*. The HICS guidebook's notional command structure is neither more nor less complicated than any other healthcare operations management system – but it is admittedly *different* (both conceptually and operationally). One of the benefits of training in this system, if it is to be used, is that it affords those in leadership roles (the principal targets of the HICS concept) the opportunity to work together under a different organizational model – and, not incidentally, develop effective working relationships with one another through the training exercises recommended or mandated. That training does not have to be exhaustive, or all-inclusive, for all staff personnel at the healthcare facility. A radiology technician's tasks, for example, will probably not change much in a disaster. A clinician's tasks *might* change somewhat. The head of a department may be required to make new and different decisions in times of crisis, and may be constrained in his or her decision-making because of actions, or limitations, in other healthcare operations sectors with which he or she has little routine interaction.

Cost/Benefit Ratios And Other Considerations

Nonetheless, there *are* some important problems associated with the HICS organizational structure in its present form, including a few not specifically addressed by Dr. Allswede. It should be kept in mind, for example, that most hospitals are not government entities. Their existence is dependent on profit margins – as he does point out. Education, training, and exercises are both labor-intensive and expensive, and allocating limited resources on these evolutions, which not only are targeted on low-probability events but also are carried out without remuneration from the federal government, simply does not make good business sense. It is true that some funding has been provided to the healthcare sector in recent years – in most cases on a per-hospital basis – but in virtually all cases the funding provided was insufficient to even add one full-time staff member for emergency operations, much less train the entire hospital staff.

Education, training, and exercises are labor-intensive and expensive, and allocating limited resources on these evolutions simply does not make good business sense.

Another socio-economic fact of life that should be kept in mind is that hospitals are not islands. Although there are many American communities that, in theory, are serviced by only one hospital, there are very few if any that are serviced by only one healthcare facility – a more generic term that also includes physicians' offices, clinics, and other medical (but non-hospital) facilities. Moreover, in almost all American communities the healthcare facilities themselves rely on an outside medical infrastructure, including freestanding pharmacies, medical supply distribution centers, and even local public health departments. For this reason, the HICS focus would perhaps be better directed toward a "community health" incident command system in which these disparate and sometimes competing components of the public health, healthcare operations, and ancillary/support services could be more cohesively organized to respond to the large-scale disasters that HICS was designed to address.

Controversy undoubtedly will continue–at least within the nation's health industries–about the utility of such command re-organizations as that offered by the HICS Guidebook. Such controversy is not only reasonable and to be expected, it also is desirable as well. It is obvious at this point that all sides want the same thing – namely, the most good for the most people. What specific system will, or will not, work best remains to be seen.

Dr. Jerry Mothershead is the physician advisor to the Medical Readiness and Response Group of Battelle Memorial Institute. An emergency medicine physician, he also is adjunct faculty at the Uniformed Services University of the Health Sciences in Bethesda, Md.

The Vocabulary of Terror

CBRNE Weapons – What's in a Name?

By Joseph Cahill, EMS

Terms are developed in every profession, and emergency management is no exception. In recent years, in fact, many of the terms used by emergency managers have seeped into common usage – and, unfortunately, have frequently been misused, making them a source of confusion rather than clarity.

Biological weapons, sometimes referred to at BT, are either disease-causing agents or toxins derived from living things or resulting from a biological process. The focus in many discussions about biological weapons is on disease-causing agents such as plague, anthrax, smallpox, and tularemia – in short, *germs* of one type or another. Also included in this class of weapons, however, are organic toxins such as ricin, which is manufactured from caster beans, and botulin toxin, which is a waste product produced by a bacteria.

Chemical weapons are poisonous chemicals that can be used as weapons. These are often broken down into five principal types: choking agents; blood agents; blister agents; nerve agents; and hazardous industrial chemicals.

Choking agents kill by displacing oxygen in the environment – for example, chemicals such as chlorine or phosgene gas fill an area, making oxygen unavailable for breathing. These chemicals also cause inflammation and damage to the lungs, creating a physical barrier to breathing. Blood agents, such as cyanide, interfere with the blood's ability to carry oxygen, in effect asphyxiating the victim in his or her own tissue, even in the presence of normal levels of oxygen.

Blister agents, such as Lewisite or mustard gas, are chemicals that cause severe tissue damage in the form of blistering of the skin, eyes, and/or lungs. Weapons such as sarin and what is called G-agent are weapons that temporarily disconnect the nervous system, including the parts of the system that allow/cause a person to breathe. The term "temporarily" is purposely used here, because if medical care can be provided fast enough to breathe for the victim, and to manage the seizures that nerve agents often cause, the victim has a good chance of survival.

Non-lethal or incapacitating agents are chemical weapons such as pepper spray or agent 15 – chemicals that cause non-life-threatening irritation or stupor/confusion. Finally, many materials used in the modern world not only could be used as weapons but also have properties similar to those of chemical weapons. These materials also would be attractive materials for terrorists.

Radiological and nuclear weapons both contain radioactive materials – i.e., materials that are unstable at an atomic level and therefore decompose, giving off radiation. The focus of much of the nation's civil-defense planning in the 1950s and 1960s was to prepare for attacks by another nation (usually the USSR or Communist China) using a nuclear weapon. Radiation and nuclear weapons use the radioactive nature of some materials as the energy source for a massive explosion.

The emergence of stateless terrorists on the global scene in recent years has led to discussions centered on the radiological dispersion device (RDD) – otherwise known as the dirty bomb. Despite its inelegant (and imprecise) name, the dirty bomb is really just a normal explosive with radioactive materials added, making it a weapon designed to damage and contaminate a relatively large area. The distinction between the dirty bomb and a true nuclear weapon is the source of the energy, which in the case of the RDD comes from a conventional explosive.

Finally, conventional explosives are simply just that: materials that cause a detonation or explosion – i.e., a rapid release of gas under pressure. A relatively large number of common-place materials can be and have been used as explosives. Among them are some substances that would not ordinarily be considered dangerous but can and would explode if they are tightly contained while the materials burn.

The Internationalization Of Everyday Acronyms

A variety of terms have been used, and shortened into acronyms, in various attempts to groups all of these weapons into a single all-encompassing term. The U.S. military used the acronym NBC to describe nuclear, biological, and/or chemical weapons; a somewhat similar acronym, ABC, was used to describe atomic, biological, and chemical weapons. A somewhat more generic term WMD – Weapons of Mass Destruction – has been common within the response community for a decade or more, but did not become part of the national vocabulary until the media spotlight started to focus on Iraq, which under Saddam Hussein used chemical weapons both against Iran and against some of its own citizens.

More recently, the term CBRNE (chemical, biological, radiation, nuclear, and explosives) has become more commonly used in emergency-management circles, primarily because it can be used to describe all of the threats mentioned above.

Links for additional information:

General

http://www.dtic.mil/doctrine/jel/new_pubs/jp1_02.pdf

http://dictionary.laborlawtalk.com/weapons of mass destruction

http://www.phsource.us/PH/CBRNE/index.htm

Chemical

http://www.cdc.gov/niosh/topics/emres/chemagent.html

http://www.bt.cdc.gov/chemical/

Biological

http://www.bt.cdc.gov/bioterrorism/

Radiological/nuclear

http://www.bt.cdc.gov/radiation/

http://dictionary.laborlawtalk.com/dirty_bomb

---

*Joseph Cahill has served as a line paramedic for over ten years in The South Bronx and North Philadelphia. He was awarded the distinguished service medal and seven pre-hospital "saves" ribbons from NYC*EMS and FDNY as well as a unit citation from the Philadelphia Fire Department, and has received both the 100-Year Association's award for "Outstanding Service to New York City" as well as the World Trade Center Survivor's Ribbon (two bronze stars).*

Can U.S. Defeat the Suicide/Homicide-Bomber Threat?

By Joseph Steger, Law Enforcement

The threat posed by suicide/homicide bombers is already a reality for American law-enforcement agencies and personnel, and seems likely to grow in both scope and magnitude in the foreseeable future. Understanding motivational variables is important – but less important in terms of response and interdiction than improvements in tactics, training, and procedures. As a small town police department in upstate New York learned nearly a year ago, a "common criminal" with explosives attached to his body is not merely another weapons system challenging American law-enforcement personnel today but a weapons system of potentially massive lethality.

Unfortunately, few U.S. law-enforcement agencies have trained officers on tactics specifically designed to interdict and cope with suicide/homicide bombing tactics. The Technical Support Working Group, however, has developed a "training support package" – *Preparation for the Suicide/Homicide Bomber* – that examines this attack tactic for domestic law enforcement from both the pre-detonation and post-detonation perspectives. The training support package has been accepted by the DHS (Department of Homeland Security) Office of State and Local Coordination (formerly the Office of Domestic Preparedness) for federal grant expenditures.

Choosing the timing and location for interdicting a suspected suicide/homicide bomber is critical. If possible, interdiction decisions must include a situational assessment based on the worst-case scenario: detonation. The dedicated suicide/homicide bomber is focused on maximizing casualties among the target population. It should be kept in mind, though, that his (or her) most important operational goal is homicide, not suicide. Denying the suicide/homicide bomber the possibility of causing a large number of casualties creates a mission-failure situation.

A Broad Spectrum Of Attack Scenarios

Another factor to consider is that certain locations may be better both for a reduction in casualties and to contain a blast resulting in massive damage. U.S. law-enforcement officers are accustomed to making location assessment – in deciding where to initiate felony traffic stops, for example, and/or in determining the best timing and location for high-risk warrant service. The same basic concepts used in those situations are adaptable to dealing with suicide/homicide bombers and other emerging threats of the 21st century.

It also is possible that a suicide/homicide bomber, particularly one who is part of a terrorist group, may have a redundant detonation option available to provide a higher probability of mission success. "Command detonation" – i.e., detonation by another person not in the immediate vicinity of the suicide/homicide bomber – is a realistic possibility in numerous "martyrdom" types of operations. In such operations the improvised explosive device (IED) carried or worn by the bomber may be either under his/her control or under the control of another person. Law-enforcement officers should be trained to deal with this possibility. Back-up response units, particularly, need not only training and operational conditioning but also the ability to look for persons, other than the bomber, who are in the area and may possess a command-detonation capability.

Persons suspected of being command operators need to be swiftly detained and rendered incapable of activating any number of wireless types of remote detonators. Implementation of this countermeasure requires not only a broad operational awareness of the threat potential but also well executed police command direction to ensure operational coordination with the on-scene interdiction actions being taken. This scenario is similar in many respects to the situations in which high-risk warrant-execution teams require cover team protection from potential threats external to the target location. In certain fire-response situations, to cite another operational example, on-scene investigators usually will be focusing their attention on the gathered crowd, looking for possible arsonists enjoying their malicious handiwork.

The First Rule of Survival

The 21st – century police officer must be prepared to face IED situations, including those in which the IED is carried or worn by the attacker. In certain respects, IEDs – like firearms, blunt objects, and edged weapons – may be viewed as merely another weapon system. *Unlike* these other traditional weapons, however, the person-controlled IED represents an omni-directional threat. Police-interdiction tactics must therefore focus on the best use of cover when facing a suicide/homicide bomber. Here it should be remembered that one of the best types of cover available, in many situations, is a depression (natural or manmade) in the terrain. In an urban environment, for example, an officer working from behind a curb is afforded greater personal safety than would be possible if he/she were behind a car or mailbox at the same distance from the IED-carrying bomber.

Law-enforcement officers need to understand the application of existing departmental use-of-force policies to the suicide/homicide bomber threat. Marksmanship proficiency also needs more attention, especially at longer distances. In dealing with IEDs the operating principle is both clear and simple: *distance equals survival*. Improved marksmanship proficiency, coupled with ready access to urban patrol rifles, will greatly enhance officer survivability in the interdiction of suicide/homicide bombers.

Precise shot placement is particularly critical in effectively applying the deadly-force option in dealing with a suicide/homicide bomber. The traditional firearms training doctrine of "center mass" shooting is *not* preferred or recommended in these situations. Applying ballistic impact to the center mass of a person with explosives strapped to his or her torso is likely to *cause* detonation, particularly if the explosive charge itself is hit. The International Association of Chiefs of Police (IACP) has issued guidance, in fact, that, whenever possible and appropriate, the officer should aim at the bomber's head in a suicide/homicide interdiction operation.

The rationale here is that the probability of immediate incapacitation is far greater in certain areas of the head than it is in any other part of the human body. The goal is immediate incapacitation – i.e., the interruption of

neuromuscular impulse so instantaneous that the suspect bomber is incapable of causing detonation. However, immediate incapacitation with a firearm requires considerable skill in applying the principles of marksmanship. In other words, there are no shortcuts in attaining proficiency when using the deadly-force option to prevent a suicide/homicide bomber from detonating the IED he/she may be wearing or carrying.

In recent years, terrorist groups have become more versatile and more flexible in their operations. For that reason, the operational doctrine for U.S. law-enforcement agencies must be equally flexible – and should assume, for example, that effective police responses, now and for the foreseeable future, must include a fundamental assumption that secondary devices may be detonated and/or that multiple attacks – either sequential or simultaneous – may be planned.

Greater Dangers Vs. Basic Strengths

In the terrorist application of martyrdom operations, a common operational objective is to overwhelm local emergency-services capabilities. Multiple attacks – as was dramatically demonstrated in the London bombings of 7 July 2005 – are often well planned and synchronized. Such attacks may be designed, in fact, to target the emergency-services units responding to the initial attack – which in retrospect would be recognized as merely a precursor to the main attack. The two-pronged suicide/homicide bombing in Bali in 2002 is an example of a strategically planned incident designed with the clear objective of maximizing casualties, specifically including first responders, by starting with a smaller person-borne attack that is quickly followed by a secondary, but larger and more lethal, vehicle-borne detonation.

Today, unfortunately, emergency services agencies throughout the U.S. homeland are behind the power curve in preparing their officers and communities for the detection and interdiction of martyrdom operations. Moreover, the recent transitioning of the suicide/homicide style of bomber tactic from ideological-based crime to economic-based crime increases the likelihood that everyday Americans will soon encounter the same fear tactic familiar to the citizens of many other nations around the world.

Applying the operational lessons learned from military, police, and security services on the global stage can help prepare the U.S. emergency-services community for this additional element in the all-hazards arena. For this to happen, though, the international experiences endured, and countermeasures developed, must be systematically synthesized into the U.S. legal and procedural processes. This requirement is particularly important when one considers that many of the new generation of law-enforcement officers now entering police academies already have received military training and – particularly if they have served in one of the nation's armed services – have first-hand experience in facing martyrdom operation attacks.

To summarize: The preparedness capabilities of U.S. domestic emergency-services agencies must be expanded and improved from the basic skills level up through the command level, particularly in development of the tactics needed to deal with the pre-detonation and post-detonation aspects of martyrdom criminal attacks. Fortunately, the U.S. law-enforcement community has a long history of adaptability in facing dynamic criminal elements. This basic strength must be leveraged in preparation for the domestic-operations phases of the asymmetric war on all forms of criminal activity that incorporate terrorist weapons systems.

In short, homeland law-enforcement training, tactics, policies, procedures, and technology all should be adapted to a "full engagement" mode to deal effectively with the suicide/homicide bomber scenario. This is not a theory and not a supposition. It is, rather, one of the real-life situational realities of domestic law-enforcement operations in the 21st century.

Joseph Steger is the pen name used by a law-enforcement officer with nearly 30 years of service, including a 20-year career with the U.S. Marshals Service, where he reached the rank of chief deputy U.S. Marshal. He also served in other law-enforcement assignments, including duty as a firearms instructor, before accepting a senior law-enforcement position with the U.S. Department of Homeland Security. He developed a training program to prepare law-enforcement personnel to deal with the proliferation of suicide/homicide bombings. Thanks to his long association with the Technical Support Working Group, that training program was published in 2004 as a training support package through the National Terrorism Preparedness Institute. For additional information about the Technical Support Working Group see www.tswg.gov

CBRNE: Beyond the Coast Guard Strike Teams

By Christopher Doane and Joseph DiRenzo III, Coast Guard

"One of the most difficult challenges we face is to prevent, deter, and defend against the acquisition and use of WMD by terrorist groups. The current and potential future linkages between terrorist groups and state sponsors of terrorism are particularly dangerous and require priority attention. The full range of counter-proliferation, nonproliferation, and consequence-management measures must be brought to bear against the WMD terrorist threat, just as they are against states of greatest proliferation concern."

National Strategy to Combat Weapons of Mass Destruction, December 2002

Most first responders in the United States and their counterparts overseas are aware of how the U.S. Coast Guard's National Strike Force (NSF) Strike Teams have been developed and trained to be able to respond both quickly and effectively in times of national crisis. These teams, which are *national*-response assets available to support any U.S. agency that needs them in times of crisis, operate out of Fort Dix, New Jersey, Mobile, Alabama, and Novato, California. These headquarters put them in good position to provide a ready response to oil spills, hazardous material releases, and CBRNE (chemical, biological, radiological, nuclear, and explosive) incidents that occur anywhere within the United States or overseas. The teams are not only well trained but also equipped with the protection gear (up to Level A – i.e., fully encapsulated) needed to enter hazardous environments to perform a variety of tasks.

Although the Strike Teams are not only very capable but also able to deploy rapidly, they are not, strictly speaking, front-line first-response assets. They first must be requested by the agency or department with command responsibility at the scene of a national incident, and then travel to that scene by land and/or air – a process that in most situations would take several hours even in a best-case scenario. The true front-line forces of the Coast Guard are the men and women operating from shore stations and ships located throughout the U.S. maritime domain and carrying out their duties on a 24/7 basis – boarding vessels, visiting waterfront facilities, and responding to emergencies alongside their local agency counterparts on a daily basis.

These are the Coast Guard members best positioned to detect CBRNE weapons or precursors that terrorists may attempt to smuggle into the U.S. homeland by sea. They also, therefore, are not only the first but also the most likely to be called on to respond to a CBRNE incident in the maritime domain.

Improving the ability of Coast Guard front-line personnel to actually operate in a hazardous environment is the focus of a new effort by the service

All-Hazards, All-Purpose Safety Equipment

As part of the U.S. strategy to improve the nation's overall ability to detect and respond to CBRNE weapons, the Coast Guard has equipped its front-line personnel with a broad and growing spectrum of detection systems and emergency-egress equipment. In the not-too-distant future, every member of every Coast Guard boarding or inspection team will be wearing both a personal radiation detection (PRD) device and a gas-alert clip – the latter is designed to detect the presence of chemical agents.

The PRD is a simple device that detects the presence of neutron and/or gamma radiation. When a PRD activates, Coast Guard team members are instructed to call back for more sophisticated equipment (U-identifiers and radiation backpacks) that can localize and characterize the radiation source. The information developed is quickly shared with Department of Energy personnel to determine if a threat exists. The latter step is necessary because so many materials carried as cargo emit radiation, thus creating a high potential for false alarms.

The gas-alert clips measure the levels of oxygen, hydrogen sulfide, and carbon monoxide in the air as well as the lower explosive limit of the local environment. Each of these readings may be an indicator of a possible chemical weapon as emission from such weapons can displace oxygen, emit the other gases listed, and create a potentially combustible concentration of gases. Activation of the gas-alert clip warns the wearer that he or she may be entering an unsafe environment. In such cases the clip wearer is instructed first to exit the space as quickly and as safely as possible, then to start an assessment to determine why the alert sounded.

The emergency-egress equipment consists primarily of protective suits and masks – including emergency-escape breathing hoods – that personnel can don quickly to escape from a hazardous environment should a CBRNE weapon detonate in the vicinity. It is important to emphasize that this equipment is designed for *escaping* the hazardous environment, not to remain in the environment for any reason.

Improving the ability of Coast Guard front-line personnel to actually operate in a hazardous environment, however, is the focus of a new effort by the service. The Coast Guard also has launched a pilot program to understand the challenges involved with developing and sustaining the expertise necessary for operating in a hazardous environment, and is equipping its people with the detection systems and sensors they need to perform a variety of other missions on a daily basis.

The service's goal is to develop an initial maritime CBRNE response capability that can function effectively in coordination with other local responders until more expert and capable surge forces such as the Strike Teams arrive. Fulfillment of that goal will be another milestone in the unending process of making the U.S. homeland safer, more secure, and more survivable.

Christoper Doane (pictured) and Joseph DiRenzo III are retired Coast Guard Officers who are now employed as civilian port security advisors at Coast Guard Atlantic Area. They also are Visiting Senior Fellows at the Joint Forces Staff College in Norfolk, Va., where they lecture on maritime security.

The National Information Exchange Model

By Thomas O'Reilly, Law Enforcement

The fundamental requirement for the sharing of information among and between the many agencies engaged in the detection and prevention of terrorist acts, and/or in the response and recovery to such acts or major hazards, is that the exchange of critical information must be both accurate and provided in real time. The management of major incidents often requires the ability to escalate the response to include other agencies and organizations from the disaster-management and emergency-management communities, as well as private-sector infrastructure providers – all of which will require active feeds of information on the status and disposition of the incident.

U.S. emergency-management systems and protocols, from pre-planning to incident command, must enable the sharing of critical information and intelligence about impending threats to public safety among the relevant government and private-sector organizations responsible for the prevention of, and response to, such threats.

To meet this need, a new standard, the National Information Exchange Model (NIEM), has been created. NIEM is designed to support the numerous communities interested and involved in improving the U.S. ability to respond to and manage major incidents of all types, and is intended to become the standard of choice for facilitating information sharing between and among: the national intelligence community and law-enforcement agencies; police, fire, and EMS first responders; emergency and disaster-management agencies and departments; and the many other organizations that may at one point or another become involved.

It is envisioned that, as the NIEM program matures, a multitude of national priority scenarios will be developed in which the NIEM model will be able to facilitate the sharing of information across a multitude of organizational and functional boundaries.

An Historical Perspective

Through its Bureau of Justice Assistance (BJA), the Department of Justice (DOJ) established a framework for collaboration through what is called the Global Information Sharing Advisory Committee – Global for short. This gave way to the development of the Global Justice XML Data Model (GJXDM), an XML-based standard designed to support the sharing of information throughout and across the justice and public-safety communities.

The GJXDM is first and foremost a set of common terminology and definitions that can be used to link disparate computer systems and technologies. BJA led the development of this standard by encouraging local, state, tribal, and federal agencies to adopt standards – working in collaboration with industry – formulated by a diverse group of practitioners. As a result of this approach, there are now more than 200 GJXDM implementations throughout the United States.

Recognizing the success of the GJXDM initiative, as well as the success of technology-based information-sharing standards used in other government sectors, DOJ and the Department of Homeland Security (DHS) executed a Memorandum of Understanding to create the NIEM program as a way to provide

broader capabilities for sharing information across multiple sectors. NIEM is an open standard that is technology-neutral and therefore can be used as the bridge to connect local, state, tribal, and federal information systems to share critical information in support of the operational missions of participating organizations.

The NIEM Program in Brief

In response to a recommendation in the 9/11 Commission Report, the Office of the Director of National Intelligence (ODNI) was created. The program manager for the Information Sharing Environment, which Congress created and placed within the ODNI, is in the process of echoing the importance of information-sharing standards and is seeking to use such standards as NIEM. Accordingly, the vision for NIEM is to become the national standard, by choice, for critical intergovernmental and cross-sector information exchange by communities essential to maintaining public safety and homeland security.

The principal goals of the NIEM program are straightforward and easy to state:

- Improving justice, public safety, and homeland security;
- Enhancing the quality of critical decision making among relevant government and private-sector communities; and
- Providing an attractive standard for government and industry that increases efficiency and effectiveness, raises quality, and reduces the risks associated with the implementation of complex information-sharing solutions.

In concert with this vision, NIEM is intended to provide information-sharing capabilities in support of major incidents, as well as daily local operations that require multi-agency responses. All too often, these situations illustrate the challenges that public safety organizations are still struggling with when trying to effectively share information across disciplines and jurisdictions. Ironically, many citizens and government decision makers alike believe that organizations today can instantly share critical information at key decision points. This is often not the case, despite the fact that these capabilities are regularly portrayed in other areas of modern society in which decision makers can readily share information and effectively communicate.

Many Approaches to the Same Goal

Those working to develop capabilities for the sharing of information within and across public-safety and homeland-security disciplines know that their own situations may be considerably different. Although many organizations perform similar operational functions, their internal business processes are dissimilar, they typically use different emergency-response protocols and procedures, and most are dependent upon information-system solutions and technologies that do not interoperate with those of other agencies.

To meet this challenge, NIEM can provide a national mechanism to provide public-safety and relevant homeland-security organizations with a standard for effectively and efficiently sharing information in a timely and secure manner, regardless of their fundamental differences in operations. First, NIEM provides a basis for addressing the nature and understanding of the information required to be shared between them. Second, NIEM provides a standard for accomplishing this without disrupting the internal operations and business practices of individual organizations.

The NIEM model already is facilitating information exchanges from state and local communities of interest, and providing the standards for implementation of shared services on a national basis. The goal is to facilitate the nationwide exchange of information among the many different organizations involved in preventing and responding to incidents threatening the nation's safety and security. An initial set of national priority exchanges have been identified and will be expanded through scenario-based planning with active and new constituent communities. Among the missions included on the list are: incident reporting; fusion center integration; case management; people screening; the reporting of suspicious activity; cargo screening; emergency and disaster management; the creation and maintaining of a terrorist watch list; and infrastructure protection.

NIEM Release 1.0 was moved into production in October of 2006 and is now available at http://www.niem.gov to interested organizations for the analysis, design, and implementation of their information-sharing solutions. NIEM users are supported by a knowledge base and help desk available at http://it.ojp.gov/gjxdm/helpdesk, and the first national NIEM training event – during which experts will provide students with "hands-on" instruction in the use of the NIEM model – is scheduled to be hosted by the IJIS Institute at its Ashburn, Va., facility in the near future.

The NIEM Program Management Office (PMO) has been working across a number of governmental organizations and industry associations seeking interested early adopters for NIEM use, and invites all interested organizations to join in this initiative of national significance.

NOTE: Organizations interested in becoming early adopters of the NIEM model should contact Thomas O'Reilly at the Bureau of Justice Assistance at 202-204-6026.

Links for Additional Information:

Global Justice XML Data Model
http://it.ojp.gov/topic.jsp?topic_id=231

Global Justice Information Sharing Initiative
http://it.ojp.gov/topic.jsp?topic_id=8

National Information Exchange Model (NIEM)
http://www.niem.gov/

NIEM Executive Briefing
http://www.niem.gov//files/NIEM_Executive_Briefing.pdf

GJXDM Executive Briefing Presentations
http://www.it.ojp.gov/topic.jsp?topic_id=195

GJXDM/NIEM National Users Conference Presentations, September 2006
http://www.it.ojp.gov/topic.jsp?topic_id=240

NIEM Definition and related terms
http://en.wikipedia.org/wiki/National_Information_Exchange_Model

---

Thomas O'Reilly serves as a Senior Policy Advisor for the National Criminal Justice Association. In this capacity he assists the U.S. Department of Justice, Bureau of Justice Assistance, and the Program Management Office of the National Information Exchange Model (NIEM) Program with information-sharing programs and also serves as the business and outreach director. A former administrator of the New Jersey Department of Public Safety, O'Reilly also has served as president of the National Criminal Justice Association, as vice chairman of the Global Project for the Department of Justice, and as a member of the NCIC Committee of the FBI Criminal Justice Advisory Policy Board.

Special Report

First National Security Cutter Christened; Bertholf Honors First Coast Guard Commandant

By Gordon I. Peterson, Coast Guard

The progressive modernization and recapitalization of the Coast Guard's aging legacy fleet marked a significant milestone on Veterans Day when the first of eight national security cutters being built under the service's Deepwater Program was christened *Bertholf* (WMSL 750) at the Northrop Grumman Ship Systems shipyard in Pascagoula, Miss.

"In the name of the United States of America, may God bless this ship and all who sail in her," said Mrs. Meryl Chertoff, the *Bertholf's* sponsor – and wife of Secretary of Homeland Security Michael Chertoff – as she smashed a bottle of champagne across a strike plate mounted to the cutter's bow. The audience of more than 1,000 guests erupted in applause, accompanied by the Coast Guard Band's spirited rendition of *Semper Paratus*, the Coast Guard's service song. The *Bertholf* is the first major cutter to be christened for Coast Guard service since the 378-foot high-endurance cutter USCGC *Midgett* was launched 35 years ago.

Although built primarily for deepwater missions for maritime patrol and interdiction, as their name implies, the *Bertholf* and her sister ships also will strengthen the Coast Guard's homeland security and defense capabilities as well, not only along the U.S. East, West, and Gulf Coasts, and inland waterways, but also throughout the entire maritime domain.

During the nearly two-hour ceremony in Pascagoula, speakers recognized Coast Guard veterans dating back to World War II who were in attendance, praised the shipyard workers who overcame the devastation of Hurricane Katrina to resume work on the cutter with minimal delay, and saluted the men and women throughout the Coast Guard for their continued vigilance and service to the nation in all of their maritime missions. "Our people cannot be effective without the proper tools," said Adm. Thad W. Allen, the commandant of the Coast Guard. "*Bertholf* and her successors will be the most capable and interoperable cutters the service has ever had."

> ***"We again face a time of great danger to our nation's security; we again are called upon to assist Coast Guard operational forces in executing their challenging missions." Rear Adm. Gary T. Blore, IDS program executive officer***

Rep. Gene Taylor (D-Miss.), a Coast Guard veteran, noted that the time will come, perhaps sooner than anyone expects, when the Coast Guard will again be called to respond to a major attack on the U.S. homeland. "So it is fitting that our nation is providing you with a great ship and great training, but at the end of the day it's going to take the great people that you are to make those things work," he said.

Flagship of the Fleet

At 418 feet, the lead ship in the new Legend-class of national-security cutters (NSCs) is designed to be the flagship of the U.S. Coast Guard's fleet, capable of executing the most challenging maritime-security missions and being supportive of a shared Coast Guard-Navy commitment to the mission requirements of the joint U.S. combatant commanders. The NSC is the largest and most technologically advanced class of the Integrated Deepwater System (IDS) program's three major classes of cutters.

Bertholf is named in honor of Commodore Ellsworth P. Bertholf, the Coast Guard's first commandant. Appointed to lead the Revenue Cutter Service in 1911, he was re-appointed to the same office in 1915 when President Woodrow Wilson created the U.S. Coast Guard by merging the Revenue Cutter Service with the Life-Saving Service. Honored in his day for the heroic rescue of more than 200 whalers stranded in the Arctic in 1897, Bertholf also led the Coast Guard with distinction during World War I.

Rear Adm. Gary T. Blore, program executive officer of the Integrated Deepwater System, noted several parallels between the Coast Guard of nearly 100 years ago with today's Coast Guard and the Deepwater program. "Beyond matters of personnel, administration,

National Security Cutter

Characteristics:

Number Planned: 8

Length: 418 ft.

Displacement: 4,300 LT

Speed: 28 knots

Endurance: 60 days

Range 12,000 nautical miles

Propulsion: Combined Diesel and Gas Turbine (CODAG - 2 Diesels, 1 Gas Turbine)

Aircraft: (2) Multi-mission helicopters (MCHs) or (4) Vertical Takeoff and Landing Unmanned Aerial Vehicles (VUAVs), or (1) MCH and (2) VUAVs

Boats: (1) Long-Range Interceptor (LRI) and (1) Short-Range Prosecutor (SRP)
SLQ-32 Electronic Warfare System

Armament: 57mm gun and Gunfire Control System, Close-In Weapons System (CIWS), SRBOC/NULKA countermeasures, chaff/rapid decoy launcher

and training," he said, "Commodore Bertholf guided the transition of the Coast Guard's inventory of cutters and boats to a wartime footing."

Blore also noted that Bertholf advocated closer cooperation between the Coast Guard and the U.S. Navy – presaging today's National Fleet Policy – and later paved the way for the creation of Coast Guard aviation.

USCGC BERTHOLF (WMSL 750) being positioned to her mooring by tug after she was launched, on Sept. 29, 2006

"I am confident that our mission and vision for the Deepwater Program would resonate strongly with Commodore Bertholf were he with us here today," Blore said. "We again face a time of great danger to our nation's security; we again are acquiring and delivering more capable and interoperable cutters, aircraft, and systems; we again are called upon to assist Coast Guard operational forces in executing their challenging missions."

Shipyard Workers Praised

Blore also recognized the important roles played by Congress and the Department of Homeland Security in translating the Deepwater Program from vision to reality. "Even the best-laid plans to rebuild the Coast Guard would come to naught without the tremendous support we have received both from our Service secretary and from our elected representatives," he said.

"Speaking for the men and women of our Service who are on patrol today – and those who will follow during the years ahead – I express our deep appreciation to our Department and our Congress for providing the critical funding necessary to sustain the Deepwater Program in the face of many competing priorities."

Taylor, Chertoff, and other speakers singled out Northrop Grumman's shipyard workers for their resilience and commitment in the wake of Hurricane Katrina last year. "When these shipbuilders leave every day," said Taylor, "they are tired and dirty and, I can assure you, they have given the citizens of this nation and Northrop Grumman a full day's work for what they got paid that day."

"I want to thank everyone at our shipyard and most particularly the fitters and welders and the fine job that they've done leading up to the christening of this vessel," Chertoff said. "It is often said that everybody is able to accomplish what they do only because we stand on the shoulders of giants. That is of course very true with respect to the accomplishment of building and christening this cutter."

Chertoff also emphasized the important role the *Bertholf* and other future national security cutters will play in the Coast Guard's multiple maritime missions. "This ship is very much a tangible symbol of our unwavering commitment as a Department to make the necessary investments in the Coast Guard and our other border forces to make sure that we can continue to keep this country strong.

"I can't predict what the next attack will be, and I cannot predict when the next hurricane will come, but I will tell you that, whenever a natural disaster or act of terror approaches, this ship and its crew – and the entire Coast Guard and Department of Homeland Security – will be there at the ready, at the ramparts to defend and protect the citizens of this region and this country," said Chertoff.

More than 70 crewmembers have reported to the *Bertholf* to date, with the balance of the crew scheduled to arrive next spring. All are now undergoing extensive training at various locations. Late next spring, *Bertholf's* crew will move to Pascagoula for additional shore training at Northrop Grumman's facilities and aboard the ship. This will lead to builders and acceptance trials and, finally, formal delivery of *Bertholf* to the Coast Guard.

"It's a great honor to be in command of the crew that will bring this ship to life and into commission," Capt. Patrick Stadt, the cutter's prospective commanding officer, said. "The crew is extremely excited about taking delivery next year, and they are fully entrenched in training for the new systems and operation of *Bertholf*. In less than a year from now, we will have the most capable Deepwater asset ever built added to our inventory and ready to answer all bells."

Capt. Gordon I. Peterson, USN (Ret.), a senior technical director with General Dynamics Information Technology, supports the Integrated Deepwater System's program office at U.S. Coast Guard Headquarters in Washington, D.C. During his 30 years of active duty, Peterson served in numerous senior-level public affairs assignments, including duty as special assistant to the chairman of the Joint Chiefs of Staff. A 1968 graduate of the U.S. Naval Academy, he served in Vietnam as a Navy helicopter gunship pilot. Following retirement from the Navy he was senior editor of the Navy League's Sea Power magazine and its annual Almanac of Seapower.

THE INTELLIGENCE SUMMIT

Conference & Trade Show

IS COMING

March 4-7, 2007
St. Petersburg Hilton
St. Petersburg, Florida

THE INTERNATIONAL INTELLIGENCE SUMMIT℠ Conference and Trade Show is a forum to bring together for the first time the International Intelligence community from the free world and the emerging democracies to learn from each other and share critical knowledge in the common war against terrorism. The SUMMIT is the most prestigious world conference on international studies, intelligence policy, terrorism and homeland security. Visit our web site at www.IntelligenceSummit.org for more information and to register as an exhibitor or attendee.

OPPORTUNITIES FOR EXHIBITORS

★ Conference participants will include Federal, state, local and international professionals in business and industry, governments, and academia who are looking for the most advanced technologies to challenge the critical threats our country and the world are battling.
★ Show the innovations and advances your company has made in your field of expertise that will benefit participants involved in actions against terrorism and public safety.
★ Collect hundreds of quality sales leads to increase your market base and sales revenue while you save significantly on 'cost of sales' by bringing your market to you.
★ You will receive two complimentary full conference passes for all events, sessions and meals for each booth you purchase.

For more information on exhibiting, contact Jerry Koenig, Exposition Project Director at 770-977-1200 or E-mail: kingsdh@aol.com

OPPORTUNITIES FOR ATTENDEES

★ Presenters at the SUMMIT will include top leaders of the intelligence, espionage, counter-terrorism, and counter-intelligence agencies from the free world.
★ The SUMMIT will include International Sessions, Business Sessions, Technology Sessions, Counter-terrorism Sessions, and Homeland Security Sessions
★ Experts in regional/international studies, as well as law enforcement and terrorism specialists should attend this vital event.

For more information on attending, contact Adam Shaneson, Conference Co-chairman at 516-431-7415 or E-mail: Shaneson@IntelligenceSummit.org

Other event sponsors include:

KONICA MINOLTA

New Jersey, Florida, Missouri, Arizona, Virginia, and California

By Adam McLaughlin, State Homeland News

New Jersey Plans to Bolster School Security

New Jersey Governor Jon Corzine took direct aim last week at violence in the state's classrooms by announcing a multifaceted plan to tighten school security. The announced intent of the SAVE (Strategic Actions for Violence Elimination) program, he said, is to give school districts the tools they need to make their schools safer.

Included in the SAVE program are plans to update the state's school-lockdown guidelines, increase funding for the training of school police, and require New Jersey schools to sign agreements with local police departments formalizing their security plans. If the SAVE plan is approved by the state legislature, the schools also would be required to run periodic security drills.

Corzine said the stricter guidelines have become increasingly important in light of numerous incidents of school violence throughout the country that have occurred in recent weeks. There have been school shootings in a number of states – Vermont, North Carolina, Wisconsin, Colorado, and Pennsylvania, for example – that not only have raised public awareness about the problem but also have validated the need to place greater responsibility for emergency preparedness in the state's classrooms as well. "If we do not take this issue seriously, I do not know what other priority we should have," Corzine said.

Richard Canas, director of the New Jersey Office of Homeland Security, said the goal of the plan is to help teachers and students spend as much time as possible focusing on their studies and other school-related activities – but without sacrificing the need for security as well. "Clearly, as a state, we are ahead … [in] keeping our children safe in schools, but we have gaps we need to fill," Canas said.

Another component of the SAVE program calls for the development of a school security website for parents and school personnel that will be hosted by the state's Department of Education. Also being planned is a security program developed specifically for school-bus drivers. In addition, the state teachers union has partnered with the State Office of Homeland Security to design a pilot program focusing on situational awareness.

Florida Receives FEMA Help in Disaster Planning

Calling Florida the state ''most vulnerable'' to hurricanes, federal emergency managers announced a decision last week to allocate approximately $4 million to help state officials develop plans to cope with two possible nightmare scenarios: a failure of the aging levee around Lake Okeechobee; and a Category 5 hurricane striking the city of Miami.

The funds allocated will pay for: (a) the development of precise, laser-based flood maps around the lake; and (b) the hiring of disaster-planning experts to help develop the consequence-management strategies needed to deal with the chaotic process of recovery following the onslaught of a hurricane strike on the state's largest city. ''Clearly, we know how to move people and get them out of harm's way, but what do we do with them afterward?'' asked David Paulison, director of the Federal Emergency Management Agency (FEMA), during a news conference at the National Hurricane Center in West Miami-Dade County.

Craig Fugate, director of Florida's emergency management division, praised the agency for responding to the state's requests for planning help. He pointed out that Florida Governor Jeb Bush had asked for federal assistance in that area after state-hired engineers described the Herbert Hoover Dike as a "grave and imminent danger.''

In the almost six months since that report was issued, the U.S. Army Corps of Engineers has defended the integrity of the dike, but also scrapped an original repair plan and agreed to study ways to reduce water levels in Lake Okeechobee to lessen the risk of a breach.

The new flood-mapping capability will add another much-needed level of protection, Fugate said, by pinpointing the areas likely to be in the most serious danger. The high-tech airplane mapping system, known as Light Detection and Ranging, or LiDar, is considered to be accurate within a foot of elevation, and therefore will provide far more precise readings than were possible with the ground-based surveys carried out a decade ago.

The Lake Okeechobee mapping plan is scheduled to be completed before the start of the next hurricane season, Paulison said; the Miami earthquake-recovery plan, though, would take two additional years, and perhaps longer.

Missouri Homeland Security Team Enhances School Safety

Missouri Governor Matt Blunt has signed an executive order adding an education representative to the state's Regional Homeland Security Oversight Committees (RHSOCs) and calling on Missouri educators to get more deeply involved in school safety planning.

The executive order, issued in late October, introduces a new approach to homeland security in Missouri that for the first time officially includes the state's education community. Blunt also has directed all of the state's RHSOCs to add elementary and secondary education as another category requiring full membership representation, thus ensuring that the state's schools are actively engaged in homeland-security planning.

In addition, he wrote personally to Missouri school officials encouraging them to implement a number of recommendations designed to enhance school safety. More specifically, he encouraged the school officials to: (a) Create a comprehensive school safety plan and review that plan on a regular basis; (b) Include all levels of public safety personnel, as well as all sectors of school personnel (instructional, administrative, and functional staff), in the planning process; (c) Continue to communicate with stakeholders on the need for improved safety in schools – parents, students, staff, and administration and public-safety personnel all should be in constant communication, Blunt said, on such matters as new safety developments and incident-prevention methods; (d) Provide training on school safety procedures, at least annually, for

personnel in all sectors; and (e) Help students feel more connected to their schools – by, among other things, providing character education as an important way of keeping students engaged as part of the school community.

"We all play a role to ensure our schools, and more importantly our children, are safe," Blunt said. "Enhancing school safety requires ongoing cooperation among schools, law-enforcement [agencies and personnel], communities, and first responders."

Arizona

Border Hosts High-Tech Security Minuteman Project

The Minuteman Civil Defense Corps (MCDC) started construction in late October of a nearly one-mile-long fence on an Arizona ranch along the U.S.-Mexico border. The MCDC started building the first of what Corps spokesmen say will be many (the specific number was not provided) state-of-the-art border-protection systems using donated technology originally developed for use along the Demilitarized Zone between North Korea and South Korea – but never before, so far as is known, used in the United States itself.

The system – which will create a dual barrier across the southern line of a 372-acre cattle ranch near Naco, Ariz. – is designed to serve as an early detection and warning system to help the U.S. Border Patrol in its fight against illegal immigration. "We are trying to demonstrate that you can have an extremely effective, multi-tiered approach to the problem of illegal immigrants coming across the border," said Peter Kunz, project manager for the Minuteman fence system, "and we are trying to show that you can combine technology with just a good old-fashioned tall fence,"

A chain-link fence covered in fiber-optic netting will detect unwanted intruders, according to the MCDC, while a 14-foot "Israeli-style" no-climb steel fence 20-30 feet behind it will bar not only people but also larger animals – cattle, for example – from crossing into the United States. Three cameras placed along the no-climb fence, Kunz said, will use facial-recognition software to identify possible intruders.

"All of this will be hooked into the Internet, which will be able to monitor all of the cameras from the Internet," said Connie Hair, MCDC spokesperson. "It will even email you and call you on your cell phone to tell you that there has been an intrusion or an attempted intrusion."

When the system is operational, the MCDC said, "Cyber Minutemen" will be able to log onto the Border Fence Project website to telepatrol the border-front property and other protected areas. "Ultimately," Kunz said, "we are looking to do about 70 miles of total fencing just in Arizona. And then we … [will be] talking to folks in California, New Mexico, and Texas as well."

Virginia

University Partners With DHS On Agro-Terrorism Defense

Virginia Tech has joined several other universities to develop a program funded by the Department of Homeland Security (DHS) to train small agricultural communities to detect areas of food supply and transportation that may be vulnerable to terrorist attacks.

The purpose of the program – officially called the Agricultural Vulnerability Assessment Training Program – is to develop classroom-like training sessions that will give farmers and producers the tools they need to detect areas of vulnerability in food production, packaging, and transportation, and also train them in ways to restore economic order in case of an attack.

"A lot of people do not realize that veterinary medicine plays a critical role in national security," said Jeffrey Douglas, college communications manager for University Relations. "The dangers of a terrorist entity contaminating our food supplies are real and the economic consequences of shutting down a food production network can be devastating.

"Target hardening, as we call it," he continued, "will make our food supplies a more difficult target to attack. We take agricultural communities through the process of making decisions of how to prioritize their efforts. Fixing potential problems costs money, so we show them what to address first."

The program is currently in its second stage of development. The training sessions, designed as modules, have been submitted to several federal agencies for approval. After approval is granted, three pilot sessions will be conducted, starting in the fall, through which problems will be assessed and solutions provided. Officials said the program will be available at more than 30 different locations throughout the United States.

California

Port Receives Mobile Radiation Portal Monitors

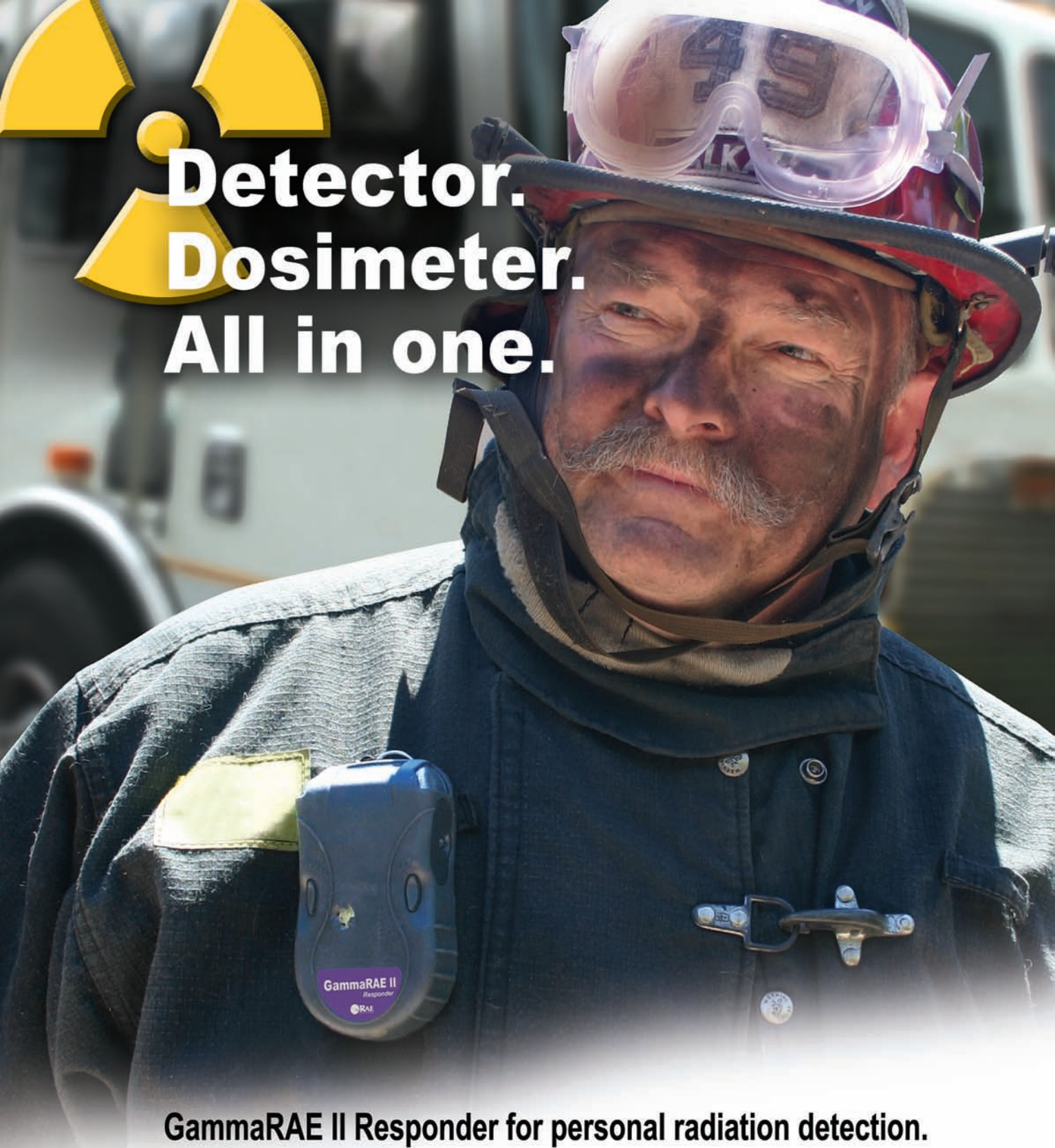
The LA/Long Beach seaport, the nation's busiest, was given a preview in late November of how the SAFE Port (Security and Accountability For Every Port) Act recently signed into law by President Bush would improve security, spotlighting new and highly sophisticated mobile radiation-portal monitors, an integral component of the U.S. Customs and Border Protection's layered-defense system against radiological weapons.

"Customs and Border Protection [CBP] has worked hand-in-hand with state and local governments to ensure that the nation's busiest seaport is also the safest," said CBP Commissioner W. Ralph Basham. "Nearly all containers currently exiting this port via truck and rail are screened for nuclear and radiological materials, and by January we will be at 100 percent. The mobile radiation-portal monitors provide CBP with a tactical edge to conduct screening operations, as they can easily be deployed anywhere, including supporting state and local [governments] … to secure a major event."

The SAFE Port Act, which the president signed into law on 13 October, calls for modernized inspection technologies, codifies two CBP global port-security programs, and instructs the Department of Homeland Security to make plans for an expedited resumption of trade should an attack force a port to close down and/or severely limit its normal operations.

Among the various sophisticated equipment systems used by CBP in its layered-enforcement strategy at LA/Long Beach, in addition to the radiation portals, are large-scale, non-intrusive X-ray units that can scan an entire sea container within two to three minutes, and personal radiation-detection devices that are provided for the protection of all front-line security personnel.

Adam McLaughlin is Preparedness Manager of Training and Exercises, Operations, and Emergency Management for the Port Authority of N.Y. & N.J. He develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs.



GammaRAE II Responder for personal radiation detection.

It has the rapid response of a detector and the accurate dose measurement of a dosimeter. Its dual detectors allow it to quickly cover a full range of gamma radiation fields while offering dosimeter functionality. The intrinsically safe, immersible design ensures reliable, safe operation in the most hazardous, rugged and wet environments and easy decontamination.

www.raesystems.com/info

Protection Through Detection

RAE SYSTEMS