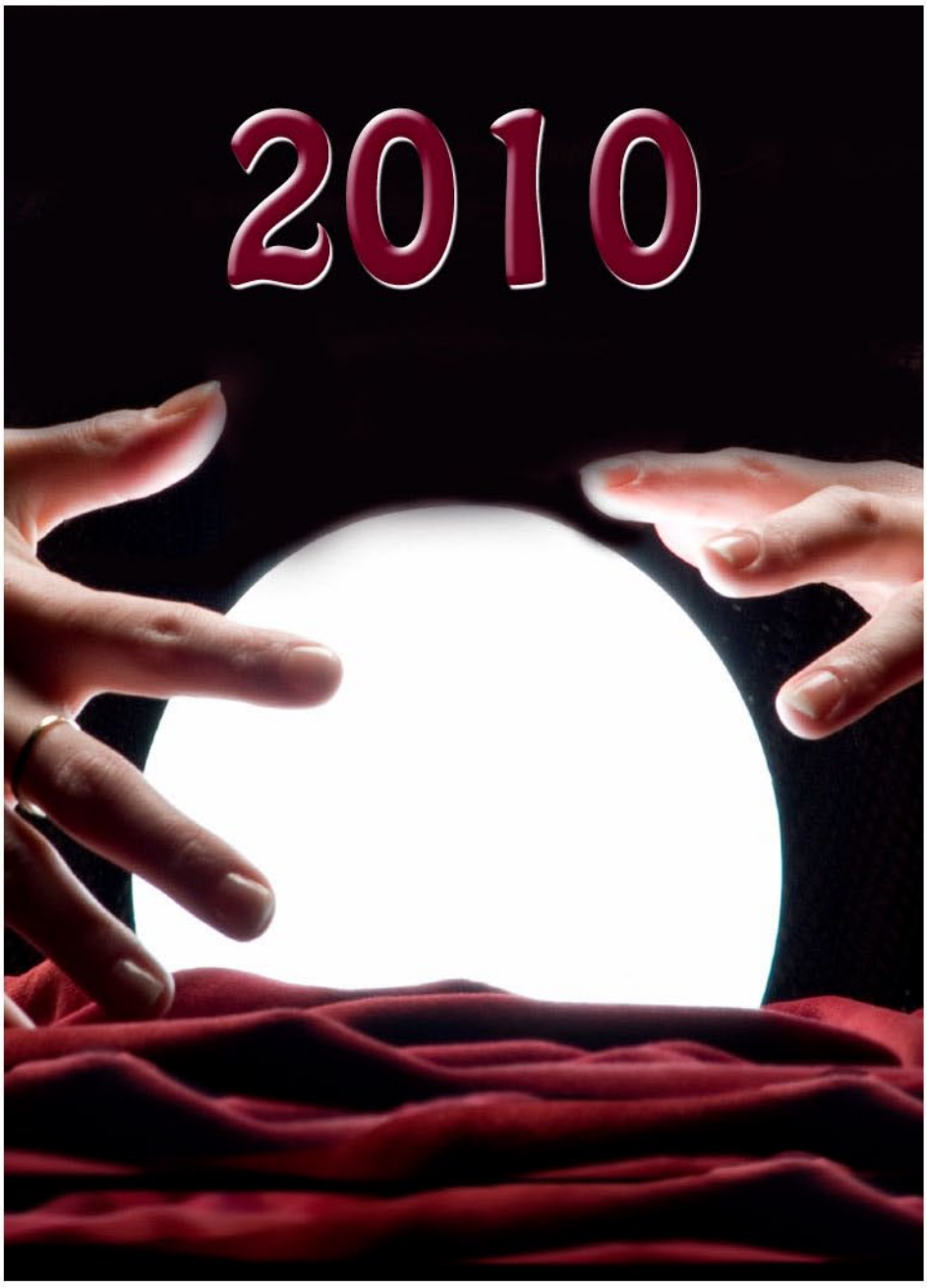
domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 5 Issue 12, December 2009

FORECAST



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

Now You Can Be with the New RAZOR™ EX

RAZOR EX

Field Portable BioHazard Detection System

Less than 1% error rate

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

Used by Military, Hazmat, and First Responders

The 10™ Target Screen Kit:

Anthrax	*E. coli* O157	*Salmonella*
Brucella spp.	Tularemia	Smallpox
Botulism	Ricin	Plague
Coxiella		

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

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

Idaho Technology Inc.

Innovative solutions for pathogen identification and DNA research

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

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

Staff

Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Dan Brethauer
Account Executive
dbrethauer@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

Editor's Notes

By James D. Hessman, Editor in Chief

The first month of 2009 was, for most Americans, a period of both hope and trepidation. A charismatic but untested new president would soon be sworn in. But the U.S. economy was still trying to recover from its steepest decline in 25 years, and there were numerous foreign-policy challenges facing the incoming administration – particularly in Iraq, Iran, and Afghanistan.

Not quite 12 months later, the economy is recovering – slightly, and very slowly. Iraq is still suffering through a prolonged period of violent peace, the war in Afghanistan has not gone as well as expected, and Iran's nuclear enrichment program, and its anti-U.S. rhetoric, continues apace.

These and other dangers and difficulties are partially offset by continued progress in most but not quite all aspects of the multifaceted U.S. homeland-security/domestic-preparedness mosaic. The specific details are spelled out in this ***"2010 Forecast"*** issue of *DPJ*, which leads off with a bullish update from Kay Goss on the numerous accomplishments of the nation's emergency-management community. Mark Merritt provides an insider's look at how Iowa coped with the drenching rains that almost changed that state into an inland sea. Corey Ranslem discusses the many ways that the U.S. Coast Guard, working in close cooperation with the private sector, is making the nation safer both on the waterfront and throughout its entire coastal domain. And Steven Grainer explores the step-by-step progress required, and being achieved, to transform a not yet cohesive group of AHIMT (All-Hazards Incident Management Team) trainees into a superbly trained "Super Bowl" team capable of meeting all challenges and defeating all foes.

Can all this progress be measured? Yes, it can – provided that valid measurement criteria are established and the correct tools are used, as Timothy Beres points out in his insightful essay on the measurement of preparedness capabilities. Complementing Beres's position are articles by: (a) Theodore Tully (on the need for continuing emphasis on emergency preparedness by U.S. healthcare facilities); (b) Dennis Schrader (who presents a cogent argument for a closer philosophical relationship between the nation's disaster-recovery and resilience policies; and (c) Craig DeAtley, who correctly points out that the post-9/11 upgrade in hospital preparedness will probably continue next year – but, because of the nation's current economic difficulties, at a slower pace.

Also included in this month's printable issue are: (1) a well-articulated report, by Joseph Cahill, on the steady improvement in U.S. ambulance-team capabilities – which, he points out, can be truly effective only when the correct "destination decisions" are made; and (2) three "Breaking News" articles. The first, by Bradley Blakeman, is a reprint of his outraged, but immensely interesting, commentary on the White House "gate-crashing" incident. The second is by Joseph Trindal, who discusses the horrifying increase in attacks against policemen in recent years, and offers seven USMC-tested "principles" that could change the odds in favor of the police. The third article, by "JL" Smither, reports on the communications upgrades that are helping Chicago and Los Angeles deal more quickly, and more effectively, with the crime breakers in those two great American cities.

Read, ponder, learn, and enjoy – and have a wonderful holiday season.

About the Cover: Those who use a crystal ball to predict the future – more specifically, the future of a well-paying customer – wrap their predictions, prophecies, and prognostications around a thick fog of rhetoric, toss in a few sprinkles of star dust, and casually suggest that a handome tip is the best guarantee of future happiness. DPJ prefers to play it straight – by assembling a diverse panel of experts, all of them with years of professional (usually hands-on) experience, to offer their well-reasoned views of what is likely to happen next year in their own specialized fields – and, of sometimes greater importance, what is not likely to happen. (Photo from istockphoto.com)

IDENTIFY CONTRABAND. SINGLE-HANDEDLY.

Introducing Fido® Verdict™, an affordable palm-size instrument for rapid identification of explosives, liquid threats and narcotics.

Used for screening containers, bags, bottles, vials and powders, Verdict™ provides military personnel, security agents and law enforcement officials with real-time results in the fight against improvised explosives and illegal drugs. Verdict uses well-established Raman spectroscopy to identify unknown materials quickly and efficiently, minimizing exposure to potentially dangerous chemicals.

For more information, or to arrange a demo, please contact:
T+ 1.866.458.ICXT(4298)
Email verdict@icxt.com

icx™ technologies

www.icxt.com

Contributors

First Responders
Glen Rudner
Fire/HazMat

Steven Grainer
Fire/HazMat

Rob Schnepp
Fire/HazMat

Joseph Cahill
EMS

Kay Goss
Emergency Management

Joseph Watson
Law Enforcement

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Medical Support
Theodore (Ted) Tully
Health Systems

Adam Montella
Health Systems

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Updates
Adam McLaughlin
State Homeland News

Viewpoint
Neil Livingstone
ExecutiveAction

Dennis Schrader
DRS International LLC

Funding & Regulations
Diana Hopkins
Standards

Borders & Ports
Corey Ranslem
Coast Guard

Degrees of Progress

Emergency Management: Today & Tomorrow

By Kay C. Goss, Emergency Management

Although emergency management, as a profession, has been around since its civil-defense origins more than fifty years ago, this is a particularly exciting time of rapid change for the profession of emergency-management in many ways, and on almost every front.

At the same time, the Federal Emergency Management Agency (FEMA), its lead agency, is growing stronger every day under the leadership of FEMA Administrator Craig Fugate and William L. Carwile III, assistant administrator for disaster operations. The principles, mission, vision, and doctrine of emergency management are being developed, defined, and revised, with special focus on planning, textbooks, training courses, and college courses. Of even greater importance is the improved and continuing collaboration between and among local, tribal, state, federal, private, and non-profit partners, led by FEMA's Emergency Management Institute and its Disaster Operations Directorate, with full participation from practitioner stakeholders, academic institutions, and interagency partners.

Standards, although voluntary, also are increasing in importance, acceptance, and application. As of late November, 21 states and three local governments had been accredited by the Emergency Management Accreditation Program (EMAP). FEMA funded two rounds of the accreditation evaluations for all states – one in 2004, the other one this year. Previously (in 1997 and 2000), the agency had asked states to conduct their own self-evaluations through the Capability for Readiness process.

EMAP built upon that experience, and 24 jurisdictions are now accredited: Alabama, Arizona, Colorado, Florida, Georgia, Illinois, Louisiana, Maryland, Massachusetts, Missouri, Montana, New Mexico, New York, North Carolina, North Dakota, Ohio, Pennsylvania, South Carolina, Tennessee, Utah, and Virginia, as well as Jacksonville, Florida, East Baton Rouge, Louisiana, and San Diego County, California.

Four other jurisdictions – Arkansas, Iowa, Nebraska, and the District of Columbia – are listed as "Conditionally Accredited" and have nine months to make the final upward adjustments needed before a second review checks them for full accreditation. Eventually, most if not all state as well as numerous local, regional, and campus emergency-management programs will apply for and receive similar accreditation. Meanwhile, increasing numbers of private and nonprofit agencies and organizations will go through the National Fire Protection Association's NFPA 1600 process. Another sign of progress is that EMAP established a Private Sector Committee several years ago.

Several Steps Forward and a Global Outreach

DHS took another step forward last month by adopting NFPA 1600 as a recommended voluntary standard for the private sector. The NFPA 1600 standard was launched in

1991 and became the first on the emergency-management and business-continuity fronts. (Canada also has signed an NFPA 1600 arrangement, and intends to apply similar standards in that country.)

Standards bodies are becoming increasingly global in their outreach and partnership building. There is increasing interest, moreover, in applying the EMAP guidelines not only to states, counties, cities, tribes, and regions but also to other public-sector entities, including colleges and universities. The International Association of Emergency Managers (IAEM) and the National Emergency Management Association (NEMA) are the lead organizations in this effort, and both are growing rapidly in numbers and in their influence with FEMA, the Congress, the White House, governors, state legislators, mayors, and county executives, as well as in the quality of services they provide to members. (For additional information about IAEM click on www.iaem.com; for more about NEMA, click on www.nema.org.)

The principles, mission, vision, and doctrine of emergency management are being developed, defined, and revised, with special focus on planning, textbooks, training courses, and college courses

There has been significant progress in other areas in recent months. The ASTM (American Standards for Training and Materials), for example, has a School Emergency Preparedness Working Group collaborating with various stakeholder groups in developing guidelines related to school safety and security. And the Commonwealth of Virginia's Emergency Management Agency and its counterparts in many other jurisdictions are encouraging inclusion of school emergency-preparedness instruction in the K-12 curricula.

Credentialing also is taking hold at both the state and local as well as national levels. Again, FEMA is leading the way with the credentialing of its own Disaster Reserve Workforce and its regular Disaster Workforce. The U.S. Department of Homeland Security (DHS) has funded several local credentialing projects such as the First Responder Authentication Credential (FRAC) program in Northern Virginia, as well as one in Colorado. Meanwhile, the American National Standards Institute (ANSI) is working closely with the private and nonprofit sectors on the credentialing of their own emergency-response teams.

Progress in Other Areas; Facebook and Best Practices

Advanced technology is taking emergency management to new heights of research, education, and analysis – and, of greater importance, to effective action. Interoperability has become easier, with progress dependent only upon building trustworthy partnerships, receiving adequate funding, and providing appropriate training. Social media provides common operating pictures and situational awareness, including Facebook – which less than three years ago, during the horrific massacre of Virginia Tech students and professors, helped other students keep in touch with one another to find out who had escaped and were safe, or were perhaps injured, as well as who had been killed. Twitter, YouTube, Emicus.com, and other here-and-now communications tools also are changing both the emergency-management profession and the leading agencies – at all levels of government, as well as in the private and nonprofit sectors, including IAEM and NEMA.

One "best practice" example is the Virginia Department of Emergency Management's (VDEM) Virginia Interoperability Picture for Emergency Response – also known as VIPER, a particularly helpful tool that not only gives the Virginia Emergency Operations Center (VEOC) staff the ability to visually assess statewide emergency-management operations in real time but also automatically offers users instant access to essential local information through traditional Geographic Information Systems (GIS) layers. For example, if a locality is coping with a rapidly escalating traffic incident, VIPER will provide information about nearby hospitals; in the case of a hazardous-materials spill, VIPER will offer data about area schools; during a flood, VIPER will alert users to low-lying areas that might be affected.

According to VDEM, VIPER monitors environmental sensors and gathers data not only from VDEM's own crisis-management system but also from such external systems and entities as Computer Aided Dispatch, the National Weather Service, and the Integrated Flood Observation and Warning System. VIPER then performs an analysis of all of the

information currently available and alerts the VEOC staff about the potential impact on critical infrastructure.

The VIPER Revolution: Degrees of Progress

This ability to evaluate how incidents visually relate to each other – combined with point-and-click access to essential local data – greatly speeds VDEM's coordination of response and recovery efforts at the state and local levels. VIPER has already aided the state's response not only during Tropical Storm Hanna earlier this year but also during the 2008 presidential election and the 2009 presidential inauguration activities.

In the future, VIPER's data will be available to other state and local government partners through data links that can operate with any GIS system. The data links will use widely accepted data standards, such as GeoRSS, .xml, and .kml, to promote a multi-platform model of GIS information sharing. VDEM developed this interoperable system so that agencies and localities will be able to share information with the VEOC regardless of the GIS systems they use, maximizing existing investments and minimizing future costs.

The goal of the FEMA Higher Education Program – launched in 1994* and operated since that time by Dr. Wayne Blanchard (the founding director of the program, and a senior FEMA career employee) – is to have an emergency-management degree program in every state. The number of such programs has increased from two degree programs 15 years ago to 173 now – with another 100 higher-education institutions considering and/or already in the process of developing and designing similar programs. During the same time frame, over 280 degree and/or certificate programs in homeland security/defense have been developed, and another 100 institutions are considering establishment of such programs.

The number of emergency-management programs will undoubtedly continue to grow exponentially for the foreseeable future. This year, the 11th annual FEMA Higher Education conference – held during the first week of June at the FEMA Emergency Management Institute (EMI) in Emmitsburg, Md. – attracted approximately 400 attendees, from seven countries, and continues to grow larger every year. Very soon, there will be an emergency-management course on almost every U.S. campus; and almost every textbook on public administration is likely to include a separate chapter devoted to emergency management.

Increasing numbers of these degree programs are available, at least partially, online – and FEMA's Emergency Management Institute offers increasing numbers (now about 200) of independent study courses, also online, with printable certificates available upon passage of the required examination for each. Increasingly, these same courses are available to international emergency managers. Completion of this education and training qualifies the recipient in the achievement of the IAEM's Certified Emergency Manager® (CEM) designation. There are now over 700 CEM®s worldwide. (Certification indicates that the recipient is a college graduate with 100 hours of emergency-management and 100 hours of general management training, plus six major public-service contributions to the profession beyond one's own job, as well as an examination and an essay.)

With the increasing number of academic programs now available, there is a parallel need for accreditation processes to evaluate these programs on behalf of students, faculty, staff, the profession, and the general public. Accreditation programs are under development in both emergency-management and homeland security/defense – the Foundation for Higher Education Accreditation in Emergency Management for emergency-management degrees (www.ffhea.org) and the Homeland Security/Defense Education Consortium Association for homeland security/defense degrees.

Perhaps the crowning jewel of the preceding and other advances is that, during the last year, the U.S. Department of Labor began, for the first time, listing emergency management both as a profession and as a specialty.

**Kay M. Goss, author of the preceding article, played a key role in establishing FEMA's Higher Education Program.*

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

Destination Decisions: Back to the Future, Again and Again

By Joseph Cahill, EMS

The concept of specialty referral centers – i.e., hospitals that specialize in the treatment of particular types of illness or injury – started in the 1970s with trauma and burn centers. These hospitals have the specialized staff, equipment, and procedures needed to improve the chances for survival and future lives of the patients suffering from those particular illnesses or injuries.

In the years since the introduction of the trauma and burn centers, numerous other specialty-center programs have been established – to help stroke victims, for example, patients in need of cardiac care or suffering from venomous bites, and/or stricken by other life-threatening illnesses or injuries. In addition, many systems are in place to assemble the equipment and staff needed to treat specific classes of patients in response to the advance information received from an ambulance at the scene of an accident or during transportation to the hospital.

Transportation decisions, however, which often are used to determine which hospital a patient should be taken to, become more complicated as the hospitals themselves continue to specialize. Typically, an EMT (emergency medical technician) or paramedic makes the transportation decision based on his or her diagnostic evaluation of the illness or injury of the patient. Specific types of injuries frequently suggest that transportation to a trauma center is advisable – because of the concern about hidden internal injuries, for example – even in the absence of visible signs or symptoms of injury. Thanks to those well informed decisions, patients usually are given the most effective care available by hospitals that specialize in the specific illnesses or injuries indicated by the on-site and/or en route evaluations.

However, the transport of a patient from one hospital to another hospital better able to care for the patient costs both time and money; the transport of a critically injured patient to another hospital is particularly expensive, of course, but the transport of critically injured patients to the *wrong* hospital also costs lives.

Costs, Capabilities, & Added Complexities

As the current national discussion on controlling medical costs intensifies, the issue of how destination decisions are made becomes increasingly important in controlling both the cost of EMS evaluations and the long-term care provided to patients. Improving such decisions is contingent on improving the ability to determine the specialized services likely to be needed – and, therefore, transportation to the most appropriate facility. There are two components of this improvement: staff knowledge and training; and the equipment available. Clearly, any future advances in diagnostic equipment must be accompanied and/or immediately followed by additional knowledge and training not only in the mechanical workings of the equipment but also in the interpretation of the data it produces.

A good example to use for this discussion is blunt trauma to the abdomen – the type of injury frequently suffered in a car wreck. For many years, the decision to transport accident patients to a trauma center was based on a list of criteria derived from historical records and patient outcomes – a roll-over accident, for example, or an accident in which another passenger had died on the scene.

There are now a number of programs that use ultrasound technology, in the field, to diagnose vascular or abdominal injuries from trauma. An ultrasound system allows the EMS professional to peer deeper into the patient's vital systems and, by doing so, may be better able to determine if the patient needs immediate transportation to a trauma center or can be evaluated just as well at a community hospital. Future data studies will determine if the ultrasound devices improve the accuracy of the destination decision for trauma patients or are no more accurate than the decisions currently made by paramedics using a standard list of criteria and their own unaided senses.

Patient outcomes from more effective transport decisions also can be affected, of course, by such seemingly insignificant "reminder" aids as a check-off list or decision tree – or as complex as advanced cardiograms, which 20 years ago were cutting-edge technology but are now standard care on a paramedic unit. In short, the future of EMS should and undoubtedly will be characterized by more knowledgeable and better trained staff, equipped with even better and more sophisticated systems and technologies that in combination will ensure that patients can be taken directly to a facility that provides the specific care they need.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem.

WE REDUCED THE SIZE. NOT THE PROTECTION.

AVON PROTECTION

1 888 AVON 440

www.avon-protection.com

An Opportunity Beckons

Converging Disaster Recovery and Infrastructure Resilience

By Dennis R. Schrader, Building Protection

Recovery from a catastrophic disaster relies on three key factors – the restoration of housing, infrastructure resilience, and business continuity. In an August 2009 Domestic Preparedness Journal article, National Disaster Recovery Doctrine was identified as a major gap in the nation's large-scale disaster-recovery plans.

In 2010, there will be an opportunity to ratify the convergence of disaster recovery and infrastructure resilience as the key step needed to build an effective national disaster-recovery framework.

The White House, the Departments of Homeland Security (DHS) and Housing and Urban Development (HUD), and the Federal Emergency Management Agency (FEMA) have organized an ambitious and very encouraging public process that next year may well produce a consensus doctrine that addresses defined roles and responsibilities as well as credible measures of success. The White House and DHS/FEMA expect that a draft of the National Disaster Recovery Framework will be available early in 2010 – in time, therefore, for a publication date of 1 June 2010.

The White House, DHS, HUD, and the Federal Emergency Management Agency have organized an ambitious and encouraging public process that next year may well produce a consensus doctrine that addresses defined roles and responsibilities as well as credible measures of success

Initiatives & Updates, Reports & Reserves

Several public and private-sector initiatives addressing infrastructure resilience that have emerged over the past 12 months can contribute significantly to the framework doctrine. The American Society of Civil Engineers (ASCE) published its updated "Infrastructure Report Card" in March 2009, for example; the Report Card, and the ASCE's new "Guiding Principles for the Nation's Critical Infrastructure," released in July 2009, address such major topics as risk, integrated systems, decision-making processes, and life-cycle adaptability.

The National Infrastructure Advisory Committee (NIAC) also has issued reports – one in July 2009, and another in September – on Critical Infrastructure Resilience and Disasters; and TISP (The Infrastructure Security Partnership) previously – i.e., in 2006 – published a Regional Disaster Resilience Guide.

The U.S. Chamber of Commerce also released a major report, in June 2009, that identifies 10 policies that states should adopt, the Chamber said, to help them recover from a disaster, more quickly as well as more effectively. Those policies include: (a) ensuring the availability of adequate capital for rebuilding and recovery; and (b) emphasizing the repair and rebuilding of infrastructure in affected areas.

How capital reserves are created is the heart of the recovery planning and resilience challenge. ProtectingAmerica.org, an influential private-sector organization, started a hotly debated initiative to create a national non-profit fund to help support state disaster-recovery funding efforts. Other organizations such as the Heritage Foundation see the initiative as opening the door to another National Flood Insurance Program (NFIP), and advocate instead that a private-sector insurance solution be sought. Complicating the situation even more is that the Terrorism Risk Insurance Program Reauthorization Act, which extends the Terrorism Risk Insurance Act (TRIA) through the end of December 2014, was originally – i.e., in 2002 – intended to be a short-term measure that would provide the insurance industry an opportunity to develop its own private-sector solutions for terrorism coverage.

Final Success: The Essential Prerequisites

Whatever else happens, the individual states must reassert their own responsibility for recovery and then develop policies that empower the private sector to help them. And state governors must personally take charge of recovery and pre-incident recovery planning, taking special care to ensure that their own states have in place an effective and affordable State Disaster Housing Plan.

The FEMA Joint Field Office (JFO)-Standard Operating Procedure (SOP) also must be rewritten. In its present form it does not support major disaster recovery effectively. Pre-incident planning for parallel response and recovery activities is particularly needed. In addition, the infrastructure recovery has to be resilience-based, and engineers have to be integrated into the state plans. The integration of private-sector resilience also should be written into the JFO-SOP as a pre-planned activity. Finally, the groundwork for the update should be spelled out in the National Disaster Recovery Framework.

DHS and FEMA have under them several offices that should collaborate to integrate the infrastructure resilience effort into the framework. Those offices include, but are not limited to, the Office of Infrastructure Protection (OIP), the National Preparedness Directorate (NPD), the Mitigation Directorate, and the Science and Technology (S&T) Directorate.

Of course, the Obama administration itself also must recognize that gaining consensus on such a complex plan, particularly while working under a very tight timeline, might well require expending some of its own political capital – but the very large gains that result would undoubtedly outweigh the rather reasonable costs required.

Recovery stakeholders, specifically including private-sector corporations, that want to get involved still have time to respond to 16 probing questions on the group's website (www.DisasterRecoveryWorkingGroup.gov) through the end of December 2009.

The opportunity to converge recovery and infrastructure resilience will make the Disaster Recovery Framework a much stronger doctrine. But completion of an effective, as well as *cost*-effective, doctrine will be possible in 2010 only if leaders fully embrace the need for infrastructure resilience and make the private sector an indispensable element of recovery planning.

Captain Dennis R. Schrader, USNR (Ret.), is president of DRS International, LLC, and former deputy administrator of the Federal Emergency Management Administration's National Preparedness Directorate. Prior to assuming his NPD post he served as the State of Maryland's first director of homeland security, and before that served for 16 years in various leadership posts at the University of Maryland Medical System Corporation.

2010: Will It Be "The Year of the IMT"?

By Steven Grainer, Fire/HazMat

In August 2009, the Department of Homeland Security (DHS) initiated its long-awaited series of Train-the-Trainer programs to develop leaders for the Command and General Staff positions in the federal government's Incident Command System (ICS). With this expansion of ICS training come a number of important decisions and commitments that must be addressed in the next several months.

Since 2004, U.S. emergency-response personnel and organizations have been striving to complete the so-called "NIMS-prescribed" ICS training in order to ensure that they qualify as being "NIMS-compliant" – i.e., that they adhere to the guidelines postulated in the National Incident Command System. Extensive efforts have been undertaken to complete training in the ICS "core" programs (ICS-100 through ICS 400). At least part of the motive for completing the ICS training as soon as possible is to ensure ongoing eligibility for federal funding through the DHS grant programs. For that reason the vigorous efforts expended have sometimes been referred to as "training for compliance" rather than training for competence.

Nonetheless, the coming year may prove to be a true benchmark of sorts for measuring the evolution of the NIMS guidelines. With additional and more advanced training becoming available it seems likely that new challenges also may surface. There already is an acknowledged need to expand the national capacity to provide better incident-command capabilities to manage the spectrum of possible emergencies that may occur. To meet that challenge the DHS has initiated an aggressive effort to develop highly capable All-Hazards Incident Management Teams (AHIMTs). Thanks to the availability of the ICS position-specific training courses, cities, states, regions, and numerous organizations and agencies must now determine the extent to which they need – and will make a commitment to establishing – an AHIMT.

Building Blocks, Commitment, And a Long-Range Plan

The ICS position-specific training already underway would be an integral building block in the process. The position-specific programs include, but are not limited to, training for such positions as incident commander, safety officer, public information officer, liaison officer, and the chiefs of the AHIMT planning, logistics, finance/administration, and operations sections.

The training of quality individuals to perform well in all of those (and other) positions is an important and necessary first step – but no more than that. In order for an AHIMT to be formed, and to carry out the responsibilities it will be assigned, several additional steps must be taken. To begin with, the individuals selected for the training, and their sponsoring departments and organizations, must make a long-term commitment not only to develop the capabilities needed but also to maintain those capabilities far into the future. The overall long-range plan must therefore include: (a) identifying individuals who will be assigned, or accepted, for AHIMT membership by judging them on their demonstrated capabilities; and (b) determining their probable availability for assignment or deployment.

The training of quality individuals to perform well in all positions is an important and necessary first step – but no more than that; in order for an AHIMT to be formed, and to carry out the responsibilities it will be assigned, several additional steps must be taken

The selection decisions that must be made should be based on the individual trainee's demonstrated competencies, regardless of his or her organizational affiliation and/or current rank. In simple terms, someone who already is the leader of an already existing unit of some type may not be best suited for a command or general-staff position in a local, regional, or state IMT – or, for that matter, may not be the best suited or most qualified for an AHIMT post at the same level. Moreover, if a current chief is expected to serve in an emergency operations center (EOC), he or she cannot also serve in the field with an IMT.

A Gridiron Analogy: All the Way to the Super Bowl

The process for developing a cohesive as well as fully qualified IMT can be compared to developing a winning football or baseball team. Almost all successful teams (no matter what sport is involved) follow much the same sequence, which includes, but is not limited to: (a) recruiting and screening the best candidates; (b) carrying out conditioning training; (c) filling position assignments, and practicing individual skills in those positions; and (d) escalating to whole-unit practices and real-time scrimmages – while also, throughout the entire process, making continuous assessments and adjustments while preparing for the opening game. For an AHIMT, of course, the "game" may be extremely dangerous, and the members of the team will seldom if ever know when it will start.

The first step in developing a strong team is to identify the players who will form the team. The players must demonstrate their individual knowledge and skills in order to make the roster. The individuals selected for the team start with conditioning – i.e., the position-specific training. Once that phase is completed, the members should develop experience through a process known as "shadowing" (which corresponds, more or less, to position practice). Shadowing gives the individual trainee the opportunity to practice the responsibilities of his/her position under the supervision, and with the guidance, of others who are already experienced in the duties assigned.

Verification of the development of individual candidates is accomplished through the process of completing what are called Position Task Books (PTBs). The PTBs verify that the performance competencies required for each IMT position have been satisfactorily demonstrated. However, the process is not complete when a trainee or even a group of trainees complete their PTBs. Two additional steps are necessary.

First, the team must develop depth for each position (the same way a football team would make sure that a backup quarterback is available to fill in if and when needed). After the decision is made to develop an AHIMT, therefore, several individuals, usually, must be trained and qualified in each command and general staff position in order to ensure that the team as a whole will be a fully functional unit if and when called upon.

Second, the team must practice together periodically. During those practices, the members' basic capabilities must be reinforced and identified, and any weaknesses discovered must be promptly corrected to prevent an adverse impact on overall team performance. Practical exercises, like football scrimmages, are needed to prepare the team for future real-life assignments. Here, the old sports adage that "A team plays like it practices" should serve as valuable guidance. Optimally, an IMT will practice together at least once a year, and those full-scale practices should include going through team transitions and shift changes. As often as possible, moreover, even in situations in which deployment of the IMT as a whole is not essential – the managing of a common emergency situation, for example – the entire IMT team might be activated and work together both to practice team activities and to enhance individual position capabilities.

An Unending Journey Toward an Always Distant Goal

The team has a number of other obligations that round out the picture. It must establish and exercise call-up procedures regularly, for example, to ensure that the individuals, and the team as a whole, can be mobilized and deployed in a timely manner. It also must conform rigorously to state and national AHIMT standards, particularly if it is likely to be made available for interstate deployments.

In short, the building of a fully qualified AHIMT is a long, difficult, and sometimes tedious process. But the task facing emergency planners does not stop there. Within the next several years it is reasonable to expect continued evolution of the already high standards required. As in many other aspects of life, each step in the process is never the last step, but simply the next one in what may well be an unending journey.

The year 2010 may therefore indeed be remembered as "the year of the IMT" – but the bigger challenge will be to ensure that in 2011, and the years beyond that, the NIMS and IMTs will still not only be around but will be more competent and more qualified as well.

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

Emergency Preparedness in Healthcare - 2010 and Beyond

By Theodore (Ted) Tully, Health Systems

In 2005, hurricanes were the "outside" factor that had the greatest and most lasting effect on emergency planning in healthcare. The 2005 devastation of the Gulf States by Hurricanes Rita and Katrina led to major changes, in 2006, in emergency planning for healthcare institutions throughout the country. The need for better evacuation planning spurred numerous multiple initiatives as hospitals and nursing homes used a considerable share of their scarce resources gearing up for future evacuations of uncertain magnitude and at uncertain times.

In much the same way, the international as well as national warnings earlier this year about the H1N1 (Swine Flu) virus had healthcare institutions re-tooling their emergency plans so they could respond to a potentially much greater health threat from this disease, predicted to hit during the flu season of 2009/2010. Today, on the eve of the second decade of the 21st century, emergency planners at hospital and healthcare institutions will have to decide what they must do to better prepare for this still looming disease, and other major threats, in 2010 and beyond.

The Next Wave: Other Infectious Diseases?

Perhaps the most obvious place that healthcare will be focused at the start of the next decade will be viruses such as H1N1.

The challenges of monitoring for index cases, using limited vaccine supplies as judiciously as possible, accelerating vaccine deliveries (including extra supplies for those segments of the population requiring multiple doses), studying the potential vaccine side effects, and preparing for an increase in emergency-room visits are issues that already have frustrated, and will continue to be major concerns of, emergency planners.

The newly emerging diseases will create planning initiatives for healthcare whether or not a virus becomes pandemic in size. A deadly infectious disease will continue to create challenges in the areas of supply chain issues, staffing problems (due to sick employees or staff family members), stockpile concerns (anti-viral medications, breathing masks and personal protective equipment, respirators and other equipment, and a host of other supplies), and, most important of all, the hospital surges that such diseases produce.

Emerging new diseases will most probably be the single most significant challenge facing the nation's healthcare community throughout the next decade. A recent review by the New York State Department of Health on how hospitals reacted to the H1N1 flu surge, both in New York City and on Long Island, revealed that the U.S. healthcare system is still not adequately prepared to deal with such events. Seasonal flu, the H1N1 virus, avian flu, and the newly emerging diseases will therefore continue to be major problems for healthcare planners to contend with for many years to come.

Surge Capacity, Hospital Security, and Related Factors

After two relatively quiet storm seasons, U.S. hospitals and nursing homes are still faced with the challenge of deciding: (a) when to shelter in place – i.e., decide *not* to evacuate anyone; (b) when to partially evacuate patients who are not at serious risk to be moved; and (c) when to actually start a full evacuation of their institutions. Future hurricanes will probably continue to be the major catalyst for such planning, but other hazards – fire, for example, or a loss of power, a terrorist incident, extreme wind damage, or similar disasters – can force healthcare leaders, ready or not, to make evacuation

FIRST RESPONDERS NEED TO BE PREPARED FOR ANYTHING...

SO DO OUR SUITS

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

USA **Tel:** +1 866 803 5956 (Toll Free)
Email: frontline@remploy.com

UK **Tel:** +44 (0)845 241 2990
Email: frontline@remploy.co.uk

www.remployfrontline.com

Remploy Frontline

SURVIVAL EVOLUTION

decisions without always having all of the facts needed to make the best possible choice.

Because of the now well documented 2005 experiences from Gulf Coast hospitals and nursing homes, however, more institutions have planned ahead of time for sudden evacuations than ever before in the nation's history. With predictions of climate change resulting in even more major storms, this hazard also will continue to be high on emergency-planning HVA (hazard and vulnerability analyses) lists.

Hospital surge caused by other than flu – the shooting massacres at Virginia Tech in 2007, for example, and last month in Fort Hood, Texas – will challenge planners for the next decade as well. Since the 2001 World Trade Center terrorist attacks, the United States has been relatively free of manmade mass-casualty incidents (MCIs) such as suicide bombings and CBRNE (chemical-biological-radiological-nuclear-explosives) incidents – accidental as well as intentional – but healthcare planners logically realize they may well see an increase in these over the next decade as well. Planners must therefore also focus on the fact that healthcare institutions themselves have become targets. If healthcare planning at every level of government does not include the protection of healthcare institutions themselves the nation could quickly lose many of these facilities and, without them, the ability to care for the most seriously sick and injured who have the greatest need for such care.

The challenges of monitoring for index cases, using limited vaccine supplies as judiciously as possible, accelerating deliveries, studying the potential side effects, and preparing for an increase in emergency-room visits are issues that will continue to be major concerns for emergency planners

Planning efforts to make hospitals both more secure and more adaptable to a major as well as unexpected patient surge are vital in the coming decade. However, because surge incidents are usually few and far between, it will be difficult for hospital administrators to continue to justify major financial commitments for what seem to be "unlikely" scenarios. In the area of surge and security for hospitals, such planning may actually decrease, therefore, unless new incidents refocus institutions on this specialized area of planning and funding.

A New Focus on Overall Healthcare Preparedness

Over the next decade healthcare institutions also must learn to use their preparedness resources in ways that can affect, and improve, daily operating efficiencies so that the costs involved can be justified by the institutional decision makers. Without sustainable funding, hospital emergency-preparedness capabilities will be much more difficult to maintain.

One possible way to at least partially resolve this problem would be through the concept of continuous institutional awareness or readiness. This type of a sustainable program can be used by institutions to react to day-to-day issues, not just emergencies. The routine availability of a hospital command center or HICS (Hospital Incident Command System) unit can help alleviate numerous problems ranging from a Friday night surge in the emergency department to the repair of a broken water pipe that floods an operating room to the rapid institutional reaction to a loss of computer/communication services.

In other words, if a hospital uses the emergency-management structure it has developed to react to disasters of an everyday nature, it can save money while increasing efficiency at the same time. This will or should be sufficient to justify a sustained budget for emergency management in the hospital setting. It also would permit hospitals to use the HICS training and infrastructure developed during the first decade of the 21st century to sustain and perhaps even improve hospital emergency planning during the century's second decade.

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

The Coast Guard Looks Ahead

A Closer Spirit of Cooperation With Local Agencies

By Corey Ranslem, Coast Guard

The Coast Guard faces numerous challenges in protecting the U.S. maritime domain, a task which has always been more difficult than it should be – mostly because the multi-mission service historically has been both under-manned and under-funded. In recent years, though, the funding stream has been both larger and more predictable, giving the service the opportunity to develop closer relationships, and working partnerships, with local and state law-enforcement and fire-rescue response agencies. The principal Coast Guard goal in forging those partnerships is to improve its own maritime domain awareness and response capabilities, with local stakeholders making greater contributions than ever before.

For operational purposes, the Coast Guard's local Captains of the Port (COTPs) are designated as the primary security coordinators, and on-scene coordinators for security-related incidents, within their respective zones. However, the Coast Guard also relies on the local agencies, more often than ever before, to handle the bulk of the primary response duties.

"The Coast Guard works with local and state agencies on a daily basis to reduce all hazards and threats to the homeland through the maritime sector," said Commander Brian Gove, the service's chief of prevention for Sector Miami. "We rely on the local and state agencies to be the eyes and ears on the water because there are numerous local agencies working within a single COTP Port Zone. In some cases the local agencies can respond to incidents much more quickly than the Coast Guard [is able to]."

A Three-Pronged Modernization & Upgrade Program

The Coast Guard is currently going through a long-term service-wide modernization program to improve its command,

control, communications, and response capabilities. More specifically, it is continuing to: (a) modernize its cutter and aircraft fleets through what is called the Deepwater program; (b) improve its communications and response capabilities through the Rescue 21 program; and (c) coordinate and expand its overall response capabilities through working relationships with such groups as the Area Maritime Security Committees (AMSCs).

"The Coast Guard, through the AMSCs, continues to work with local, state, federal, and industry stakeholders to develop risk-management plans … [as well as] business-resumption and continuity plans that … [reduce] maritime risk," Gove continues. The COTP chairs the local AMSC, but most members of the committee come from local, state, and federal response agencies, port authorities, and local stakeholders, including businessmen.

Local and state agencies, and qualified maritime businesses, are eligible for port-security grant funds to help establish and operate the security programs needed to mitigate risk and improve response capabilities within local port areas. The Coast Guard awarded $388 million in port-security grant funds in fiscal year 2009, and the American Recovery and Reinvestment Act, signed into law earlier this year, provided an additional $150 million in supplemental funding for port security.

The Port Security Grant funds are primarily intended to assist ports in enhancing maritime-domain awareness, according to Gove, but they also are used to develop and improve the risk-management capabilities needed "to prevent, detect, respond to, and recover from [terrorist] attacks." The grant program is expected to be funded at or near the same level next year so that the recent-year improvements in port security, response, and recovery will continue at much the same pace.

Rescue 21 Plus TWICs And Data Fusion = A Full Plate

The previously mentioned Rescue 21 program modernization also will continue to improve the Coast Guard's ability not only to respond to emergencies but also to enhance the service's ability to carry out its equally important law-enforcement, marine-safety, environmental-protection, and homeland-security missions. "Rescue 21 has enabled the Coast Guard to determine the location of any VHF transmission that lasts longer than one second," Gove commented. That capability "significantly reduces the time it takes for our search-and-rescue assets to locate those in distress, greatly increasing the rate of successful rescues," he continued. "Rescue 21 meets the communication standards that enable the Coast Guard's interoperability with other federal, state, and local public-safety organizations and improves our command-and-control capabilities."

The Coast Guard also will continue to work next year, as fast as possible under difficult circumstances, on implementation of the Transportation Worker Identification Credential (TWIC) program. According to the Department of Homeland Security's Transportation Security Administration, 1.4 million people are already enrolled in the TWIC program, and over 1.2 million TWICs have been issued. The Coast Guard is working assiduously both on the somewhat complicated TWIC implementation regulations and on an acceptable standard for the biometric readers used in the program to help improve overall port security in general and, more particularly, to control access to sensitive areas of the port such as those where toxic chemicals are loaded or unloaded.

Adding to the USCG's already full plate of duties and responsibilities is the fact that new "data fusion centers" are rapidly expanding throughout the United States to help improve data and intelligence sharing between and among federal, state, and local law-enforcement and emergency-response agencies. The primary objective of the 70 fusion centers already operational is to share data and analyze intelligence. Because the real goal is to improve the protection of the U.S. homeland, the centers do not focus exclusively on maritime issues but also on many other aspects of homeland security. Like many other agencies, organizations, and operational units formed since the 9/11 terrorist attacks, the fusion centers were established primarily to provide the intelligence and analyses needed to improve U.S. law-enforcement capabilities in general and thereby protect not only U.S. port and coastal areas but the American homeland as a whole.

The Coast Guard requested $9.95 billion in fiscal year 2010 for its operations and modernization budget. Assuming that all or most of that request is approved, the service's modernization efforts will undoubtedly continue to improve for the foreseeable future, as will its response and readiness capabilities – but so will the already long list of Coast Guard duties and responsibilities.

Corey D. Ranslem, chief executive officer of Secure Waters LLC – a maritime-security and consulting firm heavily involved in maritime training, maritime security, and a broad spectrum of other programs in the maritime field – is the former regional manager of Federal Government Operations for Smiths Detection. He has received numerous awards and citations from the U.S. Coast Guard and other agencies and organizations active in the field of maritime security.

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

Important Safety Information

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

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

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

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

References: 1. DuoDote™ (atropine and pralidoxime chloride injection) Auto-Injector (package insert). Columbia, MO: Meridian Medical Technologies™, Inc.; 2007. **2.** Agency for Toxic Substances and Disease Registry. Medical Management Guidelines (MMGs) for nerve agents: tabun (GA); sarin (GB); soman (GD); and VX. Available at: http://www.atsdr.cdc.gov/MHMI/mmg166.html. Accessed February 21, 2007. **3.** Holstege CP, Dobmeier SG. Nerve agent toxicity and treatment. *Curr Treat Options Neurol.* 2006;7:91-98. **4.** Data on file. Columbia, MO: Meridian Medical Technologies™, Inc.

DuoDote™ AUTO-INJECTOR

(atropine and pralidoxime chloride injection)

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

Sterile solutions for intramuscular use only

FOR USE IN NERVE AGENT AND INSECTICIDE POISONING ONLY

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

INDICATIONS AND USAGE

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

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

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

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

CONTRAINDICATIONS

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

WARNINGS

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

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

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

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

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

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

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

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

PRECAUTIONS

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

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

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

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

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

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

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

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

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

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

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

Pregnancy:

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

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

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

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

ADVERSE REACTIONS

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

Atropine

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

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

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

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

Pralidoxime Chloride

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

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

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

Atropine and Pralidoxime Chloride

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

OVERDOSAGE

Symptoms:

Atropine

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

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

Pralidoxime

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

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

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

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

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

MERIDIAN MEDICAL TECHNOLOGIES™

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

MMT 5173 11/07

Party Crashers Should Go From White House to Big House

By Bradley Blakeman, Viewpoint

An Insider's Report on the White House "Gate-Crashing" Incident

To Our Readers: During the past two weeks there have been numerous articles, editorials, and commentaries in the print and broadcast media about the so-called "Gate-Crashing" incident at the White House during which two reportedly uninvited guests showed up at President Obama's formal state dinner honoring India's Prime Minister, Manmohan Singh, and Mrs. Singh. Almost all of those articles and editorials focused primarily on the daring/presumptuousness of the couple and/or on the breach of security involved. But the full details of the security precautions that are, or are supposed to be, taken on such occasions were usually not included in the editorials, commentaries, etc.

The following article by Bradley A. Blakeman – which first appeared as a Fox News Forum Opinion article and is reprinted here with the permission of Mr. Blakeman – provides the best and most detailed report on White House security procedures that has come to DPJ's attention. We thought you might be interested in an accurate report on the behind-the-scene details. Martin (Marty) Masiuk, publisher.

We need to exchange the Salahis' 15 minutes of fame for at least 15 days in jail.

Michaele and Tareq Salahi, the social climbing couple who crashed the White House state dinner last week, should be prosecuted to the fullest extent of the law.

The couple's ability to gain access to the White House was a colossal breakdown of security and staffing procedures.

A White House state dinner is the "Super Bowl" of White House events. It is the social event of the season and the focus should be on the honored guests, not those who should never have even been there to begin with.

The following is the scenario that is typically followed when one is invited to a state dinner at the White House:

1. The Office of the Social Secretary – on behalf of the president and first lady – extends an official invitation to the guest by mail.

2. The guest replies to the invitation either by phoning or mailing the following information to the Social Secretary's Office: name, date of birth, Social Security number, race, and sex.

3. Thereafter, as information is gathered, the Social Office turns it over to the Secret Service so that they can run a criminal background check on every guest who has accepted the invitation. This procedure is referred to in the White House as being "WAVED" – "WAVES" is the acronym used by the Secret Service to denote their screening procedures for guests cleared to enter the White House's 18 acres.

4. About an hour before the official start of the event, guests are told to assemble at the Southeast gate of the White House and to produce a valid photo ID so they may be checked in.

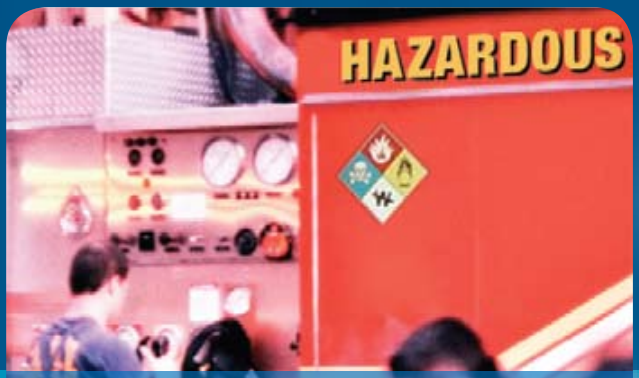
At this first checkpoint, typically there are members of the White House Social Office who are present, as well as Uniformed Secret Service, with clipboards that contain the names of approved guests.

If a person who is not on the list approaches the checkpoint, typically a Social Office staffer will call a Social Office superior to get further instructions. That person is then asked to stand off to the side, away from other guests, while information is being verified. The Secret Service, in my experience, would never have allowed someone onto the White House complex who is not on a list without first getting approval/verification from a White House staff member that the person is, in fact, an invited guest. The Secret Service would then require the person to wait while a computer criminal background check – aka "WAVES" – is performed before the person is walked through the magnetometers. All other guests who have been checked in from the list would next proceed directly to the magnetometers and then be escorted to the party's location. Once a person clears the magnetometer he or she has access to the White House.

The breakdown in staffing and security that led to these impostors gaining access to the White House were numerous:

1. It was reported that no one from the White House Social Office was at the Southeast gate to assist the Uniformed Division of the Secret Service in checking in guests.

Bruker Detection Corporation



Early Detection is the First Step in Protection

E²M
GC/MS System

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

HAWK FR
Stand Off Detection

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

M-IR
Mobile FT-IR

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

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

think forward

CBRN Detection

2. The Uniformed Secret Service did not verify some guests with the White House Social Office as to whether or not the interlopers were in fact valid guests, and allowed them to proceed to the magnetometers and thereafter into the White House. It remains to be seen if, in fact, the Secret Service performed the requisite criminal background check, WAVES, before letting them through the magnetometers.

3. Once they gained access to the White House there were numerous missed opportunities to discover these phonies. When guests enter the White House they walk down a long corridor where they are met by a member of the White House Social Office and a military aide, who ask their names so they can be announced to the press in the bookseller's area of the mansion. At that point there was an excellent opportunity to discover the Salahis' deception before they could even get close to the other guests, the president or vice president, and other high-level government officials. Instead, they were in fact announced to the press using their real names. Thereafter, they boldly mixed and mingled with legitimate guests before coming to the next missed opportunity where their deception could have been discovered. Guests are asked by members of the Social Office and military social aides to join a receiving line for the president and first lady together with the president's honored guests. At the start of the receiving line members of the White House Social Office have index cards arranged in alphabetical order with names of the primary invitee and his/her accompanying guest, together with their address. That card is handed to the invitees so they may hand it off to the military aide – who announces them to the president, the first lady, and honored guests. The Social Office should have discovered – at that point –that there was NO card for these "guests" and alarm bells should have gone off. Instead, what probably happened was that the Social Office staffer made up an index card for the impostors and let them in the receiving line to meet the president. Once the impostors greeted the president they proceeded to mix and mingle with legitimate guests in the East Room before leaving before dinner was served (in a tent on the South Lawn). When the Salahis decided to leave the state dinner before the meal was served this should have, once again, set off an alarm with both the Secret Service as well as the White House staff. It is virtually unheard of for guests to leave a state dinner prior to the meal being served. In my experience, the staff usually has to kick people out of the White House at the end of a function because the guests do not want to leave.

These social climbers, the Salahis, had their photos taken with not only the president but the vice president as well. They were photographed with the president's guest of honor, the White House chief of staff, and other high government officials.

Had they had evil intentions and possessed something like, say, anthrax, they could have literally killed everyone at the state dinner including the president and vice president of the United States as well as India's leader. This could have been a national and international tragedy of monumental proportions.

The fact that they were pranksters instead of terrorists should not matter. It has been said, "the most dangerous gun is one that is unloaded." You never know how dangerous people are until after the danger has passed. History tells us that many assassins have stalked their victims before getting up the nerve to actually carry out the deed.

We need to make an example out of the Salahis. They compromised the security of our president, they embarrassed our country and our honored guests. No one will ever remember what should have been a great event for one of our closest allies. All anyone will ever remember about President Obama's first state dinner will be these two party crashers.

We need to exchange their 15 minutes of fame for at least 15 days in jail. Their next invitation should come from the U.S. Attorney for the District of Washington, D.C., to appear before a federal grand jury. This time no RSVP will be necessary. The Salahis just need to show up with a toothbrush!

Bradley A. Blakeman, former president of Freedom's Watch – a conservative advocacy organization – was a member of President George W. Bush's senior staff, serving from 2001 to 2004 as deputy assistant to the president for appointments and scheduling, vetting, and research, correspondence, and surrogate scheduling. He now appears regularly – on FOX News, MSNBC, BBC, CNN, and Al Jezeera – as a Republican strategist and is published regularly in Politico, US News and World Report, Newsmax, and Foxnews.com. An attorney licensed to practice in the State of New York and the District of Columbia, he is currently serving as president and CEO with Kent Strategies LLC, a private corporation that provides strategic advice as well as crisis management and communications strategies to foreign governments and both foreign and domestic corporations.

The Jeff Cooper Principles

Changes Needed in Personal Defensive Preparedness

By Joseph Trindal, Law Enforcement

"The final weapon is the brain. All else is supplemental."
John E. Steinbeck, The Acts of King Arthur And His Noble Knights (1976)

As 2009 draws to a close, yet another mass-shooting incident has dominated the headlines. And once again police themselves have been targeted. Statistically, 2009 is turning out to be one of the most deadly years in recent times for the ambushing of law-enforcement personnel throughout the country. Because the threat environment has changed, there also should be a conscious shift in preparedness. In fact, global trends in violence show that targeting police is one of many terrorist tactics that may provide the behavioral model for increased violence toward police in the United States itself.

In the morning hours of Sunday 29 November 2009, four Lakewood, Washington, police officers were preparing for their shift when a lone gunman entered the Forza Coffee Shop with the express purpose of killing them. Unaware of the imminent threat, Sergeant Mark Renninger and Officers Ronald Owens, Tina Griswold, and Greg Richards were engaged in conversation and schedule planning when Maurice Clemmons approached them and opened fire. Targeting only the police officers, Clemmons left other patrons and employees unscathed.

Officers standing outside the Forza coffee shop where four fellow officers were murdered on November 29, 2009.

Picture compliments of Robert Sorbo/Reuters

Clemmons' record of criminal violence was a long one, and he had more than once in the past talked about his hatred of police. The biggest unanswered question in the Coffee Shop incident, therefore, is this: What changed in Clemmons' psyche to cause him to even attempt such an attack against an apparently overwhelming force of four armed officers? Clemmons is now dead and unable to answer that question. But, even as the still ongoing investigation continues revealing various related facts and circumstances, it seems obvious in retrospect that Clemmons had fully intended to survive his assault. In fact, he had arranged an escape plan, with the alleged pre-attack collusion of an accomplice standing by in a getaway vehicle.

In addition, the four officers apparently were unaware of the threat Clemmons posed until he made his intentions clear by aiming his gun and firing at them. He was able to get close enough to hit at least one or more of the officers, in fact, while they remained seated. The officers who were not immediately hit began their personal reactionary processes and at least one of them was able to struggle with and severely injure Clemmons before succumbing to injuries.

In the preceding month just a few miles to the north – i.e., in Seattle – Police Officers Timothy Q. Brenton and Britt Sweeny were ambushed in their patrol vehicle while discussing police reports; Brenton died in the attack. The Seattle assailant, Christopher Monfort, also had manifested a deep hatred of police. This salient fact was first mentioned in academic papers, which were followed by the bombing of four Seattle police cruisers and culminated in the assassination of Officer Brenton and attempted assassination of Officer Sweeny.

One week after the Lakewood murders – i.e., on 6 December 2009, in Penn Hills, Pennsylvania – Police Officer Michael Crawshaw was assassinated in his patrol vehicle, awaiting backup before answering a domestic-disturbance call up the street. In both of these incidents, Lakewood and Penn Hills, the officers were carrying out their duties in a manner consistent with those carried out every day by hundreds of thousands of police officers throughout the United States and, in fact, in almost every other nation in the world.

February 16–19, 2010
Atlanta Marriott Marquis
Atlanta, GA

Public Health PREPAREDNESS SUMMIT 2010

Join your colleagues for the largest gathering of public health preparedness and response professionals to:

- Find solutions to enhance the preparedness efforts in your agency and community;
- Discover innovative advances in public health preparedness; and
- Network and develop invaluable connections.

KEYNOTE SPEAKERS

John M. Barry—the *New York Times* best-selling author whose books such as *The Great Influenza* have won more than 20 awards.

Ana-Marie Jones—the dynamic Executive Director of CARD – Collaborating Agencies Responding to Disasters, who is a passionate advocate for building disaster resilient communities.

SELECTED SESSION TOPICS

- Lessons learned from H1N1
- Point of Dispensing operations
- Mass fatality management
- Protecting critical infrastructure
- Public health legal preparedness
- Community and partner engagement

NEW FOR 2010

SummitUp—the Public Health Preparedness Summit blog that will keep you up-to-date on the latest conference information.

Visit www.phprep.org to register. Follow us at www.twitter.com/phpsummit.

SUMMIT PARTNERS

Association of Public Health Laboratories • Association of Schools of Public Health • Association of State and Territorial Health Officials
Centers for Disease Control and Prevention • Council of State and Territorial Epidemiologists • U.S. Department of Health and Human Services
National Association of County & City Health Officials • National Emergency Management Association • Medical Reserve Corps

Much earlier in 2009, four police officers in Oakland, California, were murdered while carrying out a "routine" traffic stop. The following month, in April, two police officers were ambushed in Pittsburgh, Pennsylvania, while responding to a 911 disturbance call – in which the assailant also killed a third responding officer. Only 20 days after that, two deputy sheriffs in Okaloosa, Florida, were murdered while attempting to arrest a suspect, on domestic violence charges, at a local gun club.

The Long & Violent History of Criminal Attacks

Ambush attacks on police officers throughout the United States are a reality of one of the many threats that have faced law-enforcement officers for more than two centuries – i.e., since the murder of Greenville, South Carolina, Sheriff Robert Maxwell in 1797. According to data available in the records of the National Law Enforcement Officers Memorial Fund (NLEOMF), this year's police shooting fatalities are up an alarming 21 percent from 2008. The NLEOMF statistics do not differentiate ambush situations by type, but the number of "multiple-officer" shooting fatalities is up from four in 2008 to 15 this year (December not included).

As the still ongoing investigation continues revealing various related facts and circumstances, it seems obvious in retrospect that Clemmons had fully intended to survive his assault – in fact, he had arranged an escape plan, with the alleged pre-attack collusion of an accomplice standing by in a getaway vehicle

The trend is clear, and police officers throughout the country must adjust their collective threat consciousness accordingly. More specifically, they must change, and elevate, their mental conditioning to avoid being surprised and overwhelmed by the sudden display of an assailant's violence.

Fortunately, there is an answer ready – seven of them, in fact. In his book on the *Principles of Personal Defense* (published by the Paladin Press in 1989), the late Lieutenant Colonel John Dean "Jeff" Cooper, USMC, discussed seven key defensive principles that he said should be engrained at the very core of each officer's survival mindset. He summarized those principles with seven words: Alertness; Decisiveness; Aggressiveness; Speed; Coolness; Ruthlessness; and Surprise. Following, compressed and paraphrased, are brief summaries of how, and why, adherence to Cooper's principles can switch the combat advantage from their would-be assailants to the police officers themselves.

***Alertness:* The baseline of situational awareness.** Here, Cooper discussed the personal defensive application of what he described as the Color Code of Mental Conditioning – in which colors ranging from white to red reflect degrees of situational awareness. Police Officers on- or off-duty should consistently maintain a state of relaxed alertness – also referred to as Condition Yellow. Officers should be constantly aware of their surroundings, recognizing that hostilities may erupt from any direction. Condition Yellow is the baseline of situational awareness. Even when in the company of fellow officers, or alone in the patrol car, constant "relaxed alertness" is vital. Given recent trends, unusual behavior or activities should cause the individual officer to elevate his or her mental alertness to a state of heightened awareness, or Condition Orange. In the context of a "routine" patrol, Condition Orange is a general or specific state of heightened awareness. If another person approaches an officer's patrol car, the officer should heighten his or her awareness to the potential that the approaching person *may* have murderous intent. From a level of heightened awareness the officer can better scale up – if and when warranted – to a defensive response, or Condition Red, in reaction to an assailant's deadly actions.

***Decisiveness:* Applicable to "any given situation."** One frequently recommended way of achieving Decisiveness is having a personal defensive plan for any given situation. In developing ad hoc plans, it is important to consider the particulars of the situation and ask "What if?" If an officer is sitting in a restaurant (asking himself (or herself) "What if an armed person comes in?"), he or she should simply play out a short defensive script to that scenario in his/her mind. This is not paranoia; it is situational preparedness. In the event a deadly-force situation does develop, the officer already has a personal defensive plan in mind.

***Aggressiveness:* Mental preparation is mandatory.** This and the remaining Principles of Personal Defense specifically apply to deadly-force situations, and recognition of that fact is an essential component of personal preparedness. Police officers are expected to *stop* aggression. They certainly must avoid *initiating* aggression; however, in response to the combative

aggression displayed by a potential assailant, they must be mentally prepared to appropriately escalate their own *defensive aggression*. In the Lakewood tragedy, for example, Clemmons' aggression was apparently much greater than that displayed by the four police officers. The evidence suggests that at least one officer, who was able to seriously injure Clemmons, was ramping up his own aggression to meet that shown by Clemmons. After being attacked, particularly in a premeditated ambush, the counter-attack must be explosive enough in nature for the officer attacked to gain, or regain, his/her personal-survival advantage.

Speed: **Swift and decisive action needed.** When conditions develop to a point in which life-saving defensive actions are necessary, time is not on the officer's side. Police officers must in almost every deadly-force encounter, therefore, react almost immediately to the life-threatening actions of the assailant. In other words, the officer must act out his or her defensive plan, swiftly and decisively, from any position and in any environment, including while seat-belted inside a parked or stopped patrol cruiser with an attack coming, in a worst-case scenario, from the left rear area behind the car.

Coolness: **The prerequisite to controlling the environment.** An ancient eastern philosophy holds that, before one can control his environment, he must first learn to control himself. Control over one's emotional state is vital in employing sound tactics and mounting an effective defense. Having a personal plan in mind and maintaining situational awareness are the vital foundations of self control. Cool-headedness is particularly difficult to maintain in an ambush situation, but most ambushers anticipate swift and easy success in their attack. The alert officer – with a plan in mind for a counterattack and the controlled escalation of accurate aggressiveness – will overwhelm the mental preparedness of all but the most ardent ambusher. Coolness of one's mindset could be simply expressed as "I knew this could happen, and I am prepared!" At a deep subconscious level, coolness may seem to be an almost "out of body" experience in which sound training and mental preparedness appear to happen automatically.

Ruthlessness: **Personal survival is at stake.** The sixth Principle must be considered in the context of coolly deliberate survival determination. An ambush is a personal assault directed against a specific person or persons. For police officers, the immediacy of their defensive survival responses must be an absolute and unwavering commitment to thwart the deadly intentions of the assailant. After a deadly ambush has been initiated, the officer's best response is to swiftly carry out his or her defensive plan with a ruthless commitment to personal survival. One must keep in mind the possibility that the personal defensive plan may not involve a firearms response per se – but instead may involve, for example, using the patrol vehicle as a defensive weapon, or as a way of evacuating the field of fire. In any instance, the same ruthless and unwavering commitment to the course of action taken is essential to survival.

Surprise: **Counter-intuitive, but it works.** Most assailants seek to use the element of surprise in their attacks. Employing the element of surprise in a defensive context, therefore, is often the best way of seizing situational advantage. In an ambush attack, turning the tables on the assailant's situational advantage is especially critical. Surprise is achieved by acting in a manner that an assailant is not likely to expect. A classic military counter-ambush technique is to attack the ambusher. Although it seems counter-intuitive, an aggressive counterattack often surprises and unnerves the attacker. The police officer's personal defensive plan should therefore consider incorporating an element of surprise. In a restaurant situation, for example, the surprise element may be simply diving for cover before engaging the threat. The assailant is likely to expect his quarry to remain stationary. But a swift, decisive, and *surprising* move may unnerve the attacker and turn the tables in favor of the police officer.

The trend is clear: Violent attacks against police officers, despite their frequent numerical advantage, are multiplying in recent years. Criminals, including terrorists, will probably continue and further increase such attacks in the coming year. Police officers can change the grim statistics of the past several years to their advantage by shifting their personal defensive-preparedness mindset to focus more specifically on ambush-attack situations. Through a swift and effective defensive response, alert and personally prepared police officers will deny these vicious criminals – who lurk in almost every major city throughout the nation – the opportunity to carry out their murderous assaults.

Joseph Trindal is a retired federal law-enforcement officer. During his almost 30-year career with the U.S. Marshals Service and the U.S. Department of Homeland Security, he developed and delivered numerous training programs in firearms, officer survival, terrorism preparedness, and personal protection. A Marine Corps veteran, Trindal continues teaching and coaching law-enforcement officers and security professionals in many facets of personal defensive preparedness.

OUR MISSION YOUR SAFETY

MSA
The Safety Company

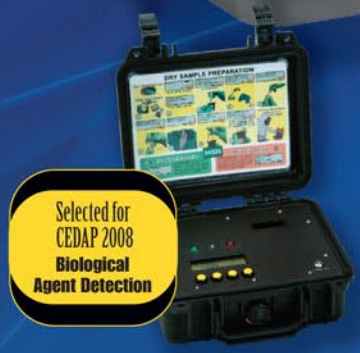
SAFESITE® MULTI-THREAT DETECTION SYSTEM

Critical Infrastructure
Emergency Response
Public Events
Perimeter Monitoring

Monitors and wirelessly communicates 6 potential threat types simultaneously:

- VOCs – volatile organic compounds
- TICs – 16 toxic industrial chemicals
- CWAs – nerve and blister agents
- Gamma radiation

VISIT US ONLINE
MSANET.COM



BIOLOGICAL
AGENT DETECTION

CWA & TICs
HANDHELD PORTABLE

FIXED-POINT CWA
MULTI-THREAT DETECTION

1.866.MSA.1001 | www.MSAPOLICELINE.com/domprep.html

First-Person Report

Forecast 2010: A New Model for Disaster Management

By Mark Merritt, Viewpoint

The nation's fifth largest recent disaster has affected the citizens of Iowa for the past 18 months but, thanks to an innovative approach to disaster management, that state's weather problems have been almost unknown to the outside world. One result is that, as we begin 2010, the most significant change in disaster management is probably going to be the way in which other states handle their own long-term disaster-recovery programs.

In 2008, Iowa experienced the most devastating series of natural disasters in the state's history, when severe floods, tornadoes, and storms hit Iowa – resulting in 85 of the state's 99 counties being declared federal disaster areas. Initial statewide estimates for damages were between $8 billion and $10 billion.

It was immediately clear that the standard disaster-recovery programs and processes were not going to work for Iowa this time around. Governor Chester John "Chet" Culver decided that much greater cooperation and coordination were needed. He sought to engage the public, primarily through the appointment of a volunteer advisory committee through which the citizens of Iowa themselves could find the solutions needed. That decision, and the processes followed, fundamentally changed the dynamics of disaster recovery.

To facilitate the changes likely to be needed, Culver established the Rebuild Iowa Office (RIO) and the Rebuild Iowa Advisory Commission (RIAC). The order's intent was to "turn tragedy into opportunity by building back smarter, stronger, more sustainably, and safer than before."

RIO & RIAC: The Agents of Change

In creating RIO, Culver envisioned a ready and responsive organization committed to rebuilding a resilient Iowa that would be safe, sustainable, and economically strong, reaffirming its ties to the land, rivers, environment, and rich cultural history. His vision in establishing RIAC – a 15-member, non-partisan commission made up of business and community leaders from every part of Iowa – was much the same. Members of the commission worked tirelessly to visit communities affected by the disasters, listened to numerous Iowa citizens – and to recovery experts, business and political leaders, and other stakeholders – and determined the top priorities for the immediate recovery process.

Only 45 days after its creation, the RIAC released its first report, which included a list of priorities and recommendations for short-term recovery operations. A more comprehensive report, addressing each of the Task Force areas and detailing longer-term disaster-recovery priorities and recommendations, was released 120 days after the RIAC's creation.

The RIO originally was staffed with consultants from my company, James Lee Witt Associates, and from the State Public Policy Group, an Iowa-based consulting firm. Other state employees were temporarily "borrowed" from other agencies. The Rebuild Iowa Office-type of organization structure was first developed when we worked with then-Louisiana Governor Kathleen Blanco following Hurricane Katrina in 2005, but the Iowa Office took on a life of its own. Eventually, the RIO was established within the Iowa Code and was allocated 12 State FTE (full-time equivalent) positions in order to remain staffed through the Office's "sunset" date of 30 June 2011.

Coordination – The Key To Sustained Progress

The RIO's most important role is to coordinate work among the many state and federal agencies and local entities involved in disaster-recovery decision-making and program administration. The coordination process not only has cleared up program bottlenecks very quickly but also has led to several innovations that probably would not otherwise have occurred. Following are but a few of numerous examples that might be used:

- Using Community Development Block Grant (CDGB) funds, an education campaign is being coordinated by the Iowa Insurance Division on future risks, and the consequences of redeveloping in a flood plain, by advocating for flood insurance in Iowa and has already helped to increase NFIP (National Flood Insurance Program) participation.

- Displaced workers who received employment through the Emergency Public Jobs Program were able to assist both

in staffing the case-management system and in administering the paperwork required for the Iowa Unmet Needs Grant Program. Their efforts helped considerably to move programs more swiftly and to increase the number of loans made to Iowa residents.

- Using Community Development Block Grant (CDBG) funds to pay for improved flood- plain maps for Iowa resulted in more accurate planning and improved risk-assessment decisions.

- Currently, EPA (Environmental Protection Agency) Smart Growth Assistance is being provided to an unprecedented number of Iowa communities to assist with their recovery plans. In addition, the Rebuild Iowa Office and other state and federal agencies are teaming up both to promote Smart Growth in the statewide disaster-recovery effort and to provide the assistance that many communities need to transform their plans into a sustainable reality.

CDGB and State Funding Programs, And a Focus on Case-Management

As of last month, Iowa had received nearly $800 million in CDGB funds, and the RIO has worked closely with other state agencies to develop innovative action plans to spend the funds provided not only effectively but also *cost*-effectively. Thanks in large part to the help provided by the RIO – along with the Iowa Department of Economic Development, the Iowa Finance Authority, and the Governor's Office – several new programs have been created to assist the Iowans hit hardest by the series of floods and other natural disasters mentioned earlier. The RIO's involvement also has resulted in using these funds in several new and different ways – providing business assistance, for example, and helping with flood-plain mapping, insurance promotion, case management, and other previously neglected possibilities. It seems likely that no other state has used its funds quite so effectively and in so many ways.

In the months immediately following the 2008 weather disasters, Governor Culver used $35 million in state funds to create two additional forward-looking initiatives – the Jumpstart Housing and Jumpstart Small Business Assistance Programs – through which individual citizens have been able to receive interim state funding for housing repairs, interim mortgage assistance, down-payment assistance on replacement homes, and other business assistance in general.

Following Culver's example, the first bill passed by the 2009 Iowa Legislature allocated $56 million in state funds for disaster-relief programs. That Jumpstart allocation has already assisted more than 1,000 Iowa families, and Individual Unmet Needs Grants have helped more than 3,000 additional families. Both programs provided funds that undoubtedly would not otherwise have been available.

Meanwhile, the RIO continued to focus on case management by creating a system – involving more than 25 Long-Term Recovery Committees established throughout the state – to help locally based case managers work with disaster-affected Iowans to navigate their way through the recovery programs available (and, not incidentally, receive additional assistance through non-profits or other private resources). Without that structure in place, local voluntary agencies would be able to receive little if any guidance in helping disaster-affected individuals through the recovery process.

Iowa's Success: An Example for the Nation

The RIO also has started several efforts to help improve and reform the fractured and incomplete *national* disaster-recovery system. Typically, federal resources: (a) are not designed for use in disaster recovery; (b) come with a multitude of restrictions; and (c) are therefore very difficult to spend in times when unexpected disasters do hit.

In the summer of 2009, the RIO and FEMA (the Federal Emergency Management Agency) joined together to complete an Iowa Recovery Analysis. That analysis looked both at "best practices" and the accompanying challenges, and suggested numerous improvements in disaster recovery that could be achieved at all levels of government – local and state as well as federal. The Iowa RIO used the analysis to develop a number of federal recommendations that are now being shared with state and federal agencies, Iowa's congressional delegation, and other interested parties.

The RIO will continue to engage with those who can change the federal disaster-recovery system and to lead discussions on this topic with the hope of improving the system not only for the remainder of Iowa's own 2008 recovery process but also to help other states cope with future disasters nationwide.

Mark Merritt, the President of James Lee Witt Associates, is responsible for the response and recovery division of the crisis and emergency management consulting firm, which is based in Washington, D.C. Witt Associates is now working with approximately one fifth of the nation's states, in addition to Iowa, to streamline and effectively manage their current systems of coping with natural disasters.

Hospital Preparedness 2010: Are Additional Advances Possible?

By Craig DeAtley, Public Health

The year 2009 will be remembered as a particularly busy one for U.S. healthcare systems, especially hospitals. The spring and fall phases of the H1N1 (Swine Flu) virus challenged the ability of hospitals of all sizes to care for above-average numbers of patients in their emergency departments and inpatient services. Included in that response effort were numerous instances in which hospitals had to deal with serious logistic and financial issues related to, among other things: (a) obtaining and issuing the personal protective equipment (PPE) needed for the hospital staff; (b) having enough vaccinations available for both staff and patients; and (c) finding sources of Tamiflu and/or other medications for their adult and pediatric patients.

Fortunately, the flow of federal funding continued for most if not quite all community hospitals – but in reduced amounts for many of them. As the end of the year approaches it seems likely – with the congressional debate over healthcare reform not yet resolved and the uncertainty continuing about what if any legislation might finally emerge – that 2010 holds the potential for considerable change. Following are some of the more important possibilities.

As the end of the year approaches it seems likely – with the congressional debate over healthcare reform not yet resolved and the uncertainty continuing about what if any legislation might finally emerge – that 2010 holds the potential for considerable change

I: NIMS Compliance Objectives For Healthcare Facilities Will Be Renewed

The Departments of Homeland Security (DHS) and Health and Human Services (HHS) will collaborate on the latest round of NIMS-compliance guidance for healthcare facilities. A work group composed of a broad spectrum of individual hospitals, state hospital associations, and AHA (American Hospital Association) representatives already has started to meet on a regular basis and to work with government officials to develop specific recommendations related to current NIMS (National Incident Management System) guidelines.

Preliminary indications suggest that there may be no *new* objectives added during the coming year to the current fourteen (14) objectives. However, the updated guidelines probably will not only provide greater clarification on how current NIMS objectives can be met but also clarify how they relate to other organizational expectations such as those proposed/recommended by the Joint Commission and the National Fire Protection Association (NFPA). It also seems clear that, with the fiscal challenges hospitals are already facing, any new recommendations that raise costs will not be well received and could be met with stiff resentment if not outright rebellion.

II: The Hospital Incident Command System (HICS) Will Be Modified

California Emergency Medical Services, using funds provided by the state's Department of Veteran Affairs, is planning to hold a stakeholders conference sometime next year to review the current design and use of the Hospital Incident Command System (which was established in 2006). The meeting may well serve as the first step in shaping HICS improvements based on: (a) lessons learned from facilities using the current guidelines during training programs; (b) real-world events that have exposed unforeseen gaps in overall preparedness capabilities; and (c) the recommendations of those who are teaching or managing current training programs. *Extensive* changes to the current HICS guidelines do not seem likely at this point, but a number of refinements to Job Action Sheets, Incident Planning materials, Response Guides, and a broad spectrum of educational and training materials also are anticipated.

III: Emergency Preparedness Could Become a Lower Priority for Hospitals

Whether because of the prolonged and costly response to H1N1, the shrinking of external funding support, and/or the nation's distressed economic conditions in general, it is entirely possible that hospital emergency preparedness, which is still a high priority for most if not all healthcare facilities, may return to pre-9/11 levels for many of them. Faced with still shrinking operating margins or worse, hospital CEOs may be forced to make more budget cuts and/or staff reductions and, without actually saying so, to move emergency preparedness down a few notches on the overall priority list. The commonly held view that most communities and their hospitals have mounted a successful response to the H1N1

virus may also lead some hospital and healthcare officials to believe that a strong response foundation is already in place – and, therefore, that reductions in the time and effort allocated to emergency preparedness may be justified. That view is reinforced, unfortunately, by the past few years of federal funding emphasizing the development of healthcare coalitions. However, any decision to lower emergency preparedness on the priority list may leave a growing number of hospital emergency preparedness managers either: (a) splitting their time between assigned tasks; and/or (b) paying more attention to other responsibilities that are *not* preparedness related; and/or (c) even worse – out of jobs altogether.

IV: Healthcare Reform (If Enacted) Will Have a Major Impact

Perhaps the greatest potential for change in 2010 will come if (when?) a healthcare reform bill is enacted into law. The current House and Senate bills do not specifically address the need for hospital emergency preparedness. A major related concern is that the bills introduced in both houses have proposed considerable reductions to current Medicare funding for hospitals. In addition, reductions in educational spending that also have been proposed, combined with increased government emphasis on outpatient services and outcome-based care, could have a negative impact on the internal funding support that hospitals can make available for preparedness efforts. One example: HHS's increased funding support for coalition-related activities may well lead to continued overall *system* improvements, but there probably would be less direct funding available for individual hospital efforts.

To briefly summarize: The major 2009 healthcare incidents and events – e.g., the H1N1 pandemic, numerous transportation accidents (on land, at sea, and in the air), and various weather-related emergencies – saw hospitals demonstrate the benefits of: (a) keeping emergency preparedness a high priority; and (b) making federal funding available to purchase needed resources and to develop and/or improve current response systems and equipment. The year 2010 may see further advances, many of them building on past successes – or, perhaps, a disturbing recognition that the best efforts to improve preparedness may have already been completed and that there may be additional advances, but at a slower pace.

Craig DeAtley is the director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the District of Columbia's largest hospital. Prior to assuming his current position, he was an Associate Professor of Emergency Medicine at George Washington University, for 28 years, before leaving to start the Institute. He also works as a Physician Assistant at Fairfax Hospital, a Trauma Center in Northern Virginia, and he has been a volunteer paramedic with the Fairfax County Fire and Rescue Department since 1972.

What Gets Measured, Gets Done!

The Long and Winding Road of Preparedness Measurement

By Timothy Beres, Funding Strategies

For the state and local organizations that have been involved in federal efforts, or efforts of their own, to measure preparedness, that task is not taken lightly. There have been many top-down federally directed efforts to measure preparedness. Most of these initiated at the direction of Congress or the Government Accountability Office (GAO) in an effort to determine the nation's current state of preparedness, the gaps in that preparedness, and the effectiveness of federally funded preparedness programs.

These efforts are already underway, because those who have been given the responsibility for preparedness programs care about the preparedness of the nation and want to improve upon those programs and preparedness efforts, rather than imposing unreasonable work requirements on those participating in preparedness assessment.

However, that does not mean that these efforts have not been burdensome. The measurement pendulum has taken great swings between *what* should be assessed and *how* to assess (subjectivity vs. objectivity), and the result has been a half dozen or so approaches that: (1) have yielded very little in answering the question "How prepared is the nation?"; but (2) have also produced a great deal of frustration. The same frustration is felt by those – from Congress to the Executive Branch and from the police station to the firehouse – who are most involved in the assessment process. In short, although a great amount of effort has been expended, a comprehensive report on National Homeland Security Preparedness has still not resulted from these assessment efforts.

In addition, although there may be problems with the data itself, analysis efforts have also been lacking. In fact, the analytic efforts to provide something useful to the federal government, and back to the states and local communities involved, have only just begun. Even if all the data provided was reliable, the current system of self assessment is a static process that is not comprehensive by any definition and therefore provides only a brief snapshot – which quickly fades – of the current state of preparedness.

The What, How, And Why of Measurement Parameters

However, the field of preparedness measurement is rapidly evolving. And, while self assessment will continue to be a part of the measurement framework, other ideas and methods are being developed to tackle the seemingly intractable problems of what to assess, and how. Many current discussions are grounded in three simple principles: (1) measure only what really matters; (2) what *is* measured should be just as relevant and meaningful to operational personnel as it is to political leaders; and (3) *how* it is measured should lead to an understanding of predicted performance, not simply produce an exhaustive inventory of operational assets and activities undertaken.

What adherence to these principles should lead to is a preparedness assessment process that does not attempt to measure everything. Measurement should be focused primarily, if not exclusively, on the critical enabling capabilities and, within that broad field, only the key indicators of performance – with special focus on those areas that are not regularly used or practiced.

Utilizing risk analysis can help apply focus to determining the specific critical capabilities that an area may need. However, it seems clear that, without being able to demonstrate certain general capabilities as defined in the Target Capabilities List (TCL) – e.g., in incident management, planning, communications, and information-sharing – then having specific site- and/or team-based capabilities may not matter. If sophisticated teams that are involved in a large-scale response are unable to communicate, they also may be unable to effectively operate during the incident. Efforts therefore

GOVSEC
THE GOVERNMENT SECURITY EXPO & CONFERENCE

U.S. LAW
CONFERENCE & EXPOSITION

MARCH 23-24, 2010
WASHINGTON D.C.
WALTER E. WASHINGTON CONVENTION CENTER

WHERE THE MISSION IS TO SECURE OUR NATION

GovSec/U.S. Law is the only event for government that offers a comprehensive perspective on homeland security and has the convergence of IT and physical security at its core. Engage yourself in the full GovSec/U.S. Law experience, including:

A 2-day, 4-track, 20-session program focusing on

- Critical Infrastructure Planning and Protection
- Cybersecurity and Information Assurance
- Domestic and International Terrorism: Deterrence, Preparation and Response
- Law Enforcement Case Studies and Tactics

An expo floor featuring cutting-edge security products demonstrated by top industry innovators. Experience, first-hand, the newest systems, tools and technologies preventing future incidents, preparing for and responding to all hazards and disasters, and ensuring the public safety.

OPENING KEYNOTE
Anthony E. Zuiker
Creator & Executive Producer of CSI: Crime Scene Investigation
"Cross Platforming: New Interactive Strategies and Creative Solutions"

Don't miss this year's only expo and conference with a comprehensive approach to securing our country. GovSec/U.S. Law—a must attend for 2010!

EVENT HIGHLIGHTS

Powerful keynote lineup jump starting each day

High-level, in-depth conference program

2nd Annual Domestic Defense Symposium: U.S. Military Forces, First Responders & Defense of the Nation

Featured areas on the show floor:
- Cybersecurity Pavilion
- Focus on Digital Forensics
- U.S. Law

And so much more!

BONUS!
Access to FOSE featuring the Defense Innovations Pavilion!

OFFICIAL PUBLICATIONS

DEFENSE SYSTEMS | Federal Computer Week | GCN | network centric Security | Security Products | Washington Technology

PRODUCED BY

1105 GOVERNMENT Information Group

UNCOVER THE CRITICAL INFORMATION YOU NEED TO COMPLETE YOUR MISSION

FOR FULL EVENT DETAILS AND TO REGISTER:
www.govsecinfo.com

PLEASE USE PRIORITY CODE NW1S12 WHEN REGISTERING
REGISTER TODAY!

Connect with GovSec/U.S. Law on facebook | govloop | LinkedIn | twitter | YouTube

should be focused on reaching consensus in determining the subset of "make it or break it" capabilities that are needed by the nation and that will, as a minimum, have jurisdictions prepared *not* to fail. Tightly focusing measurement on the most critical activities creates an opportunity for a comprehensive national approach to preparedness measurement that is not only meaningful but manageable as well.

Three Approaches, Capability Models, And Meaningful Evaluations

Comprehensive preparedness measurement should take advantage of three approaches: self assessments; quantitative measurement; and performance-based evaluations.

The first approach, self assessments, can generate very important and useful data because the information developed comes from those who know their individual circumstances the best. It should be recognized, though, that there have been several problems with self assessments in the past – overly burdensome tools, for example, as well as tight time frames, unreliable technology, inadequate guidance, and "gaming" of the assessments – all of which resulted in, at best, questionable results. In order for reliable, accurate, and useful data to be generated, capability assessments must, first of all, be meaningful to those being assessed. The goal of future self-assessments and the collection of data must therefore be to support operational planning and programmatic decision-making at the level of those who are being assessed.

Those who have been given the responsibility for preparedness programs care about the preparedness of the nation and want to improve upon those programs and preparedness efforts, rather than imposing unreasonable work requirements on those participating in preparedness assessment

Quantitative capability models can be developed both to assist with planning and resource allocation and to help determine capability gaps. Such models can provide an independent baseline estimate – based upon national averages, demographic information, and risk criteria – of the levels of capability required for a given jurisdiction. The same models can use quantitative data to inform investment decisions: (a) by determining the scalability of a capability to a given scenario, thus generating capability calculators; and (b) by estimating the full life-cycle costs of achieving a given level of a particular capability, identifying capability gains from investments, and optimizing the placement of new operational teams and capacity at all levels.

The evaluation of exercises and real-world events should be used to assess actual performance. An effective performance-testing program at the national level would not only gather consistent data but also analyze after-action reports to determine what happened (and why it happened), and compare findings across different exercises and events to identify trends and common points of failure. Moreover, it would assess holistically how capabilities integrate both horizontally and vertically. Past experience – Hurricane Katrina is perhaps the best example – has shown that the national response system frequently breaks down in complex events at the horizontal and vertical seams between capabilities. Consequently, performance evaluations must include the analysis not only of individual capabilities themselves but also of the connections across capabilities as a portfolio. All of this should be done not in an effort to judge or cast blame but, rather, to understand priority issues as quickly and directly as possible.

Without a comprehensive approach for measuring preparedness, the nation will continue to struggle to understand the current state of preparedness across all regions, and for all hazards. Some areas may over-prepare relative to their true risk-based capability needs; others may under-prepare; and still others may prepare for the wrong things altogether.

Timothy Beres, vice president, CNA Safety and Security, is responsible for that organization's safety and security research and analysis program in the fields of public safety, criminal justice, homeland security, emergency management, and emergency public health. Prior to joining CNA he held senior leadership positions in the Department of Homeland Security and the Department of Justice. He is responsible for, among other accomplishments: development of the first risked-based preparedness grant program - the Urban Areas Security Initiative (UASI); establishing the first communications and terrorism prevention technical assistance programs for state and local jurisdictions; developing a national Weapons of Mass Destruction training program for state and local first responders; managing establishment of the Center for Homeland Defense and Security at the Naval Post Graduate School; initial implementation of Homeland Security Presidential Directive 8 (HSPD-8); and creation of the first transit security grant program.

Protecting Citizens by Predicting Future Threats

By JL Smither, Viewpoint

In order to protect citizens, responders should, as often as possible, be aware of and react to threats before they escalate into incidents. Threats can be observed, or deduced, through local crime trends, interstate intelligence bulletins, forecasts of extreme weather conditions – and/or a number of other ways. By predicting the pattern of threats, responders can keep the damage caused by incidents down to a minimum.

In 2006, because of changing trends in criminal activity, members of the Chicago Police Department's Deployment Operation Center realized that officers would probably benefit from the development and promulgation of real-time crime data in each of the Chicago metropolitan area's 25 districts. The center, working together with the Informational Services Division, created the District Intelligence Bulletin System (DIBS), an online application that maps real-time crime and threat data by district. By providing this information to law-enforcement officers, they increased not only situational awareness but also the chances that law-enforcement agencies will be able to stop a threat from becoming a reality.

The DIBS application pulls information from several sources, including: (a) 911 calls from citizens who have seen people with guns and/or observed gun crimes; (b) drug sales; and (c) gang-related crime and other disturbances. The application also includes information about the eight most recent shootings in the district and as many as six individuals in each district wanted by law-enforcement agencies. Law-enforcement and fire officers can upload additional information to the system as needed. With the availability of these additional resources, DIBS provides officers with a more predictive crime capability. When officers monitoring the incoming information notice a spike in criminal activity, they can deploy additional officers to the "spike area" to prevent an increase in violence.

The DIBS Web site, which is available through the department's secure intranet portal, can be accessed on the squad-car personal-data transmitters carried by Chicago Police Department officers. The site, and the application data, have been made available to the Chicago Fire Department, and to the U.S. Secret Service, to use to expand and enhance their own daily situational awareness.

Similar Goals, Half a Continent Away

Another initiative with predictive goals similar to those of the DIBS system is the Los Angeles Department of Public Health's WMD (Weapons of Mass Destruction) Technical Advisory Group (TAG). The group, established in 2005, consists of Department of Public Health (DPH) staff members – including a psychiatrist, infectious-disease epidemiologists, bioterrorism lab staff members, toxicologists, environmental health experts, veterinarians, and radiation experts. The group's coordinator, assigned from the DPH's Emergency Preparedness and Response Program, works closely with the local Federal Bureau of Investigation Field Office WMD coordinator to share information related to public-health threats.

Among its other responsibilities, the TAG: (1) works to provide public-health threat prediction, mitigation, and investigation strategies; (2) helps determine the credibility of public health threats; (3) notifies the proper authorities in the case of an imminent threat; and (4) conducts on-scene consultations in the event of a public-health incident. In 2006, for example, the TAG was activated for and responded to what seemed to be a major health threat – the possible breach of a Los Angeles County reservoir. TAG members worked closely with hazardous-material professionals to determine the specific biological or chemical agents that might have evaded the reservoir's purification system and contaminated the county drinking water. They also provided instruction on how to test the water, and ultimately concluded that there was no threat to the area's water supply.

They are half a continent apart, and they differ in a number of organizational particulars, but the Los Angeles TAG and the Chicago DIBS have similar goals: both agencies work to predict, and respond to, threats before they escalate into real events.

For additional information on predictive systems and information-sharing resources, please visit Lessons Learned Information Sharing at www.llis.gov.

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

innovative technology solutions.

Upp

scalable.
mobile.
robust.

irms

The premier homeland security COTS application

Emergency, Resource, Patient, Clinic, Asset and Warehouse Management

Upp Technology, Inc. 3075 Highland Parkway Downers Grove IL 60515 800.777.6092 www.upp.com

IDGA
Institute for Defense and Government Advancement

5th Annual

CBRN DEFENSE

February 8 - 10, 2010
Washington, D.C.

Enhancing and Developing Capabilities to Prevent, Protect, and Respond to Threats Against America

Attend this year's event to gain insight into:

- Preparedness on a state and national level
- Industry standards and requirements
- Coordination response efforts between various departments and agencies
- R&D / Future technologies and management systems

MEET KEY DECISION-MAKERS AND HEAR TOP-NOTCH SPEAKERS INCLUDING:

STEVE HENRY, SES
Deputy Assistant to the Secretary of Defense for Nuclear Matters

COL WILLIAM BARNETT, USA
Joint Requirements Office for CBRN Defense

COL DAVID WILLIAMS, USA
Joint Project Manager, Chemical Biological Medical Systems (CMBS), JPEO-CBD

CSM PATRICK ALSTON
Command Senior Enlisted Leader to the Director of the Defense Threat Reduction Agency and U.S. Strategic Command Center for Combating WMD

LTC NICHOLAS PRINS, USA
Acting Assistant Director, Transformational and Applied Research Directorate, DNDO, DHS

www.CBRNEvent.com 1.800.882.8684