DomPrep Journal

US Annual $100 Volume 5 Issue 8, August 2009

"C" Is For Credentials

Time is of The Essence

The Development of
National Standards for Credentialing
By Diana Hopkins, Standards

A New and Challenging Era
For Rural Homeland Security
By Jonathan A. Dudek, Law Enforcement

Emergency Services
Credentialing: FEMA Leads the Way
By Kay C. Goss, Emergency Management

Qualifications, Credentials
And a Need for Speed
By Glen Rudner, Fire/HazMat

National Recovery Doctrine:
The Next Preparedness Frontier
By Dennis R. Schrader, Viewpoint

EMS: Increased Emphasis
On The Medical Aspect
By Joseph Cahill, EMS

Responding to Incidents
In a Neighboring Port
By Corey Ranslem, Coast Guard

Fusion Centers & Public Health Agencies:
Unlikely or Natural Partners?
By Adam Bulava, Law Enforcement

Managing the SNS Stockpile
By Joseph Cahill, Case Studies

California, Connecticut, and Texas
By Adam McLaughlin
State Homeland News

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

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:

GEOMET Technologies LLC

ICx Technologies

Idaho Technology Inc.

IDGA - Latin American Border Summit

IDGA - Maritime Security

Meridian Medical Technologies

MSA

PROENGIN Inc.

© Copyright 2009, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

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

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

IMR GROUP

Editor's Notes

By James D. Hessman, Editor in Chief

It took the United States less than four years to develop, build, test, and eventually use the atomic bombs that brought World War II to an end. It is now almost eight years since the 11 September 2001 terrorist attacks that started the U.S.-led global war on terrorism and, as a by-product, renewed interest in the definition, development, production, and distribution of a valid national identification system.

There is ample evidence that such a system was and is needed – today, more than ever before, unfortunately. Identity theft has become an international as well as national problem with major economic, national-defense, and political dimensions, and particularly grim implications for the nation's law-enforcement, first-responder, and homeland-security communities.

Glen Rudner spells out some, but by no means all, of the difficulties and complexities involved in his report – one of three "credentialing" articles in this month's printable issue of *DPJ* – on the need for speed in the writing, approval, and promulgation of the qualifications and definitions required. But accurate and effective credentialing does not simply happen – specifications and standards must first be established, so Diana Hopkins follows up with a detailed description of how those standards are being developed (by several representative stakeholder groups) and of the milestones that already have been met.

Kay Goss rounds out the triad with an insider's analysis of how three National Capital Region jurisdictions – the Pentagon, the state of Maryland, and the commonwealth of Virginia – teamed up with the Federal Emergency Management Agency to test the credentialing process in the multi-agency Winter Fox Interoperability Demonstration.

Dennis R. Schrader continues the march with an incisive article on another high-priority FEMA goal: the development, writing, and distribution of a much-needed National Recovery Doctrine, which will serve as the blueprint for governors, mayors, and emergency managers throughout the country to help their communities rebuild themselves, as quickly and as cost effectively as possible, in the wake of future terrorist strikes and/or such natural disasters as hurricanes and earthquakes.

Also in the August issue are three specially commissioned articles by: (1) Jonathan Dudek, who reports on the recent-year spread of terrorist actions and operations into the nation's rural communities; (2) Adam Bulava, who presents encouraging evidence of how the rapid growth of fusion centers has helped healthcare organizations throughout the United States become much more effective; and (3) Corey Ranslem, who spells out the difficulties and dangers involved in protecting the U.S. port system – but also notes the greater degree of cooperation and coordination now prevalent throughout the numerous agencies, organizations, political jurisdictions, and private-sector stakeholders involved in port safety and security.

Joseph Cahill again contributes two articles: one on how the U.S. emergency medical services community has continued to mature and "professionalize" at an astounding pace; the other a real-life Case Study on how Ohio and Tennessee worked with Upp Technology Inc. to develop an effective and reliable logistics system to expedite the distribution and use of vaccines and other pharmaceuticals when (no longer "if," it now seems) the H1N1 flu pandemic strikes those states.

As in previous issues, Adam McLaughlin serves as cleanup hitter with timely reports on the improved "states of preparedness" in: California (its new public-safety radio network); Connecticut (several innovative drills and exercises testing emergency-response capabilities at the U.S. Navy's submarine base in New London); and Texas (how a new fusion center in Central Texas is helping law-enforcement agencies as well as first responders and emergency managers).

About the Cover: Imitation signboard depicting a rustic "time concept." (iStock Photo)

Life Protection Systems

Protecting those who put their lives on the line.

GEOMET's Life Protective Systems offers a full line of fully integrated, modular, and performance tested personal protection equipment designed for the civilian and military first responder. Our systems provide protection against chemical warfare agents, biological agents, and toxic industrial materials (TIMs) using proven materials, modern sealing techniques, and customized breathing systems to ensure that the user is fully protected. GEOMET's Life Protective Systems include:

- *NFPA Certified Garments*
- *Protection Against Chemical Warfare Agents*
- *Flexible and lightweight*
- *Exceptional Fabric Strength*
- *Chemical Splash Protection*

GEOMET
A VERSAR COMPANY

www.geomet.com
800.296.9898

Contributors

First Responders
Glen Rudner
Fire/HazMat

Stephen 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

The Development of National Standards for Credentialing

By Diana Hopkins, Standards

Credentialing is defined as the process of establishing an individual's background, legitimacy, and qualifications for performing a specific task – and in that context is a key tool in the interstate deployment and interoperability of *trusted* resources when disaster strikes. There are many extant credentialing systems used by various agencies and organizations in the emergency-management field. However, and despite the availability of such systems, a need for *consistency* in credentialing prompted the development of national credentialing standards under the National Response Plan of the Department of Homeland Security (DHS).

By definition, a *national* standard applies to all levels of government – federal, state, tribal, and local. Among the most important requirements of the proposed national credentialing system are that: (1) It must be able to function within existing jurisdictional protocols, if feasible; (2) Its deployment cannot impose an undue burden on the numerous jurisdictions at various levels of government; (3) It must conform to the protocols, principles, and guidelines set forth in the federal Incident Command System (ICS); and (4) Current emergency-responder credentialing systems must be used or integrated with the national system whenever possible.

The development of a national credentialing system – a fundamental underpinning of the National Incident Management System (NIMS) – has specifically been assigned to the Federal Emergency Management Agency's NIMS Integration Center (NIC). That important task also involves: (a) The development of standards for and/or related to the level and currency of an individual's training, experience, physical and mental fitness, and professional capabilities; (b) The use of establishing/accrediting organizations to carry out credentialing certification and training programs; and (c) The standardization of not only job titles but also credential documentation and recordkeeping so that all appropriately qualified emergency responders in all jurisdictions, at every level of government, can be quickly identified and dispatched if, when, and where disaster strikes.

Consensus Agreement on Titles, Qualifications, and Gaps

As part of the credentialing standards development work, seven stakeholder working groups were formed to address, and then approve by consensus: seven discipline-specific job titles in emergency management; the role that responders in each discipline would be assigned in critical activities; and the qualifications, certifications, training, and education that those responders would have to meet.

The stakeholders involved in developing the job titles not only reached consensus on the "requisite" as well as "recommended" baseline standards (for education, training, experience, physical/medical fitness, certification, and licensing) but also identified certain gaps in the responder roles that NIMS-level decision makers would have to address.

With regard to the deployment of emergency responders, FEMA's National Emergency Responder Credentialing System – another system developed by the NIMS Integration

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

Center – has been assigned the responsibility of identifying and mobilizing qualified responders, selecting them based on standardized job titles and descriptions.

The principal purpose of the DHS credentialing initiative is to develop integrated and comprehensive systems for identifying, and deploying, credentialed responders – and other qualified personnel resources – to deal with a major incident when local resources are overwhelmed. As with all national standards, the stakeholder participation in developing credentialing standards is voluntary, as is stakeholder use of a finalized credentialing standard. However, it is important to note that acceptability for federal grants and funding is tied to a stakeholder's participation in such DHS initiatives.

On 21 November 2008, a draft of the proposed *NIMS Guideline for the Credentialing of Personnel* was distributed for use and comment by emergency-management professionals and other key stakeholders in the government and private sectors. Earlier this year (in April), FEMA produced the 2009 Annual Operating Plan for the National Preparedness Directorate, which lists the finalization of credentialing guidelines as one of its principal goals and names NIC and the Incident Management Systems Integration (IMSI) division as the leading agencies involved in that task.

For additional information

On job titles, see http://www.fema.gov/pdf/emergency/nims/ems_jobtitle_0308.pdf;

On the NIMS Credentialing Guideline, see http://www.fema.gov/good_guidance/download/10280;

On the 2009 FEMA Annual Operating Plan for the National Preparedness Directorate, see http://www.fema.gov/pdf/about/divisions/npd/npd_operating.pdf

---

Diana Hopkins is the creator of the consulting firm "Solutions for Standards" (www. solutionsforstandards.com). She is a 12-year veteran of AOAC INTERNATIONAL and former senior director of AOAC Standards Development. Most of her work since the 2001 terrorist attacks has focused on standards development in the fields of homeland security and national defense. In addition to being an advocate of ethics and quality in standards development, Hopkins is also a certified first responder and a recognized expert in technical administration, governance, and process development.

Rant Or Rave!

Click on 'COMMENTS' to provide feedback to the "*The Colony*"

Experts from the fields of homeland security, engineering and psychology have helped design the world of The Colony to reflect elements from both real-life disasters and models of what the future could look like after a global viral outbreak. The Colony is a controlled experiment to see exactly what it would take to survive and rebuild under these circumstances. For 10 weeks, a group of 10 volunteers, whose backgrounds and expertise represent a cross-section of modern society, are isolated in an urban environment outside Los Angeles and tasked with creating a livable society.

Tune in every Tuesday (for next 9 weeks) @ 10 p.m. ET/PT on the Discovery Channel
Follow up report to follow every Wednesday in the DPJ Weekly Brief
by Adam Montella, Homeland Security Advisor.

Discovery CHANNEL

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

A New and Challenging Era for Rural Homeland Security

By Jonathan A. Dudek, Law Enforcement

As much as I converse with sages and heroes, they have very little of my love and admiration. I long for rural and domestic scene, for the warbling of birds and the prattling of my children. ~John Adams

It might have seemed like a drill, but it was not: *First responders have been dispatched to a rural residence to investigate a domestic homicide. While searching the house they see walls draped with Nazi memorabilia, an application to join a white supremacist group, pamphlets describing how to make a "dirty" bomb, and a cache of chemicals and other toxic substances, including radioactive materials. They later were told that the deceased was "angry" about the election of President Barack Obama and had been mixing some of the chemicals in the sink.*

This frightening incident actually took place in December 2008 in Belfast, Maine, a picturesque New England seaport. *The Bangor Daily News* later reported that resident James Cummings apparently had been shot and killed by his wife, an alleged domestic abuse victim, who said he had discussed the making of dirty bombs and had in fact, as suspected, been mixing chemicals in the sink. A closer search of the house found many of the materials required to manufacture a "radiological dispersal device," the more formal name used to describe a so-called dirty bomb. Among those materials were four one-gallon containers of mixed chemicals, including: (a) the precursor materials needed for the manufacture of peroxide-based explosives; and (b) certain metal agents that are used to sensitize and amplify the effects of explosions. A number of smaller jars containing radioactive isotopes also were recovered. The police also found additional Nazi memorabilia in the house, along with a completed application to the National Socialist Movement, a white supremacist group.

Belfast, a popular tourist town, hardly seemed a likely site for a dirty-bomb laboratory. Indeed, when Americans conjure up images of Maine, lobsters and rocky coastlines usually come to mind – not FBI special agents wearing hazmat suits. Residents of Maine (and other rural states) also seek a better quality of life in which to raise their families in relative safety, to enjoy the outdoors, and to decompress from the pressures of the outside world. Many movie stars, politicians, corporate executives, authors, and other celebrities also seek the solitude of these less hectic states, where they and their families can lead more of a normal life – i.e., without paparazzi – and blend in more or less anonymously. The rural states also have a reputation of respecting individual privacy. Moreover, the more extreme forms of violent crime are less frequent in those states.

Major Changes in the Great Outdoors

However, and despite the fact that actual or suspected incidents of terrorism are rarely encountered in the rural states, last year's incident in Belfast is a reminder that the peaceful pattern of the past is changing – and that serious incidents are, in fact, now occurring more frequently in the backyards of rural America. Ironically, terrorists and extremists also are attracted by the same sense of anonymity, and the opportunity to be left alone, that is offered in rural areas.

Although the record remains unclear in some respects, it is known – from *The 9/11 Commission Report* as well as extensive media coverage (by the *Portland Press Herald*, for example) – that terrorists Mohammed Atta and Abdulaziz al-Omari drove to Portland, Maine, from Boston on 10 September 2001. They were identified shopping, dining, and making an ATM withdrawal near the Portland International Jetport before spending the night at a Comfort Inn. They then took a connecting flight to Boston – on the day of the attacks.

The 9/11 Commission, and the FBI, floated various theories as to why Atta and al-Omari had made the side trip to Maine. One theory was that they were trying to throw off law-enforcement authorities; another was that they thought security would be more lax at the Portland airport. Whatever the real reason, their mere presence in Portland underscores the need, in the Age of Terrorism, for continued vigilance – by private citizens and law-enforcement personnel alike – against international terrorists and/or their domestic counterparts.

There have been, in fact, several domestic terrorism incidents – including some with strong rural roots, not incidentally – in recent years. Eric Rudolph – the serial bomber and convicted murderer whose crimes included the Centennial Park Bombing at the 1996 Olympic Games in Atlanta, Georgia, and the 1998 bombing of an abortion clinic in Birmingham, Alabama – was one of the better known domestic terrorists. Another was Theodore Kaczynski, the so-called Unabomber who murdered three persons and injured 23 during a lengthy campaign of mail bombings between 1978 and 1995. Before being apprehended in Murphy, North Carolina, Rudolph lived in a camp in the

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

woods, feeding himself by stealing food from local farms (and sometimes from dumpsters). Kaczynski was living in an isolated shack in Lincoln, Montana, at the time he was arrested.

From the Top of the Mountain To the Bottom of the Heap

Domestic terrorism is not limited to individual eccentrics; it also includes groups – violent groups. Over the past decade, the ecoterrorist group Earth Liberation Front (ELF) and the animal-rights extremist group Animal Liberation Front (ALF) have carried out dangerous operations against U.S. industries nationwide. One of the more spectacular ELF attacks occurred on 19 October 1998, atop Colorado's Vail Mountain, where ELF members burned eight buildings, including a restaurant, and damaged ski lifts, radio towers, and a ski patrol office. The group was reportedly protesting a proposed 885-acre ski-area expansion into a known habitat for the endangered Canada lynx. The $12 million in damages caused by the ELF attack was the most costly U.S. ecoterrorist incident reported to date.

The ELF and ALF groups have been particularly active in Maine – where, since 1999, they have vandalized property, damaged a number of heavy vehicles, and committed numerous break-ins and thefts. Among their principal (and extremely varied) targets were Boise Cascade, Jackson Laboratories (renowned for its genetics research), several hunting clubs (including one in which the propane heating system of one building was rigged to explode), and a municipal landfill. Other ecoterrorist attacks occurred in 2005 in response to the Plum Creek Timber Company's plans to develop resorts, sporting camps, and hundreds of housing units in Maine's relatively undeveloped Moosehead Lake region.

Today, well organized and sophisticated criminal groups – such as the violent jihadists, ecoterrorists, animal-rights extremists, white supremacists, and anti-abortion radicals – represent unique challenges to law-enforcement agencies operating in rural environments, where the coordination of interagency operations may be more difficult and personnel as well as material resources are relatively scarce.

Well organized and sophisticated criminal groups such as the violent jihadists, ecoterrorists, white supremacists, and anti-abortion radicals represent unique challenges to law-enforcement agencies operating in rural environments, where the coordination of interagency operations may be more difficult and personnel as well as material resources are relatively scarce

An Innovative and Effective Solution

One solution for the latter problem has been the creation of so-called fusion centers – a concept that evolved after the 9/11 terrorist attacks to improve intelligence collection and sharing from diverse sources. In the Executive Summary of its August 2006 *Fusion Center Guidelines*, the U.S. Department of Justice (DOJ) said that the nation's fusion centers also could serve as a means to implement the National Criminal Intelligence Sharing Plan (NCISP) – a set of 25 recommendations, collectively described as a "blueprint," that law-enforcement officials were encouraged to use to facilitate the creation or enhancement of criminal intelligence entities.

The Guidelines – which were created by law-enforcement officials and experts from federal, state, tribal, and local agencies – address such issues as collaboration between agencies, intelligence-led policing, and community policing. Following are brief summaries of some of the more important sections of the Guidelines that are particularly relevant to state and local as well as national law-enforcement agencies and organizations.

The DOJ describes a fusion center as "an effective and efficient mechanism to exchange information and intelligence, maximize resources, streamline operations, and improve the ability to fight crime and terrorism by analyzing data from a variety of sources." The fusion process itself pertains to the acquisition, management, exchange, and analysis of homeland security-related and crime-related intelligence and information – obtained from law-enforcement, public-safety, and private-sector sources to produce meaningful and actionable intelligence and other helpful information. The fusion process also permits the augmentation and reevaluation of existing intelligence data, thus allowing for the latest updated information to be provided to the field.

The DOJ stresses the importance of public-safety and private-sector participants to the fusion centers because they collect and generate critical information, including risk and threat assessments and suspicious-activity reports that may be merged with the criminal intelligence already available. The public-

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

safety and private-sector agencies also offer a pool of available subject-matter experts whose talents may be particularly helpful with threat identification. The DOJ recommends that the fusion centers should be organized at the state level at a minimum, and should be designed to encompass all levels and entities of government as well as the public and private sectors,. The composition of the center's participants may vary across jurisdictions, but each should have a core criminal-intelligence component. To help meet these requirements, the DOJ compiled a non-exclusive list of "functional categories" – such as, for example, agriculture, banking, water, hazardous materials, energy, and health services as well as public works and transportation.

Privacy Concerns & Mandatory Safeguards

The DOJ further recommends that public-safety and private-sector data be virtually fused with law-enforcement information through networking (with the help of a search component). Federal, state, tribal, and local agencies should be able to access information about and available from current fusion centers, other criminal-intelligence units, and operations agencies working through a secure portal (www.ncirc.com) operated by the National Criminal Intelligence Resource Center (NCIRC), an agency sponsored by the Department of Justice's Bureau of Justice Assistance (BJA).

Because of privacy concerns, it is important to note, the fusion centers will not combine any of the personal information contained in federal databases with similar types of information in state, local, and/or tribal databases. Rather, should there be a threat, a criminal-activity "predicate," or a public-safety need, the necessary information will be compiled, analyzed, and shared by federal, state, local, and tribal representatives at the fusion center, who will access their respective proprietary databases. The final intelligence product in this case, according to the DOJ, will be safeguarded by the "entity taking action in accordance with any applicable fusion-center and/or department policy, including state and federal privacy laws and requirements."

About five years ago – i.e., circa 2004 and 2005 – the DOJ also reports, numerous states created fusion centers, using federal, state, and local funds. However, because there was a lack of standards at that time to address cooperation and communication concerns between the centers, most of them became repositories of information rather than the active vehicles needed to exchange information. At least partly for that reason, the DOJ later formed a Law Enforcement Intelligence Fusion Center Focus Group (FCFG) to help remedy the problem.

DHS and Focus-Group Contributions

Meanwhile, the U.S. Department of Homeland Security (DHS) had also been working – through its Homeland Security Advisory Council's Intelligence and Information-Sharing Working Group – on the development of guidelines for collecting, analyzing, and sharing intelligence information related to terrorism. It was through the combined efforts of the two departments that the initial *Fusion Center Guidelines* were developed and published. Two additional focus groups (FGs) were then created – the Public Safety FCFG and the Private Sector FCFG – to compile the respective guidelines needed by these key fusion-center participants.

The various focus groups that had been formed included members representing federal, state, and local law-enforcement agencies; other public-safety agencies; members of the private sector; actively operating fusion-center members; and members of national public-safety, law-enforcement, and private-sector professional organizations. Today, the Guidelines offer a uniform way to establish and operate the fusion centers both to maximize interagency coordination and cooperation while at the same time improving anti-crime and counterterrorism operations.

In October 2007, President George W. Bush spelled out, in a "National Strategy for Information Sharing," his administration's plan for an integrated national system of fusion centers. To support that plan, both DHS and the FBI provided staff to the fusion centers. There are now 70 such centers throughout the United States, and DHS Secretary Janet Napolitano last week described them as a "top priority" in the Obama Administration's own anti-terrorism strategy.

Back to the State of Maine

Maine's fusion center, officially known as the Maine Information and Analysis Center (MIAC), was established in December 2006 and today represents a collaborative effort between the Maine State Police, the Maine Emergency Management Agency, and the U.S. Department of Homeland Security whereby terrorism intelligence is collected, analyzed, and shared with appropriate entities at all levels of government. The MIAC also plays an active role in border protection.

Maine's fusion center operates a 24-hour toll-free hotline, along with a confidential online portal to report "suspicious activity." A dedicated advisory board oversees the MIAC's activities and also serves as a civil-liberties watchdog. Interestingly, it was the Washington Threat and Analysis Center (official name of the Washington, D.C., fusion center) that flagged the dirty bomb case

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

in Belfast, Maine, following up on information developed about potential threats to the then-ongoing presidential inauguration.

If nothing else, the incidents described earlier are a continuing reminder that, when confronting homeland-security threats, such traditional (but not necessarily wise) sayings as "not in my back yard" and "let well enough alone" do not, and should not, apply to terrorists and extremists. These are dangerous and unwanted guests. In rural settings, law-enforcement professionals and other first responders, as well as local residents, must challenge yesterday's culture by actively looking for things that seem "out of place" – specifically including suspicious activity and unusual behavior. Seemingly innocuous observations may be of critical value in a later investigation. Information of interest should therefore be carefully observed, reported, documented, analyzed, and shared by appropriate police and intelligence officials. Creating a police-community partnership is paramount in fostering the accumulation of critical intelligence and the mitigation of potential threats to national security. Seen in that context, the development of fusion centers in back yards nationwide is obviously a major step in the right direction.

For additional information

About the Belfast, Maine, "dirty bomb" incident, see http://www.bangordailynews.com/detail/99263.html;

or http://wikileaks.org/leak/dc-sec-08-0116.pdf

About the Maine connection to the 11 September 2001 terrorist attacks, see http://www.9-11commission.gov/report/911Report.pdf

About the Earth Liberation Front, see http://en.wikipedia.org/wiki/Timeline_of_Earth_Liberation_Front_actions

About the Animal Liberation Front, see http://www.ainfos.ca/02/dec/ainfos00587.html

About Fusion Centers in general, see http://www.it.ojp.gov/default.aspx?area=nationalInitiatives&page=1181

Lieutenant Brian T. McDonough of the Maine State Police's Criminal Investigation Division I assisted in the preparation of this article.

Jonathan A. Dudek, PH.D., is senior vice president, Forensic and Behavioral Science Services, and deputy director, Investigations, at Executive Action LLC. A highly respected forensic psychologist and published author, he also provides consultation services to investigators of high-profile criminal cases involving sexually violent and/or deviant behavior. His pioneering sexual-homicide research for the FBI has earned him international honors. Dr. Dudek also provides a broad spectrum of risk-assessment and mitigation strategies to corporate, public-safety, and government-agency clients.

Emergency Services Credentialing: FEMA Leads the Way

By Kay C. Goss, Emergency Management

The National Capital Region (NCR) Coordination Office of the Federal Emergency Management Agency (FEMA) has completed a major initiative to develop a "smart" identity-card system for emergency responders that gives first responders from agencies and organizations throughout the region the ability to quickly and easily gain access to government buildings and other federal properties in times of disaster. The initiative also is designed to remedy access problems such as those encountered by state and local emergency officials responding to the 11 September 2001 attack on the Pentagon.

FEMA not only played the key role in developing the system but also was quick off the mark in using it to meet its own credentialing requirements. The agency is working hard in providing professional credentialing not only for its own response employees but also for its Disaster Reserve Workforce employees. The latter has 23 major cadres for deployment during disasters officially declared by the President.

A Viviv WFID Multi-Agency Demonstration

In February 2006, NCR coordinated a multi-agency demonstration to test the interoperability and usability of its credentialing model through simulated emergency incidents at federal, state, and local facilities – including the Pentagon, a Virginia state facility, a port controlled by the State of Maryland, and a checkpoint in a Maryland county.

What was called the Winter Fox Interoperability Demonstration was conducted by NCR officials and hosted by the Pentagon Force Protection Agency, the State of Maryland, and the Commonwealth of Virginia.

Approximately 500 First Responder Authentication Credential (FRACs) cards were issued to senior federal, state, and county public-safety officials for the demonstration. The smart identity cards, which were FIPS-compliant – i.e., they met the standards postulated in Federal Information Processing Standard 201 – enabled the users to electronically validate their identities so that security personnel could make informed decisions for granting or denying access. Standardized electronic-identity verification was required for various levels

of perimeter security at all demonstration sites regardless of agency affiliation.

WFID also validated the ability of participating agencies to use the FIPS 201 architecture to electronically validate NIMS (National Incident Management System) and/or NIPP (National Infrastructure Protection Plan) personnel qualification information, which was needed to facilitate the incident-management capabilities of human resource assets. For example, incident commanders requiring a certain emergency support function, or sector qualification, could readily determine if anyone at the scene met the requirements needed.

FRACs also assist incident commanders in preparing after-action reports and assessments by enabling them to electronically reconstruct the time and attendance of each individual within the incident area upon both entry and departure. These reports are electronically transmitted, in real time, via satellite communications to national, state, and local emergency operations centers – including the Northern Command Headquarters (NORTHCOM) in Colorado, the Pentagon's Emergency Operations Center, the NORTHCOM/NCR Joint Operations Center, and the Maryland Emergency Management Agency.

FRACs also assist incident commanders in preparing after-action reports and assessments by enabling them to electronically reconstruct the time and attendance of each individual within the incident area upon both entry and departure

The FRACs are now a performance measure in NCR exercises, which require full implementation and integration by emergency officials throughout the National Capital Region to identify those responding to incidents at a large number of previously designated federal, state, local, and private-sector facilities.

Major Roles Played by ANSI & Virginia Commonwealth

The Governor's Office of Commonwealth Preparedness in Virginia, the first statewide effort, is moving smartly forward throughout the commonwealth on its own credentialing project. Mike McAlister, the director of that project, is becoming known nationally for his knowledge and expertise in this arena, which is a key element in Virginia's vigorous efforts to plan ahead to ensure the safety and security of over a thousand critical infrastructures.

Colorado is another state in which the initial credentialing efforts are moving forward expeditiously. Its program, known for a few days as CRAC (the "C" standing for Colorado, of course), brought too many smiles along the emergency-services grapevine so the acronym was changed to COFRAC and under that name enables interoperable credential-validation technology to support the rollout of the Colorado First Responder Authentication Credential (COFRAC) Bridge.

The COFRAC standard was created by the State of Colorado as a quick and effective way to validate the identity and personal/professional attributes of those who are required or volunteer to respond to any hazard. Through the COFRAC Bridge, all of the state's first responders' personal attributes, qualifications, and access privileges will now be aggregated, allowing for full interoperability of the credentialing project throughout the state.

Previously, according to Colorado's Office of Information Technology, the state had several disparate systems in place for validating first responders' identities, but no fully established and promulgated credentialing standards or policies. The new system enables first responders to move seamlessly throughout Colorado and gives incident commanders the ability to know exactly who they have on the scene and what skill sets they possess.

The American National Standards Institute (ANSI) also is working at the national level to incorporate the private sector into an effective credentialing process by using systems similar to the interoperable FIPS-201 credential-validation technology to give public-sector organizations the ability to control access to future disaster sites. In short, at all levels of government, the new credentialing capabilities will be critical to mounting an effective response to and recovery from emergencies of any type that require the support not only of various federal, state, and local agencies but also from a number of private-sector organizations as well.

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.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

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

Important Safety Information

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

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

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

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

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

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

DuoDote™ AUTO-INJECTOR

(atropine and pralidoxime chloride injection)

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

Sterile solutions for intramuscular use only

FOR USE IN NERVE AGENT AND INSECTICIDE POISONING ONLY

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

INDICATIONS AND USAGE

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

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

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

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

CONTRAINDICATIONS

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

WARNINGS

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

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

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

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

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

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

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

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

PRECAUTIONS

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

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

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

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

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

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

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

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

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

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

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

Pregnancy:

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

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

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

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

ADVERSE REACTIONS

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

Atropine

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

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

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

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

Pralidoxime Chloride

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

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

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

Atropine and Pralidoxime Chloride

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

OVERDOSAGE

Symptoms:

Atropine

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

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

Pralidoxime

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

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

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

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

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

MERIDIAN MEDICAL TECHNOLOGIES™

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

Qualifications, Credentials, and a Need for Speed

By Glen Rudner, Fire/HazMat

Since the mid-1990s, the U.S. emergency-response community has been increasingly frustrated by the difficulties involved in coordinating operational security when first responders from a number of disparate agencies respond to large-scale incidents. The ability to bring multiple jurisdictions and agencies to the incident scene has been stymied primarily by the lack of a common system for the credentialing of personnel. The need for credentialing is important both to ensure operational security at the incident scene and to facilitate coordination and cooperation in response and recovery operations – which is best achieved by ensuring that all responders on the scene possess valid identification and have had the training needed to carry out their various responsibilities.

The competence and proficiency of individual responders must be certified by a common credentialing process that encompasses, among other things: (a) an objective evaluation and documentation of each individual's current certification, license, or degree; (b) certification that that same individual possesses the training, competence, and proficiency needed to carry out his/her assigned tasks; and (c) demonstrable proof that he/she has demonstrated the ability to meet nationally accepted regulatory rules and standards.

The achievement and certification of these requirements has been simplified by the Department of Homeland Security to some extent by the development and promulgation of a list of regulations and standards that are now accepted as the "Gold Standard" for the training of responders. The individuals receiving such DHS-approved credentials should be able to provide assigned services and/or functions based on mission assignment by the authority having jurisdiction (AHJ) at the scene of a specific incident.

To provide the appropriate level of OPSEC (operational security) required, each person carrying the credentials should, in addition, have had a background check completed certifying his/her ability to support the level of proficiency needed to carry out the duties and functions assigned by the AHJ.

Reasonable Standards And Essential Qualifications

The Holy Grail of the nationwide credentialing system – a fundamental component of the National Incident Management System (NIMS) – is a system that documents the minimal professional qualifications, certifications, training, and educational requirements that meet the baseline criteria of the skills reasonably expected of emergency responders and volunteers eligible for short or no-notice deployment to major incidents and events. The principal goal of a national credentialing system is to objectively verify the identity and qualifications of emergency responders, but the system also can and should be used to help prevent unauthorized (i.e., self-dispatched or unqualified) personnel access to an incident site.

To support the credentialing initiative, the National Integration Center (NIC) has developed several working groups that will designate not only the positions that should be credentialed but also the qualifications, certification, training, and educational requirements for each position. The working groups are focused primarily but not exclusively on the following disciplines: incident management; emergency medical services; firefighting and hazardous materials response; law enforcement; public health/medical needs; public works; and search & rescue operations.

In addition to these discipline groups, the NIC is working with other organizations to help in the development of credentialing standards for the disciplines they represent – the Telecommunication Emergency Response Taskforce (TERT), for example, and the Citizen Corps. The subject-matter experts for the working groups have already been identified by the NIC,

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

which also is working on the development of the documents needed to meet the credentialing and identification parameters established. (The graph accompanying this article illustrates the recommended credentialing process.)

Emergency responders have provided mutual aid to neighboring communities for many years whenever a local system was overwhelmed. Today's national landscape offers several new challenges, though – as well as the probable need for communities to seek help of various types from emergency-response organizations across the nation. The scarcity of certain specialized emergency-response assets, moreover, will undoubtedly put additional demands on the nation's emergency-response communities. When completed and fully operational, the national credentialing system will provide timely identification of personnel from the field to the national level. Moreover, the development and full implementation of a national credentialing database will give incident commanders, emergency managers, and EOC (emergency operation center) directors a way to quickly and accurately identify qualified emergency responders throughout their localities, in neighboring states, and across the nation as a whole.

Having a national credentialing program in place also would ensure minimum standards of training and operational competencies, and serve as a common scope of practice for all response agencies. National credentialing – implemented prior to a catastrophic incident – also will enable efficient and effective emergency operations and facilitate the sharing of duties and responsibilities of emergency responders across all boundaries without concern about the level of training of the responders – both paid and volunteers. The credentialing system also could be used to provide clear legal protections for emergency responders, employers of the responders, and victims of the disaster by clearly defining the scope of actions for which the various groups of responders have been trained.

Aligning the goals of all response agencies responsible and planning for disaster mitigation will produce an effective and efficient emergency-responder program that may be utilized by other disciplines to prepare their own disaster-response plans. Requiring that a credentialing program be an essential component of disaster-preparedness planning would serve as the foundation and initial building block of a true national preparedness strategy.

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

National Recovery Doctrine: The Next Preparedness Frontier

By Dennis R. Schrader, Viewpoint

A recent (14 May 2009) Heritage Foundation Lecture – "Unfinished Business at FEMA" – made the case that the development of recovery doctrine should be a key priority of the Federal Emergency Management Agency (FEMA). The past decade has highlighted the turmoil that occurs, after response operations reach their closing stages, during the recovery phase of a serious disaster. Claire Rubin, author of *The History of Emergency Management: 1900-2005* (Public Enterprise Risk Institute, 2007), and Ted Steinberg, author of *Acts of God* (Oxford University Press, 2000), have documented the phenomenon effectively in those books.

The stakes are high for politicians who are not prepared to play their roles effectively. The range of potential hazards is daunting and 24x7 news coverage brings the recovery operations into the nation's living rooms. Public-safety personnel and first responders get the job done during the response phase of an incident, but they must also be both able and willing to pass the responsibility to others when the recovery begins.

The restoration of housing, infrastructure resilience, and business continuity is the key to recovery from a catastrophic disaster. Land development, engineering, and project management – an umbrella term that includes zoning, design and construction codes, building permits, and both civil and environmental engineering – are the core issues involved in recovery operations. The management of the recovery is fundamentally a state, local, and private-sector responsibility. FEMA itself is not organized, resourced, or trained to lead and/or direct recovery operations, nor does it have a surplus pool of dedicated CBRNE (chemical, biological, radiological, nuclear, and explosives) personnel waiting in the wings to carry out those tasks.

A Logical Distribution Of Roles and Responsibilities

State and local elected officials must therefore lead and direct most if not quite all recovery efforts. States are usually in charge of large-scale recovery operations and for that reason should incorporate a disaster-housing plan in their HUD (the federal Department of Housing and Urban Development) Community Development Block Grant programs. Guidance is

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

available, though, from the DHS/FEMA-developed National Housing Strategy, which was written in 2008 with the expectation that state housing plans would drive recovery preparedness, with DHS/FEMA retaining the responsibility of developing a National Recovery Doctrine.

Local governments generally have responsibility for such inter-related matters as zoning, building codes, environmental systems, and local housing programs. However, as Steinberg points out in *Acts of God*, local control of development can either contribute to increased risk or, on the other hand, can mitigate losses and help create more resilient communities.

FEMA itself is not organized, resourced, or trained to lead and/or direct recovery operations, nor does it have a surplus pool of dedicated CBRNE personnel waiting in the wings to carry out those tasks

Business continuity and supply-chain resilience are vital to short- and long-term recovery operations. Maintaining or restoring the infrastructure and ensuring building resilience are the keys to an effective recovery strategy. In fact, the American Society of Civil Engineers (ASCE) has established specific initiatives to focus attention on the nation's infrastructure and recovery capabilities, and the ASCE infrastructure "report card" includes a wealth of data on the condition of the nation's infrastructure.

A recent report – *Policies That States Need to Recover from Disasters* – developed by the U.S. Chamber of Commerce-Business Civic Leadership Center identified 10 policies, several of them focused on private-sector coordination, which states could use to more effectively recover from a disaster.

Reasonable Expectations & a Ticking Clock

Effective national doctrine would clarify the private-sector roles of post-disaster recovery for engineers – as well as housing, healthcare, and many other professionals – who play key roles in the recovery process.

In December 2008, the White House-led Homeland Security Council initiated a Disaster Recovery White Paper process to define the scope and organization of an initiative to develop a consensus National Recovery Doctrine that would assign the specific roles and responsibilities for federal interagency, state and local, and private-sector entities. The DHS/FEMA Preparedness Directorate has been assigned the responsibility of documenting the process – working in coordination with the DHS Office of Infrastructure Protection and with other DHS/FEMA divisions responsible for mitigation and long-term recovery operations. As with the National Response Framework (NRF), the success of this effort also requires the significant involvement of state, local, and private-sector interests as well as the DHS/FEMA National Advisory Council (NAC).

There are several private-sector organizations that can provide input to the process. They include but are not limited to the Disaster Recovery Institute (DRI), the Urban Land Institute (ULI), the Urban Institute (UI), and the National Governors Association (NGA).

Emergency managers and other working professionals seem to agree that the National Recovery Doctrine must be finished soon – in any event, well *before* the next major disaster occurs. Various polls and surveys suggest, moreover, that the public at large will not accept anything less. Over the past decade the American people have become much more knowledgeable about reasonable expectations, and experts in the field of recovery operations know that the clock is ticking.

For additional information

The Heritage lecture [by Dennis R. Schrader, author of the preceding article],
see http://www.heritage.org/press/events/ev051409a.cfm

The infrastructure report card,
see http://www.infrastructurereportcard.org

The engineer's role in emergency management,
see http://ciasce.asce.org/podcast/engineersrole

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. A licensed professional engineer in the State of Minnesota, he holds a bachelor of arts degree, with a focus in engineering, from Kettering University, and a master's degree from the State University of New York at Buffalo. While on active duty as a Navy Civil Engineer Corps officer he served overseas tours in Guam, Diego Garcia, and Sicily. He also has served on numerous homeland-security committees, including the Anti-Terrorism Advisory Council of Maryland and the Homeland Security Senior Policy Group.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

Most Biohazard Detection Systems Come with a 20% Error Rate

Shouldn't You Be More than 80% Prepared for an Attack?

Instruments using antibody-based detection are less reliable because of their high false negative rate. Their results need to be verified at a separate lab using PCR. Idaho Technology's portable biohazard detection system, the RAZOR® EX utilizes the same PCR technology that health labs use without a need for in-depth knowledge of the science behind it. The RAZOR EX was made for HazMat and first responder teams that require more from a detection system.

The RAZOR EX is a complete product solution that is easy to setup, run, and read. Capable of testing ten bioterrorism agents in one run, the RAZOR EX provides more accurate results than other products in less then 30 minutes.

Visit our web site or call today and let us help you get the most trusted and accurate field portable detection system into the hands of your team.

Turn Your False Negatives Into Cash

Idaho Technology has many ways to help you get the best products for your team. For example, take advantage of our trade-in program by giving us your inferior antibody based detection system for cash towards the purchase of our more reliable PCR based detection system.

The RAZOR® EX with rugged carrying case

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**

Evolution of an Acronym

EMS: Increased Emphasis on the Medical Aspect

By Joseph Cahill, EMS

The name Emergency Medical Services or EMS was adopted as part of a strategy to shift ambulances slightly out of the transportation field and much more into the field of emergency *medical* care, both in the public consciousness and in the mindset of the nation's medical and healthcare communities.

The increased emphasis on medical responsibilities is symbolic of the goal of further professionalizing the ambulance service and staff, and is intended not only to put greater emphasis on the emergency nature of the service but also to emphasis the medical aspect – in other words, to reinforce the fact that what EMS professionals provide is more than transportation per se; they usually also represent, in fact, the first stage of medical treatment provided to victims during and after an accident or emergency.

Moreover, as EMS continues to move into the future its progress will be marked by new interactions between the paramedic in the street and the medical staff in the emergency room (ER) of a hospital or other healthcare facility. In the early days of EMS, paramedics were required to contact a hospital for approval of their care plan. That requirement is still valid to some degree, but the scope of treatments available under the paramedic's discretion has continuously expanded. (There still are, however, some treatments that cannot be provided in an ambulance, either because of logistics and/or space limitations, or because of the medical risks involved.)

A heart attack occurs when the blood flow to the muscle of the heart is interrupted – often, but not always, by a blood clot getting stuck in an artery. In certain types of heart attacks the clot could be removed by a procedure called cardiac catheterization – more formally described as percutaneous coronary intervention (PCI).

From the first moment an EMS professional is on the scene of an accident or incident, he or she is collecting information, both by interviewing the patient and by measuring the patient's heart functions. This is standard practice throughout the country, and in areas where paramedics are available they usually employ a large and increasing variety of advanced technologies and systems – e.g., a 12-lead electrocardiogram (EKG).

Today, cities such as Los Angeles, California, and Louisville, Kentucky, are harnessing the power of their highly trained EMS staffs to improve cardiac care. In those cities, and many others, the paramedic quickly transmits the information he/she has gathered at the scene, or while en route to the hospital's emergency room; the ER, in turn, activates a cardiac care team, the members of which receive the patient and provide emergency cardiac care.

Unfortunately, not all U.S. hospitals have PCI capabilities available at all times, or are able to quickly get a team in place. However, the system provides a two-way flow of information, therefore – in addition to warning the hospital that it can scramble the cardiac team – specific PCI centers are designated in advance so that the paramedic can make the hospital selection knowing that the best treatment for *this* specific type of heart attack is available at *this* specific hospital.

The goal, of course, is to reduce the time-to-treatment for the patient and thereby improve outcomes by decreasing the damage done to the heart.

Thanks in large part to this new and still evolving system, EMS is moving from strictly a transportation service – with a modicum of emergency medicine thrown in – to a larger and more active component of a more comprehensive overall medical system. As the current EMS system continues to mature and evolve its model will undoubtedly affect system design in the future.

Not incidentally, the decreases in wait time for medical treatment not only save lives but also enhance them, because the treatment provided on the scene and/or on the way to the hospital often means the difference between a life in which shortness of breath and overall weakness are constant companions and a much better life – one without those debilitating symptoms.

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.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

IDGA
Institute for Defense and Government Advancement
presents a training conference:

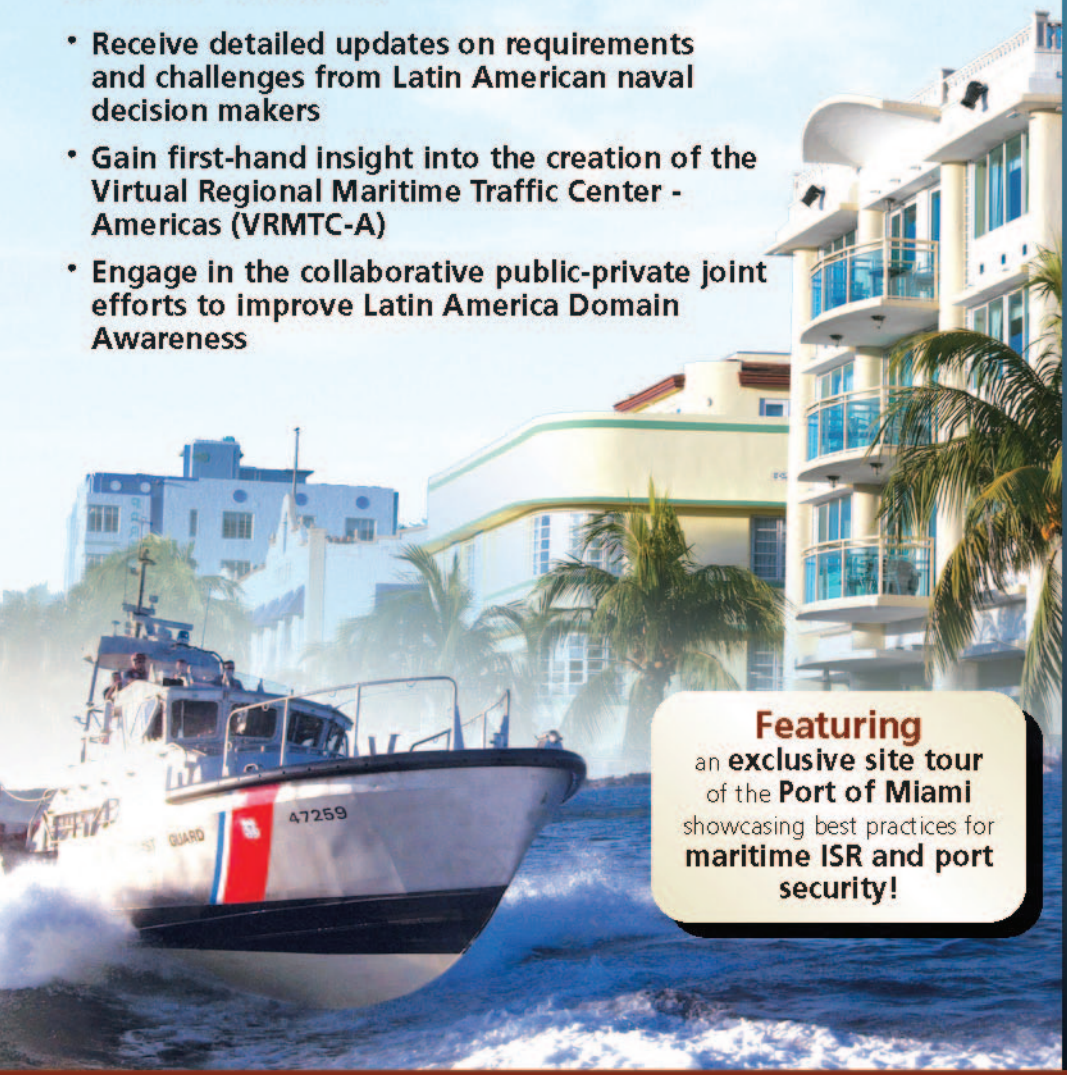
MARITIME SURVEILLANCE LATIN AMERICA™

Creating Partnerships in Latin American Maritime Domain Awareness

October 26 – 28, 2009
Miami, FL

DON'T MISS YOUR BEST OPPORTUNITY OF THE YEAR TO:

- Receive detailed updates on requirements and challenges from Latin American naval decision makers
- Gain first-hand insight into the creation of the Virtual Regional Maritime Traffic Center - Americas (VRMTC-A)
- Engage in the collaborative public-private joint efforts to improve Latin America Domain Awareness



Featuring
an **exclusive site tour** of the **Port of Miami** showcasing best practices for **maritime ISR and port security!**

Register Early & SAVE!

FEATURING A DISTINGUISHED SPEAKER FACULTY THAT INCLUDES

Brig Gen David Fadok, USAF
Director for Policy & Strategy, US SOUTHCOM

CT Valter Citavicius Filho
Commander Brazilian Navy (Marinha do Brasil)

Cdre Gary Best, MSM
Chief of Defence, Guyana Coast Guard

CDR Fran Cloe, USN
OGMSA Latin American Outreach & Coordination

CDR David Edwards, USN
MARLU-LATAM SOUTHCOM

CAPT Fernando Zamudio
Capitán de Navío, Perú (Peruvian Navy)

Bill Johnson
Executive Director, Port of Miami

Ted J. Venable
COMUSNAVSO/COMFOURTHFLT, CNT Program Manager

Guy Thomas
Science and Technology Advisor, Global Maritime Awareness, OGMSA

WWW.MARITIMELATAM.COM

Responding to Incidents in a Neighboring Port

By Corey Ranslem, Coast Guard

The port is one of the more challenging – i.e., dangerous – work environments in countries throughout the world. The goal of each port is to move cargo and passengers in and out as efficiently and safely as possible. By their very nature, ports present unique challenges for law-enforcement and fire-rescue agencies from concurrent jurisdictions. Most of the larger ports within the United States have their own internal fire and police departments, but require outside assistance during mass-casualty events or other major disasters. Those critical resources will almost always come from the police and fire departments in cities, towns, and other jurisdictions relatively close to the ports.

Captain James Maes, USCG (Ret.), is the director of Port Services for ABS Consulting. Before working for ABS he was the Coast Guard's Captain of the Port for Sector Miami and also the director of safety and security for the Port of Miami. He points out that there are three key prerequisites to successfully responding to port incidents: (1) Developing an effective plan; (2) Testing the plan through drills and exercises; and (3) Incorporating into the plan the essential "lessons learned" from the drills and exercises. "Any plan worth having is a plan worth exercising," Maes comments. "The public-safety agencies, port tenants, and federal agencies all have different plans so it is important to exercise those plans to understand how the separate plans work together."

"The public-safety agencies, port tenants, and federal agencies all have different plans so it is important to exercise those plans to understand how the separate plans work together"

An effective emergency-response plan will not necessarily address each and every possible aspect of a particular situation, but it is nonetheless important to have a fairly comprehensive response plan in place to understand how the various agencies from neighboring jurisdictions are going to work together in the event of a true large-scale emergency. "It is also a good idea for the agencies that surround the port to become familiar with the port and maritime environment before an incident," Maes says. "Training and exercises expose responders to potential situations they may encounter during an incident. The training helps responders understand how to get out of a potentially dangerous situation."

People and Cargo – a Lethal Mix

Many ports house not only all types of cargo – including hazardous chemicals and fuel – but also handle large numbers of cruise passengers. Port Everglades in Fort Lauderdale, Florida, for example – which does handle both hazardous cargo and fuel – is the largest cruise port in the world. "There are a lot of things to consider and understand before responding to an incident in the port," says Chief Dan Cummings of the Broward County Sheriff's Office, which is responsible for law enforcement in Port Everglades. Cummings says he must always consider how the law-enforcement actions are going to affect the local community. "We shut the port down for over 12 hours" after the terrorist attacks on 11 September 2001, he recalls. However, gas stations along the Florida Turnpike "were running out of fuel, so we had a find a way to safely get fuel moving again."

Port Everglades is bordered by three different cities in Broward County – Hollywood, Fort Lauderdale, and Dania Beach. "It is important that we understand the response

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

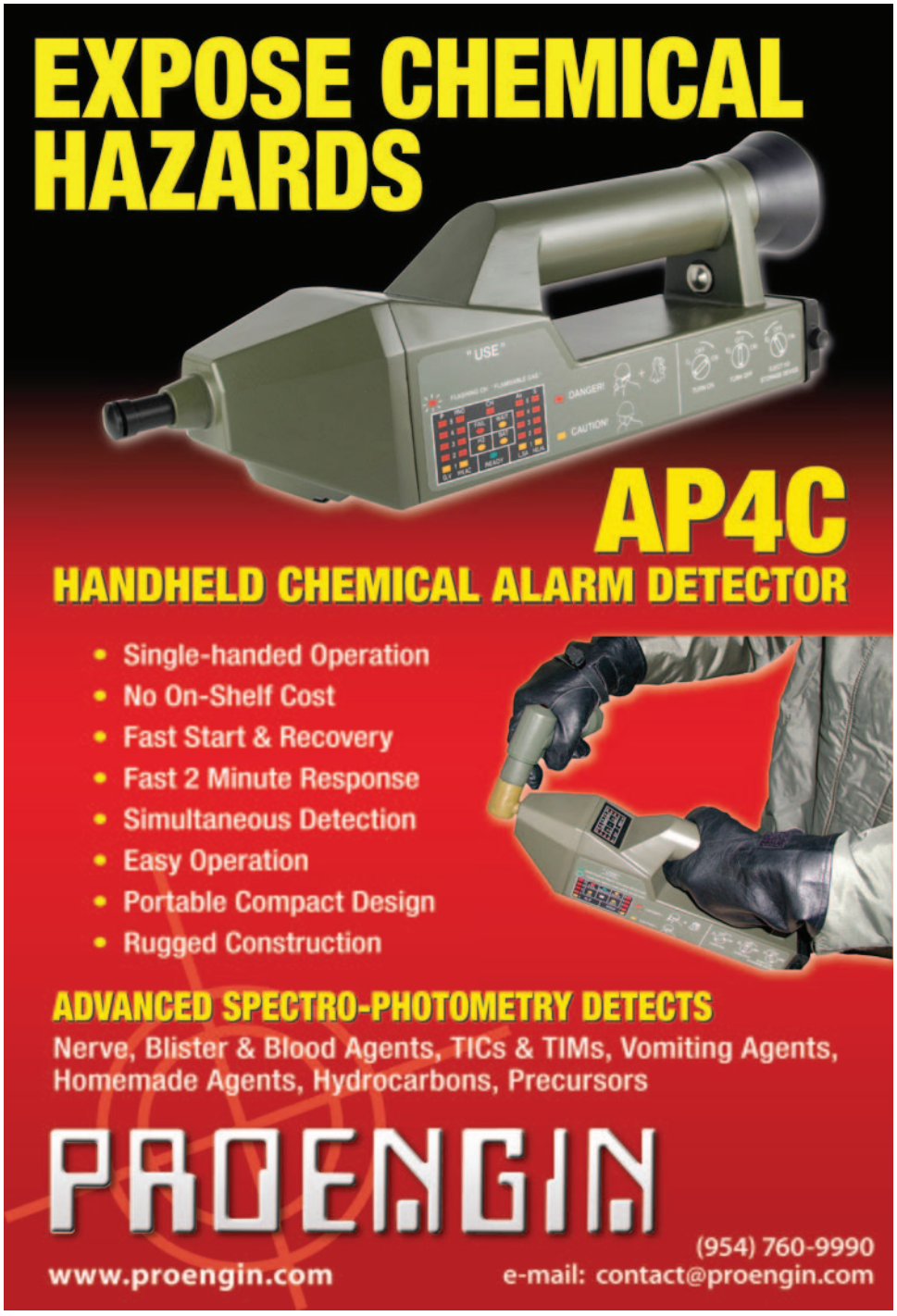
capabilities of our surrounding agencies," Cummings points out. For that reason, he continues, "We hold monthly meetings at the port with the surrounding agencies, port tenants, federal agencies, and the port director to discuss what is going on in the port." The meetings not only help in the planning process, but also serve as "a way for people from the different agencies to get to know each other."

When there is a port incident that requires help from neighboring response agencies, Cummings must immediately consider not only how to maintain the flow of people and vehicles into and outside of the port but also where to set up a large-scale staging area with a reliable official on the scene to keep track of: (a) what agencies are at the staging area; and (b) the capabilities of those agencies. "We have had incidents in the past," he points out, "with multiple agencies responding where everyone tries to get as close to the situation as possible and then leaves their vehicles in the way – blocking additional response units and [other] traffic."

Cummings and Maes agree that multi-agency planning, training, and effective communications are the keys to successfully responding to port incidents. "Training helps responders understand how the plans and people are going to work together during an actual situation," Maes says. "During any incident," Cummings adds, "it is important to establish good communication with the different responding agencies and also the news media" – which, he points out, serve as "an important link to quickly get information out to the local community."

Today, fortunately, most U.S. ports have in place, and have exercised, fairly comprehensive response plans that define the roles and capabilities of all of the agencies likely to work with one another in a large-scale incident in and/or affecting the port, but it is still important for the surrounding communities to continue to be involved in planning and training for any future incidents that might occur.

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. He holds a Bachelor's Degree in Communication and Political Science from the University of Northern Iowa, an MBA in International Business from Georgetown University, and has almost 15 years of experience in maritime law enforcement and security.



Fusion Centers & Public Health Agencies: Unlikely or Natural Partners?

By Adam Bulava, Law Enforcement

At a recent Council on Foreign Relations event held on July 29, 2009, Department of Homeland Security (DHS) Secretary Janet Napolitano touted the importance of fusion centers in "ensuring that local law enforcement has better information necessary to protect our people, our neighborhoods, [and] our infrastructure." In the aftermath of September 11, 2001, top officials in the U.S. intelligence community conceived fusion centers as a means to break down stubborn information-sharing barriers that had existed between federal, state, and local law-enforcement agencies. These barriers were reinforced by a persistent Cold War "need to know" mentality, where information is considered so precious that only those with the most immediate and obvious needs should have access to it.

Today, however, "need to share" has all but replaced "need to know" as the success of the intelligence-led policing movement has motivated law-enforcement agencies to embrace information sharing and collaboration efforts with non-traditional partners. As of July 2009, 72 fusion centers, primarily staffed by state and local law-enforcement personnel, had been stood up across the country. DHS has been tasked with assisting states in developing and operating these centers through the State and Local Fusion Center Program (SLFCP). There are also a growing number of DHS intelligence analysts (36 as of July 2009) working as federal liaisons at 28 of these centers.

Several centers are now seeking to include the fire, public health, and private sectors in the fusion process. The main benefit of this collaboration is the ability for fusion-center operators to obtain a comprehensive threat perspective by collecting and analyzing information from a wide variety of sources. One way to achieve this has been for fusion-center officials to look to state and local public-health agencies as natural partners.

Specifically, public-health personnel may have information or subject-matter expertise that can assist law-enforcement officials in their investigation of bioterrorism threats as well as naturally occurring diseases. The 2008 ricin investigation in Las Vegas, the December 2008 white-powder mailings to several state governors' offices, and the 2009 H1N1 influenza outbreak all illustrate the important role that public-health agencies play in preparedness and response efforts as well as law-enforcement investigations. Fusion-center and public-health officials are beginning to recognize the value of cooperation and are establishing formal information-sharing arrangements. For example, some fusion centers staff public health personnel, while others share access to information databases or hold regular meetings to discuss emerging threats or issues of concern.

Fusion-center and public-health officials are beginning to recognize the value of cooperation and formal information-sharing arrangements; some fusion centers staff public health personnel, while others share access to information databases or hold regular meetings to discuss emerging threats

Common Challenges In Collaboration Efforts

However, integrating public health into fusion-center operations, and vice versa, is a process rife with challenges. First, and unsurprisingly foremost, are budgetary constraints. Many fusion centers cannot afford to bring on additional staff members, especially ones outside normal law-enforcement functions. In addition, personnel working at fusion centers may need to obtain government security clearances, a costly and often time-consuming process.

Another major obstacle stems from culture clash. Public-health personnel may provide fusion centers with subject-matter expertise for investigations, access to public-health databases, or information regarding infected patients. However, due to law enforcement's traditional reluctance to share information with non-law enforcement entities, public-health agencies often receive little information in return (one example: information regarding developing

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

threats that may have a nexus to bioterrorism). Without this information, public-health agencies are unable to properly plan for, or exercise, such threats to their communities.

A third point: Civil liberties groups have historically raised privacy concerns over fusion-center intelligence operations, an issue that could be compounded by the sharing of public-health information. Despite these apparent challenges, there are several cases in which fusion centers and public-health entities have been able to collaborate successfully.

Successful Fusion-Center/ Public-Health Collaboration

In 2005, the Los Angeles County, California, Department of Public Health (DPH) partnered with the Federal Bureau of Investigation's (FBI) Los Angeles Field Office and the Joint Regional Intelligence Center (JRIC), the region's fusion center, to develop and launch the Weapons of Mass Destruction (WMD) Technical Advisory Group (TAG). The group serves as an early detection mechanism for public-health and law-enforcement personnel to share and mutually assess health and medical information that may have a nexus to terrorism or may suggest an emerging terror threat. The TAG is composed of DPH medical and epidemiological experts as well as FBI and JRIC personnel. The group activates as needed to assess health-related threats and to initiate joint DPH-FBI investigations, if warranted.

In addition, DPH has detailed public-health staff members to the JRIC to function as public-health WMD intelligence analysts. These individuals alert the TAG of developing health threats and provide the TAG with relevant information and intelligence. The analysts also serve as direct points of contact for DPH personnel when contacting the JRIC. To date, the TAG has proved invaluable for the timely investigation of potential threats to the Los Angeles area.

In early 2007, the Palm Beach County, Florida, Sheriff's Office initiated the development of the South Florida Virtual Fusion Center (SFVFC) to serve as a collaborative workspace for law-enforcement, public-health, fire, and other emergency-response personnel. In April 2009, personnel from the Miami-Dade Police Department created a subpage on the SFVFC specific to the emerging H1N1 influenza threat. The page contained news feeds from the state health department, links to CDC (Centers for Disease Control and Prevention) and HHS (Department of Health and Human Services) information, national and local outbreak statistics by location, and information on pandemic influenza preparedness and safety measures. Public-health, law-enforcement, fire, and emergency-management personnel accessed the page and uploaded their own relevant content. The page served as a valuable resource for up-to-date information on the outbreak and helped local agencies prepare for the threat in their own jurisdictions.

The Way Forward: Overcoming Obstacles to Collaboration

The previous examples demonstrate some of the ways in which public-health departments and fusion centers can benefit from keeping a close and open relationship. DHS has been promoting such a relationship with the recent creation of the Health Security Intelligence Enterprise (HSIE), an initiative aimed at integrating public-health and healthcare-community interests into the process of homeland-security information and intelligence exchange. The goal of the HSIE is to enhance the preparedness level of public-health practitioners across the country while supporting an all-hazards approach to prevention, protection, response, and recovery.

One of the ways that DHS hopes to achieve this is through hosting workshops similar to the Health Security Intelligence Workshop, held in October 2008 in Denver, which brought together over 150 public-health, homeland-security, and intelligence personnel to discuss methods for improving information sharing and collaboration. While these efforts, combined with the work of a handful of fusion centers, indicate promise, there is still a long road ahead for achieving the level of integration sought by proponents of a "need to share" intelligence framework.

Adam Bulava, a researcher for the Lessons Learned Information Sharing system of the Department of Homeland Security's Federal Emergency Management Agency, collects and analyzes information received from federal, state, and local agencies and organizations involved in homeland-security and emergency-preparedness initiatives, and combines his research data with critical knowledge received from subject-matter experts to create original LLIS.gov content. His principal research expertise on the LLIS program is in the area of intelligence and information sharing, with a particular focus on fusion centers and their development. Prior to joining the LLIS.gov team, Bulava served as a policy associate for Business Executives for National Security (BENS), where he focused primarily on intelligence-community issues. He holds a bachelor's degree from The George Washington University, where he concentrated in counterterrorism and transnational security threats.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

Managing the SNS Stockpile: A Case Study

By Joseph Cahill, Case Studies

In June, responding to the continuing international spread of the Influenza A H1N1 flu outbreak, the World Health Organization (WHO) raised the global pandemic alert warning system to its highest level, Phase 6 – which indicates that the human-to-human transmission and ongoing community-level H1N1outbreaks have been confirmed and are now worldwide. The WHO announcement was intended to signal public-health officials in every country in the world to step up their efforts in dealing with the disease. By then, many U.S. states had been affected, making it necessary to execute emergency-response plans that had been in place and exercised for years.

H1N1 is both widespread and emergent, but the responses required are beyond the day-to-day capabilities of the medical community of any nation. In the United States, a Strategic National Stockpile (SNS) was created to deal with just this type of situation. The SNS is a federally controlled cache of vaccines, pharmaceuticals, and other medical supplies and equipment that can be activated in the event of a national emergency. The stockpile represents both a real – i.e., material – asset in a federal warehouse and a virtual VMI (Vendor Manager Inventory) asset. In SNS terms, VMI represents additional production capacity that can be quickly activated to meet the country's needs during a crisis.

The SNS is managed, and the vaccines and pharmaceuticals distributed, by the U.S. Centers for Disease Control & Prevention (CDC). When the deployment and distribution of vaccines, pharmaceuticals, and/or other medical supplies is necessary, the CDC pushes critical inventory from the SNS to the states needing those supplies. Potentially that could mean all 50 states – more when U.S. territories are included – but it is usually far fewer because most threats to public health tend to be regionalized. The states in turn pass the inventory items to the local level – an umbrella term that includes counties, cities or towns, hospitals, and clinics. In turn, the public-health working professionals on the front line dispense the supplies to individual patients – here the potential number could be in the tens of thousands.

In its fight against H1N1, the CDC authorized the shipment of 25 percent of the SNS medical-materials inventory to those states with already documented H1N1 cases. Following this action on the part of the federal government, many states – Ohio and Tennessee are among the most prominent examples – recently put their own SNS distribution strategies (planned from the tabletop, tested, optimized by implementing the lessons learned, and worked out in full-scale disaster-preparedness exercises) to the ultimate real-world test.

Needed: A Faster and More Flexible Multipurpose System

In the first few years following the creation and gradual buildup of the SNS, Ohio and Tennessee, like many other states, used a flat-file spreadsheet to keep an inventory of: (a) the state-owned materials already on hand; and (b) those provided by the CDC. The principal advantages of this system were the ease with which the file could be created and the speed with which it could be used locally. The principal disadvantage was that it worked only on a small scale: Only one person at a time could use the information available.

Prior to actually having to use the SNS in a real-life situation, both Ohio and Tennessee looked for a better system that could store the data centrally so that many users could access it at the same time. With a system of that type available, an emergency manager could view up-to-the-moment data and use it in his or her decision making. Moreover, the personnel assigned to handle the SNS shipments could incorporate shipping and receiving data in near to real-time. (Here it should be noted that, after federal SNS assets are deployed, they become state assets, and the states would then have total responsibility for inventory accuracy and control over the materials acquired from the national stockpile.)

Although there are a number of commercial products and systems available for the purpose of inventory management, few are intended to support SNS distribution requirements. Ohio and Tennessee selected a commercial inventory-control software platform – called the Inventory Resource Management System (IRMS) – that uses a module designed specifically for SNS distribution. Developed by Upp Technology Inc., IRMS is based on a warehouse inventory-control platform that allows states to use the software not only in their day-to-day warehouse and storage operations but also, in an emergency or crisis situation, to receive, stage, store, and track inventory received from the SNS.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

The Ohio plan calls for distribution from the CDC to a central RSS (receive, stage, and store) warehouse. Materials taken from the RSS are apportioned to eight distribution nodes strategically prepositioned throughout the state; the node locations are based on the population in a specific geographic area and the weather conditions there, topographical data, and other relevant information both on the ground and projected for the future. There is considerable flexibility built into the plan, moreover. For example, if the population of one affected county had increased significantly since the initial system setup, state officials could use the IRMS software to quickly recalculate the SNS apportionments planned for that county.

At the node itself, the materials shipped from the RSS warehouse are again apportioned (to a county or hospital level) and can be shipped out immediately. Ohio uses a three-person "picking team" to assemble an order for shipping: An inventory controller scans the material into the inventory database (wirelessly, and in real time); a picker picks the material from its SNS storage space; and a packer first confirms that the item is the correct one needed and then places it on the pallet being prepared. A separate quality-control process then confirms the order and applies a color-coded label, indicating the destination, to the pallet.

In combating H1N1, a decision was made at the governor's level to distribute the materials only as far as the node level and hold them there, thus eliminating the initial order fulfillment and shipping tasks. Holding the materials at the node obviously allows greater control. However, moving the materials from the RSS to the node ensures that the RSS itself is now ready to accept another 25 percent shipment from the CDC without delay. Shipping materials beyond the nodes to local users would be triggered by the exhaustion of commercially available materials on hand. Fortunately, this situation has not yet occurred.

Quantity, Quality, and Other Mandatory Virtues

In any event, the bottom line is that Ohio is now ready. And it is likely to stay ready, for the simple reason that, as Mark Keeler, the Ohio Department of Health's State SNS Coordinator, commented, "The biggest thing you can do with any system is train regularly."

Just as emergency-response agencies have tools that allow them to respond effectively, commercial warehouses have software and plans that improve their own efficiency and level of awareness. Warehousing is not just a simple matter of putting things on and taking things off trucks. There is a well defined process in place: When new inventory arrives it must be counted and recorded, stored, and tracked; as need is identified, orders are assembled and verified for fulfillment; and as they are packaged for shipping, pallets are documented in considerable detail and made ready for delivery.

When the deployment and distribution of vaccines, pharmaceuticals, and/or other medical supplies is necessary, the CDC pushes critical inventory from the SNS to the states needing those supplies

Whether in the commercial warehouse, or in the state RSS warehouse facility used by the Ohio Department of Health (ODH) in an emergency-response situation (such as that dictated by the H1N1 pandemic), getting the right material to the right place, on time – and in sufficient quantity and quality – is what matters most, particularly when those materials are items such as antiviral medications and personal protective equipment. N-95 masks, for example, which are certified by the CDC's National Institute of Occupational Safety and Health (NIOSH) as being able to block 95 percent of particles less than 0.3 microns in size (the standard for responders to a virus-based threat).

In Ohio, several state agencies provide professional staff for the RSS warehouse. Those staff members, augmented by department of health staff, are both the on-site subject-matter experts in warehousing as well as the equipment operators. During a public-health emergency, Ohio's partnership with the RSS warehouse frees up the ODH's frontline disaster-response personnel for deployment in clinical, laboratory, and epidemiological settings where their skills may be used both more efficiently and more effectively. The assignment of highly qualified professional staff to warehouse operations also decreases both the likelihood of inventory loss through breakage and the possible loss of staff members through injury.

Testing the System – And the Fortitude of Participants

The Ohio Department of Health, together with other state agencies, conducts a full-scale exercise of the state's distribution system every year. Few if any exercises, however, could come close to reality in terms of scale, in pressure, and in stress ing the system as the H1N1 outbreak did. In a very real sense, therefore, the SNS deployment made necessary by the real-life H1N1pandemic has been the best full-scale run-through of the

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

SNS process that could be conceived, testing both the timing of deliveries and the accuracy of inventory management – but without a wide-scale loss of life.

Having had a real-life event to test and evaluate the state's emergency response and preparedness software and plans, Ohio plans to test only two components of the system this year: (a) the process used by the state to request additional materials from the CDC; and (b) the processes used by local officials to request the materials from the state. None of these processes was needed during the H1N1 outbreak.

As in Ohio, Tennessee's SNS distribution plan uses a regional system for command, and for the communication of requests, that relies on a single point-of-contact model. In Ohio, local health

The future public face of an H1N1 pandemic? (Getty Images photo)

agencies make requests through their emergency-management agencies, which in turn pass the request to the state emergency management agency, which passes it to the ODH. In contrast, Tennessee operates a central state health operations center, which receives orders and reports from regional health operations centers, which use a single point of contact for ordering materials.

The systems in both states funnel orders to singular phone numbers, e-mail addresses, and fax numbers. Using multiple points of contact creates a consistent risk of some orders being recorded for the same singular need. During a disaster this could cause the waste of vital resources. In addition, using software without this discipline requires updating phone contacts (and other information) as shifts change in the operations center and in the other levels of the system.

Despite its somewhat different approach, Tennessee, too, is ready.

The Super-Bowl Philosophy – In Real-Life Emergencies

Vince Lombardi preached that, "If you practice the way you play, there should not be any difference." In accordance with this philosophy, he trained his football teams as hard as he expected them to play on game day. Dr. Paul Petersen, the SNS coordinator for the Tennessee Department of Health, carries the same philosophy to the next level by postulating that there is no special level of play required for what might be called "the big game." This approach is somewhat different from Ohio's way of thinking, but has been no less effective.

To Dr. Petersen, having a special plan in place for disaster distribution virtually guarantees that only a select few will know of the plan, and of the system designed to use it, when it matters most. For that reason, Tennessee decided to use an operational warehouse that had the material-handling equipment, warehouse personnel, and transportation resources readily available. The Tennessee approach allows for efficient distribution and tracking of medical countermeasures shipped throughout the state, using a systematic process already being practiced daily. Partnering with Upp Technologies provides the inventory-management system needed to ensure the accurate allocation and record-keeping of state assets.

The Tennessee DOH has acquired and successfully tested the skills it needs to receive, inventory, and ship SNS assets in an emergency. The state's future goal is to implement IRMS as an all-hazard solution for emergency-response inventory management and patient tracking as well as the carrying out of these same functions day-to-day in the state's health departments. By exercising the plan daily, it becomes embedded in muscle memory, and the public health and warehouse staff need only act on what has already become an almost routine situation.

When thinking about a response to a large-scale outbreak of disease – and/or coping with another incident that taxes state and local medical-community planners – public-health officials must consider the SNS and how this federal asset will be controlled, distributed, and secured at the state level. Not only because it is the responsibility of those who receive it but also, and of much greater importance, because it could be the difference between the success or failure of the overall response effort.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

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

California, Connecticut, and Texas

By Adam McLaughlin, State Homeland News

California
Focuses on Long-Term Public Safety Radio Needs & Capabilities

California's Public Safety Radio Strategic Planning Committee (PSRSPC), composed primarily of the state's emergency responders, has initiated the strategic planning process needed to develop and build a statewide interoperable communications network that would allow PSRSPC members to communicate not only with one another but also with local, tribal, and federal partners throughout the state. Officials said at a public meeting last week that current plans call for building the network over the next 10 years.

The meeting focused both on the importance of building partnerships with local first responders and on the need to build the network from the bottom up. "We have to understand [that] while we at times are first responders, mostly we are also there to coordinate, cooperate, and work with our local partners," said Matthew Bettenhausen, acting secretary of the California Emergency Management Agency.

The state is already engaged in a major IT consolidation and officials want to ensure that the new network is built with a view toward sharing resources and assets. "It is important from a technology perspective that my organization is working to really look at those technologies that go across the state – that go across all of your state agencies – and the way that those are delivered," Teri Takai, the state's CIO, told the other attendees at the meeting. "Then, looking at the way that we do it at a state level," he continued, "to set an example for the way that we want the rest of the state to operate and the way that we want to interact with the locals."

One major hurdle the state's first responders face in trying to achieve interoperability is knowing where all components of their communications infrastructure – including radios, towers, and dispatch centers – are located. To help with that task, the U.S. Department of Homeland Security developed an organizational tool – the Communication Assets Survey and Mapping (CASM) agency – that represents the locations of those assets on a map.

"We suspect that part of this process is getting CASM fully populated," Bettenhausen said. "You can't make some of these decisions until you understand not only the assets that we own as a state and state agencies but – more importantly – what our local partners own and how we tap in and leverage those resources and to some extent the private sector as well."

The first scenario, a simulated attempt by a boat to enter the restricted waters; the second drill simulated a car accident, focused on dispatch procedures & appropriate emergency medical response needed to help a mock "victim"; the third drill simulated a telephoned bomb threat and the discovery of a "suspicious" package

Connecticut
Naval Base Carries Out Emergency Response Exercises

Practicing the procedures needed to effectively respond to threats is an important element of the force-protection plan for the U.S. Naval Submarine Base in New London, Connecticut. The base's Installation Training Team (ITT) simulated three events last month to evaluate the ability of the base to cope with threats that might evolve into mass-casualty incidents. The base, located on the east bank of the Thames River near Groton, Connecticut, occupies approximately 500 acres and has over 400 buildings to protect, along with the housing and other support facilities needed by the approximately 10,000 active-duty naval personnel, civilian workers, and Navy family members on the base at any given time.

During one scenario, emergency responders faced a simulated attempt by a boat to enter the restricted waters around the submarine piers. The second drill involved a simulated car accident and focused both on dispatch procedures and on the appropriate emergency medical response needed to help a mock "victim" who had been hit by a vehicle.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

The third of the 15 July drills simulated a telephoned bomb threat and the discovery of a "suspicious" package – contents unknown. That drill required the assistance of an Explosive Ordnance Disposal (EOD) team headquartered at the U.S. Naval Station in Newport, Rhode Island. The EOD team – Explosive Ordnance Disposal Mobile Unit Two Detachment Newport – is actually a unit of a larger EOD force based in Norfolk, Virginia. The faked bomb threat required the use of Fulton Hall, one of the older (and currently uninhabited) barracks at the Submarine Base. Equipped with full body armor and accompanied by a robot ("HD1"), the Newport EOD team followed the procedures that would normally be used to safely detonate an explosive device.

The exercise concluded with a mock media event and the simulated establishment of a Family Assistance Center (FAC). Commander Daniel Rossler, the base's executive officer, answered questions similar to those that probably would be, and are, asked at press conferences which almost automatically follow major "real-life" incidents. Members of the New London Fleet and Family Service Center, and other family-support communities at the Submarine Base, practiced the skills they would need to help Navy personnel, and members of their families, following an incident such as the bomb threat.

"This exercise, with its multiple events and its incorporation of a press conference and a FAC, had been a goal of the ITT for more than a year," said base training officer and ITT coordinator John Bozeman. "It was great to see all of our SUBASE emergency-response elements come together and meet such an unlikely and complex challenge head-on. As the adage goes, 'practice makes perfect,' and we are certainly on our way."

Texas
Police, Sheriffs Unveil Plans for Regional Intelligence Center

For months, detectives from two law-enforcement agencies had been on the trail of the culprits in a series of home burglaries in Southeast Austin and southern Travis County. Neither agency knew that the other was tracking similar unsolved cases.

Authorities say that the case – and others like it – highlights the need for law-enforcement agencies in Central Texas to routinely exchange data about crimes, trends, and suspect descriptions, an information flow they think will help solve more cases and decrease duplicate policing.

Beginning next year, Central Texas law-enforcement agencies will be able to coordinate their efforts through a federally funded multimillion-dollar intelligence center, one of dozens of such "fusion centers" across the nation. As part of the information exchange, the Austin Regional Intelligence Center will give investigators broader access to confidential information about suspects and criminal organizations.

The Austin and Round Rock police departments – and the sheriff's offices in Travis, Williamson, and Hays Counties – are the primary agencies involved in the project and will staff its operation with about eight to 10 crime analysts and detectives, some of whom will be hired with the funds provided by federal grants.

David Carter, an Austin assistant police chief in charge of the intelligence center project, said that the analysts assigned to the facility will have the capability to stitch together information collected by various agencies to create new files on suspects in criminal cases and/or on suspects they believe may be planning to carry out crimes and therefore merit closer surveillance.

The center will also allow investigators to access reports from other departments in the area that show any involvement suspects may have had with police there, including investigations into crimes the suspects may not have been charged with. In addition, investigators at the center will be able to access certain databases created by other agencies, such as those documenting suspected gang members and drug traffickers.

Austin police officials and other Central Texas law-enforcement officials began last year to start the drive to obtain the funding needed to build and staff an intelligence center. The city received a $1.8 million grant for the center in 2008, and an additional $2.7 million grant this year. If the grant money runs out, Carter said, the departments probably would begin using local funds to cover the salaries of the analysts assigned to the center.

Adam McLaughlin is with the Port Authority of NY & NJ, and is the Preparedness Manager of Training and Exercises, Operations & Emergency Management, where he develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs. He designs and facilitates emergency response drills/exercises for agency responders, state and federal partners, and senior Port Authority executives. Adam is a veteran and former U.S. Army Military Intelligence & Security Officer, having served with the 10th Mountain Division in Afghanistan during Operation Enduring Freedom and Operation Anaconda.

Copyright © 2009, DomesticPreparedness.com; DPJ Weekly Brief and DomPrep Journal are publications of the IMR Group, Inc.

IDGA
Institute for Defense and Government Advancement

Presents its 5th annual training conference:

NEW THIS YEAR!
The summit goes **tactical** and **practical!**

BORDER MANAGEMENT™ Summit

October 26 - 29, 2009
Ronald Reagan Building & International Trade Center, Washington, DC

Gain exclusive insights from top-notch speakers including:

Alan Bersin
Assistant Secretary, Office of International Affairs, DHS

Alonzo R. Peña
Senior Advisor to the Assistant Secretary, Immigrations and Customs Enforcement, DHS

Colleen Manaher
Director, Western Hemisphere Travel Initiative Program Office, DHS

CDR Louis J. Orsini, USCG (Ret)
Chief of Counter Drug AMIO Division, USCG

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

Featuring back-to-back sessions from Chief Border Patrol Agents!

Can't-miss topics at this year's summit include:

- Inter-agency and information sharing operations
- Biometrics and identity management systems
- Drug interdiction programs and requirements
- Current and future surveillance technologies

Sponsored by:

LOCKHEED MARTIN · CITRIX · TERADATA · THE CENTECH GROUP, Inc. · ManTech International Corporation · DRS TECHNOLOGIES · at&t

www.BorderManagementSummit.com