domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 9 Issue 2, February 2013

HAZMAT

Dual Threat Respirator

SCAPE
CO/CBRN30

The **FIRST & ONLY** NIOSH CBRN Escape Respirator with Carbon Monoxide Protection

- Ultimate protection
- User friendly
- Maximum comfort
- Automactic "ON" blower
- Panoramic field of view
- No Nosecup or Mouthbit
- 5-year shelf life

For more information visit
www.ilcdover.com/scapecocbrn

ILC DOVER
creating what's next

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

Catherine Feinman
Associate Editor
cfeinman@domprep.com

Susan Collins
Director of Marketing & Sales
scollins@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

John Morton
Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; 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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

With the long-looming threat of terrorist groups seizing Syrian chemical weapons, it becomes apparent that even the most comprehensive plans and preparations may, at best, only limit the amount of damage and number of casualties that might reasonably be expected. According to current intelligence estimates, there is a strong possibility that any of a long list of terrorist groups may raid Syria's chemical weapons warehouses, randomly scattered and not very well guarded, and use chemical weapons against U.S. friends and allies – and perhaps against the United States itself. Some of those chemicals are already "absent and unaccounted for," so to speak, as Richard Schoeberl points out in his opening essay on what is now a dangerous scenario facing the U.S. defense establishment itself.

That scenario, fortunately, is the worst of the bad news in this monthly wrap-up issue of *DPJ*. The good news in the nation's emergency preparedness community comes in two clearly unequal parts: (a) what has already been accomplished; and (b) what still has to be done. However, work is proceeding at all levels of government, in an unending effort to resolve or at least ameliorate current known problems while at the same time finding out more about other problems not yet looming just over the horizon.

Amanda Faul points out that at least some issues and concerns may be addressed, if not resolved, in the near future with the release of additional details and the guidelines needed to fully implement Presidential Policy Directive Eight (PPD-8), signed by President Obama on 31 March 2011. Joseph Cahill adds that significant assistance is already available to most communities – but (to cope with flu epidemics and similar health hazards) city mayors and state governors must know when and how to issue a formal Declaration of Public Health Emergency. Fortunately, as David McWhorter, points out the sometimes hidden cost of manufacturing, which could be ruinous to some companies, can be safeguarded thanks to liability-protection from the federal government's SAFETY Act.

Additional help is pending, or already on the way. Glen Rudner comments on the new chemical-detection systems and devices already on the market, and the better ones now being designed and tested. Uniform and significantly improved all-hazard assessments – a political as well as communications challenge – Joseph Trindal asserts also are needed, and no stakeholders should be directly involved. The same holds true, Patrick Coyle adds, for the nation's chemical facilities – public as well as private-sector, which should be regularly and rigorously inspected and regulated not by the industry itself but by highly qualified and independent agencies using their own inspector generals.

In short, tomorrow could and should be better – the day after tomorrow even more so. Wrapping up this month's printable issue are forward-looking commentaries by: (a) Thomas Moran, who discusses the fiscal advantages and new opportunities made possible by "partnering" between the private sector and government agencies; and (b) Jack Herrmann, who discusses the increasingly helpful annual Public Health & Preparedness Summit conferences, with special focus on this year's conclave – 12-15 March in Atlanta.

About the Cover: Two Department of Defense training photos, merged by DPJ's Susan Collins, show the strain imposed on responders as well as "victims" of two simulated mass-casualty attacks – one of them a chemical liquid spill from a portable water tank and the other a bombing during an operational readiness exercise. (Photographers: Marine Sgt. Daniel K. Brown and Air Force Master Sgt. Daniel W. Mosher.)

Kestrel

High Comfort & High Protection CBRN Oversuit

Kestrel

High Comfort & High Protection CBRN Oversuit

The Kestrel is a highly comfortable and highly protective two piece CBRN oversuit harnessing much of the technology used in the Phoenix Lightweight Protection suit. At around 30% lighter than conventional systems, it provides qualified CBRN vapour protection with the added benefit of water/oil repellence and fire retardant coatings, thus making the Kestrel an extremely versatile CBRN protection system for use in multiple CBRN threat environments

The Ketrel is constructed using a lightweight activated carbon liner, combined with a breathable, rugged and anti-rip outer.

- Lightweight and breathable, the Kestrel has been tested using the Avon FM12 respirator, and can be configured to suit many other types of respiratory protection

Highlights

- Conforms to NATO standards
- High protection
- High air permeability
- Greater comfort and low physiological burden
- 20 times launderable
- 10 year shelf life
- Compatible with a range of accessories
- Fire retardant and water/oil repellent
- Stand alone garment or overgarment
- Rugged and durable
- Available in various colours and camo patterns

For further information:
W: http://frontline.remploy.co.uk
E: frontline@remploy.co.uk
T: +44 (0) 151 630 3811

Remploy
Putting ability first

Frontline

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Craig DeAtley
Public Health

Kay C. Goss
Emergency Management

Stephen Grainer
Fire/HazMat

Rodrigo (Roddy) Moscoso
Law Enforcement

Corey Ranslem
Coast Guard

Glen Rudner
Fire/HazMat

Richard Schoeberl
Law Enforcement

Dennis R. Schrader
CIP-R

Joseph Trindal
Law Enforcement

Locked & Loaded With Chemicals in Syria

By Richard Schoeberl, Public Health

The 2011 Libyan revolution and the ongoing civil conflict within Syria have sparked fears around the world that chemical weapons could find their way into the hands of terrorist groups, particularly those within the Middle East. Syria's stockpile of chemical weapons dates back to the early 1970s and is considered by U.S. intelligence agencies to be the largest in the entire region.

International concerns that Syrian President Bashar al-Assad may order the use of chemical weapons against his own people have escalated further since December 2012, when Pentagon sources told NBC News that chemicals used inside Syria to produce sarin, a lethal nerve agent, were being loaded into bombs that could potentially be launched from fighter jets (Mi-25s). Syria may in fact possess in excess of 500 metric tons of the sarin precursor agents, according to press reports. The same sources also confirmed the fear that the Syrian military is prepared to use, against other Syrians, one of the most toxic of all the weaponized military agents.

Origins & Effects

Originally developed in 1938 in Germany as a pesticide, sarin is not found in the earth's natural environment but is, rather, an extremely lethal "man-made" chemical warfare agent. As the most poisonous of the known chemical agents, nerve agents are hazardous in both the liquid and vapor states – and can cause death only a few moments after exposure. Moreover, and making control even more difficult, is the fact that nerve agents can be spread by various mediums including but not limited to rockets, spray tanks, missiles, and – probably the first choice of Syria's own military – bombs.

After sarin is released, exposure can occur through contact with the skin and eyes, or simply by breathing air that contains the agent. Symptoms of exposure – for example, convulsions, paralysis, respiratory failure, and/or the loss of consciousness – may occur almost instantaneously or take as long as several hours.

Iraq and Japan suffered two devastating sarin attacks. In 1988, Iraqi President Saddam Hussein's forces killed an estimated 5,000 or more Kurds with a single sarin release against Halabja, a major city in the Kurdish region of Iraq. In 1995, the terrorist group Aum Shinrikyo used sarin, concealed and transported in portable packets, to launch an attack on the Tokyo subway system. The immediate result was 13 people killed and an estimated 5,000 or more others hospitalized – 17 of them in critical condition and 37 listed as severe. More than 900 victims also were diagnosed with long-term vision problems.

If chemical agents are in fact used by Assad, the effects on the Syrian people could be equally or more devastating – both in the short and long term:

- Those directly impacted could be exposed to a large dose of the agent, which would ultimately suffocate most of the victims by paralyzing the muscles around the lungs.
- Because sarin has no distinct odor or color, and is tasteless, some victims may not even know they had been exposed and therefore would delay treatment.
- Those not directly impacted might still be exposed to a low dose of the toxic agent, either by breathing in air or eating food or water tainted with sarin.
- First responders who care for those who come in direct contact also could experience some or all of the same symptoms as those who had been directly exposed to the agent.
- In addition, the clothing of those directly exposed would probably continue to release toxic vapors (for up to about 30 minutes after exposure).

Major Questions & Concerns

There are mounting concerns that go well beyond whether Syria itself is prepared to and/or would ultimately use chemical agents against its own people. The international community remains on alert that such weapons could eventually fall into the hands of terror groups such as al-Qaida, which has been attempting to acquire chemical weapons for years, or even Hezbollah, which since the 2006 Hezbollah-Israeli war has threatened to use chemical weapons against Israel.

Hezbollah has not yet acted on those threats, of course, but its alliance and close working relationship with Iran is good reason for concern. If Assad's government is in fact overthrown, Israel and other U.S. allies, including some nations bordering Syria, already have expressed concern that terrorist groups would gain access to Syria's stockpile of chemical weapons, which includes mustard gas and sarin.

According to various intelligence reports, Hezbollah already has established bases in close proximity to some of the Syrian weapons caches, a step that escalates considerable concern as the instability in Syria continues to worsen. Two possible scenarios of particular concern are that: (a) Syria's chemical weapons caches would ultimately fall into the hands of Hezbollah (and possibly other terrorist groups); and/or (b) Assad would use chemical weapons on his own people in an eleventh-hour struggle to save his government. If even a relatively small amount of those weapons were to fall into the hands of al-Qaida or Hezbollah, it would significantly upgrade the capabilities of those groups – and, quite possibly, require some very difficult political decisions on how the international community would have to respond to them.

Preventing a chemical attack by the Syrian government against its own people would be extremely difficult. Largely because of the current hostile circumstances surrounding the civil conflict in Syria, the U.S. Department of Defense estimates that military efforts to secure Syria's cache of chemical weapons would require the deployment of more than 75,000 U.S. troops, according to 2012 press reports. Given the current distribution of U.S. military forces – and the increasing likelihood of large new cutbacks in defense spending – it is questionable at this time whether the

United States would have the resources needed to effectively address this mounting concern.

Another factor to consider is that Syria itself has not signed the 1997 Chemical Weapons Convention (CWC), which bans the manufacturing, stockpiling, and/or use of substances such as nerve agents. Moreover, it is uncertain what other types of chemical weapons, in addition to sarin, that Syria may have in its arsenal and is prepared to use. (The answer, according to several press reports – not officially confirmed by the U.S. government – is that Syria possibly already possesses hundreds of tons of numerous chemical agents, including VX and sarin nerve agents, in addition to blistering agents such as sulfur mustard.)

Promises, Security & Future Threats

In July 2012, Syria's Foreign Ministry spokesman, Jihad Makdissi, said in a televised news conference that, "No chemical or biological weapons will ever be used, and I repeat, will never be used, during the crisis in Syria no matter what the developments inside Syria." However, less than a year later, the Syrian government now has the nerve agent "locked and loaded" – and apparently still has no desire to comply with the CWC.

According to the United Nations, at least 60,000 people already have died during Syria's two-year internal conflict. Israeli hospitals currently, and very prudently, are scheduling regular training sessions so their staffs can respond both quickly and effectively to a chemical weapons attack – if or when there is one. U.S. President Obama himself also cautioned Syria, in a press statement on 3 December 2012, that, "The use [by Syria] of chemical weapons is and would be totally unacceptable ... [and] there will be consequences and you [Assad and Syria's other political and military leaders] will be held accountable."

Fortunately for the Syrian people, the combination of such a stern warning from the United States – backed by public support from such disparate nations as Russia, Iraq, Turkey, and Jordan – seems to have suspended the chemical mixing and the bomb preparations, at least for the time being.

However, the most important unanswered question still looms: Whether they are used or not used against its own citizens, will the Syrian government be able to effectively secure and protect its chemical stockpiles from falling into the hands of persons, or groups, looking to acquire them? In an effort to address this question, the United States and its key allies have deployed specialists to neighboring Jordan to help prepare for the possibility that Syria may in fact lose control of its chemical weapons cache. That modest step forward is no guarantee, of course – but it is at least an offensive move much needed in a game with too many unanswered questions and no end in sight.

Richard Schoeberl has more than 17 years of counterintelligence, counterterrorism, and security management experience, most of it developed during his career with the Federal Bureau of Investigation, where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the U.S. National Counterterrorism Center. During most of his FBI career he served in the Bureau's Counterterrorism Division, providing oversight to the agency's international counterterrorism effort. He also was assigned numerous collateral duties during his FBI tour – serving, for example, as a Certified Instructor and as a member of the agency's SWAT program. He also has extensive lecture experience worldwide and is currently a terrorism and law-enforcement media contributor to Fox News, Sky News, al-Jazeera Television, and al-Arabiya.

Developing & Deploying Multi-Use Technologies

By Glen Rudner, Fire/HazMat

Detection is required at different stages of both planned events and emergency incidents. Many of the modern detection technologies and devices that have been developed are "multi-use technologies" that serve as emergency response, homeland security, medical, and/or industrial tools. Coordination is necessary because detection developers (i.e., industrial manufacturers), policy makers (e.g., intelligence, health, energy), and stakeholders (e.g., government departments, local administrations, first responders, academic community, industry) each have a vested interest in the outcome of incidents involving the use of such technologies.

Detector Development & Stumbling Blocks

When addressing the development of these detectors, the emergency response community must define: (a) what the detectors are going to be used for (i.e., detecting a specific threat, or only allowing for early warning once the threat is confirmed); (b) who will use the detectors (e.g., civilians, military personnel, lab technicians, first responders); and (c) who will develop the detectors and with which financial resources (i.e., public programs/public funding, public-private partnerships, civilian-military partnerships).

Response communities depend on the availability and use of reliable equipment that fits their needs. Therefore, they should be involved in the various development phases of such technology.

A major stumbling block for development of the technologies is that the organizations that create the standards and set the parameters for development of detection devices have antiquated testing standards in place. A good example is continuing to use the same military challenge chemicals – for example, diesel exhaust, glass cleaner, and glycol ethers – to challenge modern detector and sensor technologies. The primary issue is that more highly refined processes have been developed that would make many of those interfering agents less than effective. As a result, the abilities of the instruments to detect as well as the decisions made based on the resulting data would be flawed.

Another stumbling block is the lack of end user participation on the same standard organization. The current economy certainly plays a role in the level of participation, but it is important that the end user have input into all phases of an instrument's manufacturing process – from the concept phase to the final production and field testing, which includes day-to-day use. Many field instruments have become nothing more than "paperweights" as a result of ineffective development that does not meet the needs of the end user.

Deployment, Applications & A Standardized Process

Once the development phase is complete, detection policies must define the guidelines for appropriate deployment of these instruments. A decision also needs to be made by the planning organizations such as the U.S. Department of Homeland Security and its individual agencies – the Federal Bureau of Investigation, the Federal Emergency Management Agency, and others – to prioritize what critical infrastructure should be identified and monitored for the presence of chemical, biological, radiological, nuclear, and explosive (CBRNE) agents (e.g., government buildings, public transportation facilities, postal sorting offices, water supplies, chemical and nuclear plants). The policy then must be applied nationwide, in order to provide consistency for each agency that will be tasked with the process of collecting data and formulating additional planning processes.

Additionally, applications for using the detectors need to be developed, including the detectors' properties and the ways that the data should be interpreted and used during the decision-making

process. More importantly, the appropriate people to make the decisions based on the information generated by the detectors also must be clearly identified.

Lastly, a standardized process would allow for the validation of the detectors, the assessment of their performance, and their adaptation. Validation refers to an official authority ensuring that privately produced detectors meet all specifications.

However, trying to adapt the current technology in detectors to meet the changing needs of the users is a critical challenge. There are many flaws in both existing technologies and the development of newer technologies. The risk to the response community is that a partial deployment of an imperfect technology could create a false sense of security. Nevertheless, the focus on CBRNE threats has led to technological advances in each of the various categories of detectors, and new technologies are constantly being developed and tested.

In conclusion, the choice between the different types of detectors is usually dictated by considerations regarding the purpose of the detector. In other words, detectors must be adaptable to meet multiple needs of the users – on the battlefield as well as on city streets.

Glen Rudner is an independent consultant and trainer who recently retired as a Hazardous Materials Response Officer for the Virginia Department of Emergency Management. His 35 years of experience in public safety includes 12 years as a career firefighter/hazardous materials specialist for the City of Alexandria (VA) Fire Department; he also served as a volunteer emergency medical technician, firefighter, and officer and, as a subcontractor, served as a consultant and assisted in the development of many training programs for agencies such as the Federal Bureau of Investigation, the International Counter-proliferation Program, the U.S. Department of Justice's Office of Justice Programs, the U.S. Department of Homeland Security, and the Defense Threat Reduction Agency. He is now Secretary for the National Fire Protection Association Hazardous Materials Committee, a member of the International Association of Fire Chiefs' Hazardous Materials Committee, a member of the American Society of Testing and Materials, and Co-Chairman of the Ethanol Emergency Response Coalition.

Protecting Chemical Facilities Against Terrorist Attack

By Patrick Coyle, Building Protection

The U.S. Department of Homeland Security (DHS) Appropriations Act of 2007, passed by Congress in 2006, authorized the secretary of that department to establish a regulatory program to oversee the security of chemical facilities considered at high risk for terrorist attack. In the spring of 2007, the Chemical Facility Anti-Terrorism Standards (CFATS) program was born.

Using his/her authority to evaluate the risk levels of chemical facilities, the secretary determines the nature and likelihood of a potential threat based on an operational definition of a chemical facility and the possession of a "screening threshold quantity" (STQ) of specific chemicals of interest (COI). The COI list (found in CFATS Appendix A, 6 CFR Part 27) includes the chemicals that, if released during a terrorist attack, would pose a threat of fire, explosion, and/or toxic exposure to the local community. Other chemicals are also included on the COI list that, if stolen or misdirected, could be used to manufacture explosive devices or chemical munitions for a subsequent attack.

The U.S. Department of Homeland Security has established and is using some common-sense standards and procedures to determine and mitigate the risk of terrorist attacks on the nation's chemical facilities.

The STQs are established at a level commensurate with the specific risk of the chemical, meaning that a high-risk chemical facility might not be a theoretically "typical" chemical manufacturing or distribution center. Any facility, in fact, that is home to a COI at or above the STQ limit could be declared a high-risk chemical facility. For that reason, the current facility list includes (but is not limited to) such disparate facilities as university laboratories, food processing plants, and agricultural complexes.

Risk Also Based on Location

The impact of a terrorist attack that includes the release of a certain quantity of a toxic chemical would vary to some extent according to the location of the chemical facility. For example, the effects of a 10,000-lb. release of anhydrous ammonia would be more serious in an urban area than on a Kansas farm, a consideration that puts the urban target at higher risk of an attack than the agricultural target.

In 2007, to evaluate the comparative risks based on location, DHS established the Chemical Security Assessment Tool's Top-Screen program, which requires any facility that possesses a COI at or above the STQ level to submit certain information to the department's Infrastructure Security Compliance Division (ISCD) – specifically including the maximum amount of each COI on hand within the past 60 days – along with certain basic information about the location of the facility. After reviewing the data submitted, the ISCD makes a preliminary determination of the high-risk status of the facility.

The need for that information quickly became evident. DHS Under Secretary Rand Beers stated in Senate testimony on 3 March 2010 that, when the first Top-Screens were received – in December 2007 and January 2008 – nearly 38,000 facilities had submitted their reports, and over 7,000 of them were notified that they might be at high risk for a terrorist attack. The other facilities were informed that their risks did not meet the criteria established for participation in the CFATS program – but were also advised that, if their COI inventory changed, they would have to submit a new Top-Screen.

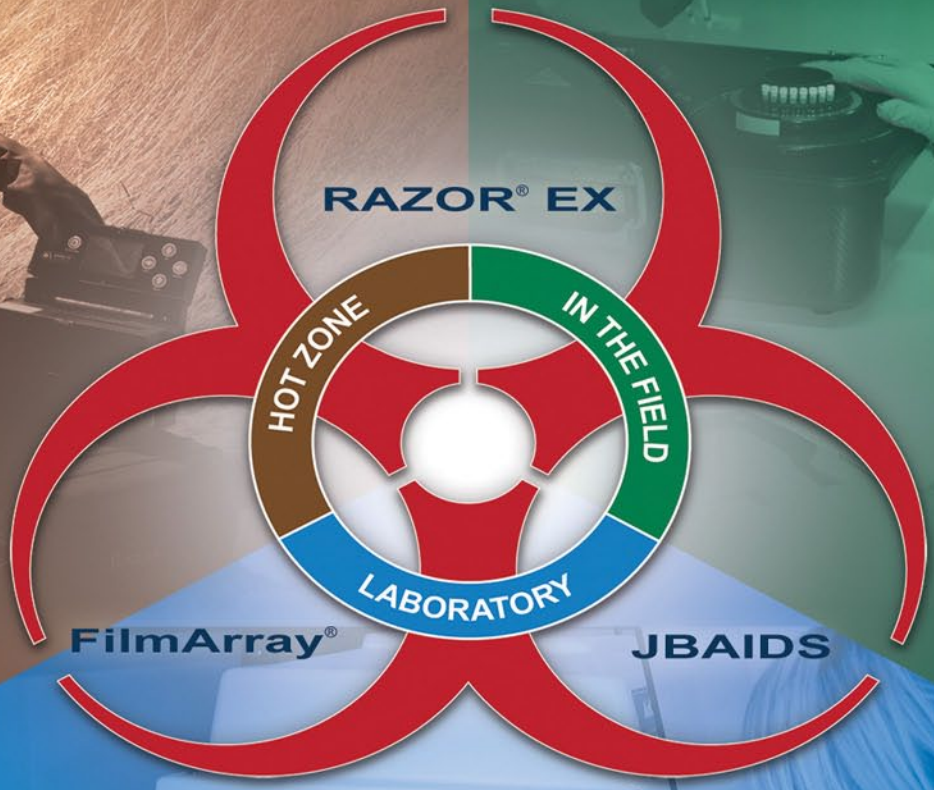
Information Protection & Vulnerability Assessment

Once designated as a high-risk facility, that facility then must provide additional and more detailed information to ISCD. To ensure that the business and security information provided in the submissions is protected from disclosure by the government, Congress also required the DHS secretary to develop an "information protection" program that would exempt, from various federal disclosure rules, the information provided by the facilities participating in the program.

BioSurveillance

Flexible, Accurate, Proven Ready

BioFire Diagnostics delivers a fully integrated suite of Biological Agent Identification Systems. Since 1998 we have fielded BioSurveillance products that span the range of operations from the lab to the field, clinical diagnostics to environmental surveillance.



Idaho Technology is now

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

In response, DHS developed in 2006 a new Chemical-Terrorism Vulnerability Information program to protect the information provided to ISCD under the CFATS program from disclosure under the Freedom of Information Act. In court proceedings, therefore, such information receives protection similar to that afforded classified information – but there also are some provisions included that permit information sharing with state and local emergency response officials.

To make a final determination that the initially designated facilities would actually be at a high threat of terrorist attack, DHS requires the submission of additional facility information under what is called a Security Vulnerability Assessment. Such assessments, which are submitted via another secure application in the Chemical Security Assessment Tool, provide ISCD with additional information about the facility layout, chemical storage, and safety/security systems.

After analyzing the Security Vulnerability Assessment data, ISCD makes a final determination of whether or not a specific facility is at high risk of terrorist attack, then assigns the facility to one of the four risk tiers – tier one being the highest risk and tier four the lowest. The tier ranking is important because the standards for the facility security measures are tied to that ranking.

Standards, Plans, Metrics & Guidelines

When Congress authorized the CFATS program, it included a provision that prohibited the DHS secretary from requiring any specific security measures for the approval of a site security program. To comply with that requirement, DHS incorporated into the CFATS regulations a list of 18 Risk-Based Performance Standards (RBPS) that must be met for a security plan to be approved.

In 2009, ISCD also published an RBPS Guidance document that provides additional information about not only the standards mandated but also the types of protection measures that may be appropriate for meeting those standards. The Guidance also provides a series of security metrics for each RBPS, based on the tier ranking of the facility, that spell out the difference in the requirements that must be met for each of the standards postulated.

CFATS-covered facilities are required to submit their security plans to ISCD for approval – by, for example, using a Site Security Plan (SSP) application in the online Chemical Security Assessment Tool. The SSP application provides a series of questions that the facility must answer about its current security processes, planned security measures, and proposals for future improvements.

Slow Progress – But Improvements Promised

Analysts at ISCD headquarters review the SSP submissions to determine if the measures planned are adequate to protect the facility in accordance with the RBPS for the appropriate tier ranking. If it is determined that those standards are in fact met, ISCD then: (a) authorizes the facility to implement the plan; (b) sends chemical facility security inspectors to the site to review the implementation process; and (c) approves the SSP – but not until *after* the inspectors report that the plan is in fact being properly implemented.

The step-by-step submission, authorization, and inspection process has proven, however, to be much more difficult and time-consuming than DHS had anticipated. In fact, according to the latest testimony (on 11 September 2012) of Beers before a subcommittee of the House Energy and Commerce Committee: (a) More than 3,600 facilities had by that time received final notification of their high-risk status and tier rankings; but (b) only 73 facility SSPs had been authorized as of that date; and (c) only one had been approved. David Wulf, Director of the Infrastructure Security Compliance Division, reported on 17 January 2013 that DHS is currently working on various procedures and process changes that will enable the authorization and approval rate to be significantly improved.

The chemical security program authorized by Congress in 2006 was intended to be an interim solution while Congress considered and approved a more comprehensive program. That has been more politically difficult than initially expected. Meanwhile, though, the continued authorization of the CFATS program has been renewed every year in the DHS appropriations bills. The current spending bill, and authorization for CFATS, expires on 27 March 2013.

Patrick Coyle is a 15-year veteran of the U.S. Army and has worked for 17 years in the chemical process industry – including 12 years as a process chemist and one year as a quality assurance manager. He also has taught industrial safety, and has been a freelance writer since 2006. For the past six years he has used his unique background to write a chemical security blog: the "Chemical Facility Security News."

A Continuing Need for Accurate All-Hazard Assessments

By Joseph Trindal, Law Enforcement

There is general agreement that accurate and reasonably comprehensive risk assessments are needed before making major decisions of almost any type. Far too often, though, many of those assessments are based on erroneous assumptions. In today's world, risks associated with various types of chemicals are among the least understood, outside of the chemical industry itself.

Risk assessments are particularly important in communities that are heavily involved in the chemical production, storage, processing, and supply-chain industries. Nonetheless, whether considered as a whole, or only in part, the need for an accurate understanding of chemical risks is essential throughout the United States.

Current and future fiscal constraints in both the public and private sectors – compounded with changes in threat characteristics involving extreme violence and/or cyber attacks – enhance the need for accurate hazards analysis. Failure to minimize the various unknowns in hazards analysis of risk assessment models in effect magnifies errors in both vulnerability and consequence assessments. Moreover, any initial hazard assumptions that prove to be erroneous often contribute to costly errors in planning, capital expenditures, and consequence management.

A Current "High-Risk" Example

When updating its risk assessment and emergency response procedures in 2013, the administration, staff, and engaged stakeholders at one high-value "site" – identification necessarily anonymous, but one with custodial responsibility for the safety of a large number of people – were particularly concerned with the perceived consequences of potential accidents involving rail cars and an ethanol transfer station within one mile of the site. Before conducting an official risk assessment, the response procedures for hazardous material contingencies at or near the site included the full evacuation from the site, of those considered to be in danger, to a large shopping center parking lot several streets away. Added to the dangers posed by crossing several busy streets was the fact that many of those under the site's custodial care have diminished mobility, which may hamper swift and independent movement.

The assumptive hazards assessment supported a response scenario that envisioned a toxic cloud moving slowly toward the site. Sheltering in place was deemed to be a secondary response procedure in the event that the toxic cloud was moving toward the site at a fairly rapid speed. Unfortunately, the shelter-in-place procedures did not include shutting down the site's air handling (HVAC) system.

Considering the physical properties and characteristics of the actual chemical products in transit near the site and the combustible properties and characteristics of an ethanol transfer operation, the basis for the response procedures already in place was questionable. Those responsible for safety procedures at the site had used "technical" guidance from engaged stakeholders and site officials, but they failed to consider the hazmat expertise available through the local fire department. A meeting – between the parties involved and the fire department's hazmat professionals – was convened to accurately assess the chemical hazards in close proximity to the potentially endangered site.

That meeting led to a more accurate and comprehensive understanding of the unique transit restrictions for hazardous materials anywhere near the site. As a result, the earlier somewhat vague concerns were replaced by reality. In this example, no toxic-release chemical currently transits the rail system near this site – and common carrier hazmat movements by truck, it was agreed, are not a relevant hazard to that area. As for the potential risk posed by the ethanol transfer station, the materials transfer rate and procedures being followed significantly minimize the potential impact from flammable combustion (the worst-case scenario for the chemicals involved). Moreover, any evacuation requirements would be dictated by the fire department incident commander.

After assessing the real risks, site officials prudently adjusted the response procedures to shelter in place as the first option – possibly followed by an orderly evacuation, with enough time available to arrange transportation directly from the site to a safe area. The new procedures eliminate the risks associated with moving occupants across busy streets to a shopping center parking lot.

AP4C

Handheld
CWA, TICs/TIMs
chemical detection
in confidence

Easy to use,
reliable, sensitive
and always ready

PROENGIN
Chemical and biological detection system

PROENGIN, inc.
140 S. University Dr, Suite F
Plantation, FL 33324 USA
Ph: 954.760.9990
contactusa@proengin.com
www.proenginusa.com

Many Advantages of Accurately Avoiding Risk

The preceding real-life situation is an accurate microcosm example in which initial errors in hazard assessments led to the adoption of procedures that posed unnecessary risk to the site's occupants – and to the organization as a whole. If an incident had actually occurred at that site, the procedures previously adopted would have further strained the emergency response resources available by substantively contributing to a predictable and preventable emergency – for example, one or more of the site's high-value occupants being injured or killed in a pedestrian-vehicle collision during evacuation.

Considering the degree to which emergency planning is becoming more commonplace in communities across the nation, particularly in the private sector and non-emergency agencies of the public sector, the need for accurate hazard assessments continues to grow. The whole-community resilience model now being adopted in many states and cities throughout the country offers solutions in the form of public-private sector team building. The community-based team-building approach already available provides hazard-specific expertise from the nation's local and national fire, hazmat, emergency medical services, public health, and law enforcement communities.

Accurate hazard analytics is the foundation of the efficient and economical procedures that can be achieved by incorporating best practices to mitigate and manage real risks. Accurate and comprehensive public/private-sector emergency planning also greatly enhances the mutual situational understanding of planned response actions, thereby grounding mutual expectations and improving the cohesion of integrated responses.

Joseph Trindal is managing director at Defense Group Inc., where he leads the company's risk management services. He also serves as executive vice president of InfraGard Nation's Capital Member Alliance. He retired in 2008 from the U.S. Department of Homeland Security, where he had served as director for the National Capital Region, Federal Protective Service, Immigration and Customs Enforcement. In that post, he was responsible for the physical security, law enforcement operations, emergency preparedness, and criminal investigations of almost 800 federal facilities throughout the District of Columbia, Northern Virginia, and suburban Maryland. He previously served, for 20 years, with the U.S. Marshals Service, attaining the position of chief deputy U.S. marshal and incident commander of an emergency response team. A veteran of the U.S. Marine Corps, he holds degrees in both police science and criminal justice.

Implementing PPD-8: New Opportunities, Greater Challenges

By Amanda Faul, Standards

The U.S. homeland security and emergency management communities are now waiting for the release of the five national planning frameworks outlined in Presidential Policy Directive 8 (PPD-8) issued by President Obama two years ago. For most members of the preparedness community, the two-year anniversary of PPD-8 will provide the first full-scale insight into how the White House plans: (a) to position the nation to effectively prepare for a possible worst-case scenario; and (b) to coordinate, across all levels of government and the private sector, the operational actions likely to be needed.

At the state level, law enforcement and emergency management agencies have been reviewing and discussing the five frameworks mentioned above: prevention, protection, mitigation, response, and recovery. The specific details of how the federal government will address each one are still being finalized. However, some changes already have been initiated at the state and federal levels to address each framework and take advantage of the new opportunities provided by the preparedness doctrine. Nonetheless, at least some of the likely barriers to full implementation may be prohibitive. These barriers include the necessary re-organization and re-writing of agency and jurisdictional plans to reflect core capabilities, and the complexity of some core capabilities, which span multiple, diverse functions.

Full Implementation Likely – Several Caveats Also

It seems likely that PPD-8 may be "fully" implemented, insofar as possible, at the federal level in President Obama's second term. Although some PPD-8 tasks already have been issued by the Federal Emergency Management Agency (FEMA) to states and major cities, it may be several more years before the second-anniversary changes can be fully implemented by state and local governments. Nonetheless, leaders across all levels of government are evaluating the practicality and sustainability aspects of adopting the PPD-8 guidelines beyond what they are required to do to maintain their eligibility for the homeland security grant funding provided by the federal government.

The federal government's last attempt at capabilities-based preparedness, articulated in the U.S. Department of Homeland Security's (DHS) *National Preparedness Guidelines*, put special emphasis on use of the *Target Capabilities List* (TCL). Both of those documents were released in 2007. The TCL identified 37 specific capabilities across four major mission areas – prevention, protection, response, and recovery. However, the *National Preparedness Goal* (issued in 2011) revised the capabilities goal to 31 across five mission areas (expanding the emphasis on community resilience by inclusion of a new "mitigation" mission area).

Over the past five years, the 578-page TCL has proved difficult both to navigate and to implement. The revised core capabilities list included in the National Preparedness Goal identifies fewer capabilities, in a simplified presentation with a greater degree of flexibility, which can be used to identify what is needed in terms of planning, organization, equipment, training, and exercises (POETE) to achieve and/or improve preparedness.

A Forest of Acronyms on The Road to Full Implementation

The first full exposure most state and local governments had to the core capabilities was in preparing their State Preparedness Reports (SPRs) for 2011 (before that, states were not required to define their core capabilities) and, to a greater degree, their 2012 Threat/Hazard Identification and Risk Assessments (THIRAs). Both the SPRs and the THIRAs are required to maintain eligibility for the DHS grants. Those preliminary tasks facilitated the later incremental rollout of overall national preparedness concepts. In their submission of the 2012 THIRAs and SPRs, states and urban areas participating in DHS's Urban Area Security Initiative (UASI) set performance targets for each of the 31 core capabilities and are now annually required to assess levels of preparedness against those same targets.

With the planned release, later this year, of additional capability guidance, states and urban areas will probably repeat last year's THIRA/SPR process in 2013 – but in

accordance with more specific instructions to assess what resources they now possess and what additional resources they will still need to achieve their individual contributions to the National Preparedness Goal.

Whether or not states and jurisdictions participating in the UASI program used previously existing coordinating structures, or developed a new preparedness process, the volume of preparedness data already being gathered as part of the THIRA/SPR requirement is or could be very valuable. PPD-8 has provided a straightforward methodology that also serves as a much needed refresher course in how to assess and "strategize" the management of risk. Decision-making officials at all levels of government now have a much clearer picture of capability strengths – areas for improvement as well – that they can use to develop and justify the expenditure of limited resources and increasingly scarce homeland security funds.

The nation's state and local governments are faced with the challenge of refining and expanding their preparedness levels across five distinct mission areas.

New Risks & Challenges

Several additional challenges are sure to arise in implementing PPD-8 at the state and local levels. The first challenge arises from the fact that several core capabilities cover such a broad range of preparedness activities that it is extremely difficult: (a) to set an overarching target; and (b) to assign responsibility for the development and evaluation of rather wide-ranging core capabilities. An example of a core capability that is extremely complex is what is described, in the National Preparedness Goal, as Public and Private Services and Resources. This capability encompasses but is not necessarily limited to firefighting resources, private industry, volunteer organizations, fuel resources, and generator assets. Because of the wide range of response activities provided by those resources, there is a risk of the core capability being oversimplified during implementation.

Another important challenge is that, for many agencies and planners, planning based on core capabilities represents a significant shift in emergency preparedness planning – which in the past had typically been based on: (a) specific threats and hazards (scenario-based planning); and/or (b) emergency support functions (ESFs – i.e., functional planning). To manage this shift in planning methodology, a "phased" education that implements necessary/mandated changes more gradually – again, at all levels of government – seems probable. Unfortunately, at the present time there is little federal support for training related to PPD-8.

Whether the next (FY 2014) federal budget will provide additional funding has yet to be determined. Nonetheless, it seems obvious that future federal training courses should be designed to ensure that the educational preparedness program that practitioners need for a true core-capability-based planning system is as effective as possible.

Additional and more effective national preparedness guidance also is needed. Because PPD-8 is still in the initial stages of implementation, there are few, if any, best practices to help guide planning efforts. More federal guidance also is needed to assist development of best practices at the state level. Such federal guidance may at least help to bridge the gap between the federal and state levels.

The lack of best practices and federal guidance becomes most apparent when trying to integrate the PPD-8 concepts into operational planning. According to PPD-8, "The frameworks shall be built upon scalable, flexible, and adaptable coordinating structures to align key roles and responsibilities to deliver the necessary capabilities." They also must be capable of being adaptable to any jurisdiction. Those goals will be difficult to meet at a time when states are finding it challenging to merge core capabilities into the existing ESF coordination model. Determining how ESFs and core capabilities relate to one another – and how to set core-capability-based objectives and mission tasks during operations – is a daunting challenge.

The Active Art of Watchful Waiting

However, in spelling out the rationale postulated and processes needed for response-based capabilities, FEMA provided an interagency consequence management plan, which includes core-capability-based courses of action, for the 2013 presidential inauguration. That plan and the entire plan development process may usefully serve as "best

practice" examples of how to incorporate core capabilities into response planning until the White House releases a comprehensive federal interagency operations plan. Although the 2013 Presidential Inauguration Interagency Consequence Management Plan provided guidance for incorporating core capabilities into response planning and operational response, guidance on the other mission areas is still needed.

PPD-8 provides a clear methodology to help state and local governments improve and expand their preparedness levels across five distinct mission areas. Despite challenges in implementing the PPD-8 concepts, that directive does provide an improved preparedness program that can be of significant benefit to state and local governments. Hopefully, further federal guidance will reduce some of the implementation challenges to state and local governments for translating core capability preparedness into operational planning.

The early adopters are carefully working their way through the numerous and frequently complicated planning and implementation issues involved. The practitioners, meanwhile – not only planners and policy makers but also receivers, responders, managers, and others who will have to put the plans and decisions into action – are thinking about: what has to be done; how it should be done; and what obstacles might still be in the way. Adopting a wait-and-see approach is undoubtedly frustrating, but those responsible for future implementation will be that much better informed in the months and years to come.

Amanda Faul, a policy analyst with the University of Maryland's Center for Health & Homeland Security, currently works as a regional planner for the Maryland Emergency Management Agency. Prior to assuming her current post, she worked as a disaster planner for the Cedars-Sinai Medical Center in Los Angeles, California. She holds a Master's degree in public health, with a concentration in emergency public health and disasters, from the University of California Los Angeles.

Significant contributions to this article were made by Jordan Nelms, the planning branch manager at the Maryland Emergency Management Agency. He previously worked as a contractor supporting the PPD-8 Program Executive Office at the Federal Emergency Management Agency. He received a BA in political science/security studies from East Carolina University and pursued graduate studies at The Johns Hopkins University, the University of South Florida, and University of St. Andrews in Scotland.

Liability Protection:
An Often Overlooked Aspect of Business Continuity

By David McWhorter, Private Sector

Among the numerous specialized topics and activities important to the preparedness, security, and defense of the United States from terrorist acts are: protection of the food supply; response and recovery activities; special event planning; radiological preparedness; medical emergencies; bioterrorism; power-grid modernization; and the detection of chemical warfare agents.

The various technologies and services closely related to these topics and activities – and others involving the physical and cyber protection of the nation's critical infrastructure and key resources (CI/KR) – have one thing in common: the private-sector providers and consumers of such goods and services are eligible for a unique type of federal protection from third-party liability when an act of terrorism has been committed. From this liability protection comes a major component related to the continuity of operations planning (COOP), which is not only an operational advantage for the providers of the products and services but also for their customers who are the owners and operators of the CI/KR.

The COOP & SAFETY Act Nexus

In 2002, Congress passed, among other legislation, the Homeland Security Act, which created the U.S. Department of Homeland Security (DHS) and contained the less well known SAFETY Act (Support Anti-terrorism by Fostering Effective Technologies). The principal purpose of the latter Act is, through the statutory limitation of potential liability, to encourage sellers of services and technologies that protect the public to develop and deploy such technologies, as opposed to avoiding the marketplace for fear of liability.

The rationale leading to passage of the SAFETY Act was that, when a private-sector business sells technological products or services that are used at a site (physical or virtual) affected by an act of terrorism, that business could face costly, even enterprise-crippling, liability claims. Now, fortunately, sellers that have received a SAFETY Act "Designation" have limited liability, thus ultimately saving the enterprise.

An ancillary but equally important benefit provided by the seller's SAFETY Act coverage is that its customers are immune to third-party liability lawsuits related to the alleged failing of a technology or service covered by the SAFETY Act, an advantage that allows for (but does not necessarily guarantee) continued operations in the future. This "flow-down" liability protection that customers receive also serves as a significant market differentiator. Not only will customers of a SAFETY-Designated company know that the products and/or services being purchased have been vetted and approved by DHS, but also that they (the purchasers) will benefit from automatic liability protection. Seen from that perspective, the SAFETY Act serves both sellers and buyers as a critical component of the COOP equation.

Protecting Future Investments

The process for achieving SAFETY Act coverage varies depending on the specific type of product or service involved. For certain technologies, typically devices and "widgets" that can be tested to a statistical probability of success, the process is relatively uncomplicated. However, at the other end of the spectrum – for example, services that are heavily dependent on human factors – the process can be both long and arduous. Either way, the success of the application depends largely on the seller demonstrating – via documentation based heavily on repeatable processes, procedures, and quality assurance measures – that the product or service is reliably effective.

For providers of products and/or services designed to protect their customers from acts of terrorism and/or the effects caused by such acts, the SAFETY Act can be the ultimate COOP tool. It will not only allow for the continued deployment of the counter-terrorism products and/or services involved, but also help ensure the continued operations of the purchasing organizations. That combination provides unique protection that allows those same organizations to continue operations even after a potentially devastating loss.

There is one cautionary note, though, that should be kept in mind, by users as well as providers of the products and services involved. Because of the numerous nuances and details of this very complicated piece of legislation, SAFETY Act experts should be consulted *before* manufacturing, deployment, or purchasing decisions are made based on the protections afforded by the SAFETY Act.

David McWhorter is a Principal at Catalyst Partners, where he focuses on homeland-security business development and helps the company's clients navigate through DHS (especially for SAFETY Act matters). He has successfully led several dozen applications through the SAFETY Act process and is also the Practice Leader for Catalyst's Homeland Security Technology Assessment Practice. Previously, he served as the lead technical evaluator for the contractor (The Institute for Defense Analyses) supporting DHS's SAFETY Act operations and evaluations. He received his Ph.D. in chemistry from the University of Virginia.

The Timely Art of Declaring a Public Health Emergency

By Joseph Cahill, EMS

Swine flu, bird flu, and pandemic flu have been widely publicized by the news media over the past decade. Public health and emergency management officials walk a tight line, though, between the risk, on the one hand, of sounding an alarm prematurely and, on the other, of missing the pivotal moment when a warning will do the most good. When officials do sound the alarm and the prospective hazard either fizzles out or turns out to be less severe than anticipated, they are often portrayed as crying wolf – even if the reduced severity is because of their own hard work in mitigating the danger.

Capturing that moment is as much an art as it is about content – specifically including the following conditional imperatives: (a) Provide the right information at the right time (by doing so, the official looks like a hero); (b) pull the trigger too soon (and what actually happens may fall well short of expectations); and/or (c) wait too long (and the belated warning becomes more like an after-action report). Unlike the evacuation orders issued prior to an oncoming (and well tracked) hurricane – which often has a point after which there is no longer any action the public can take to avoid the destruction – infectious disease outbreaks offer the opportunity to continue action even after the event has already started.

A Timely Example in Boston

On 9 January 2013, Boston (Massachusetts) Mayor Thomas M. Menino (D) declared a citywide public health emergency because of the overwhelming volume of flu-like illnesses and influenza deaths that had already occurred in the city. By 19 January 2013, according to the Boston Public Health Commission (BPHC), there had been 1,220 cases of influenza confirmed in Boston since October 2012 – compared to only 70 in the entire 2011-2012 flu season.

A typical declaration of emergency by the senior executive of any U.S. political jurisdiction, be it the mayor, the governor, or even the president, would be used for reaching one or more of the three following goals: (a) to unlock additional powers not normally available to the executive branch; (b) to provide additional emergency funding, if and when needed; and (c) to help meet the requirements necessary before requesting assistance from a higher level of government.

Typical emergency communications consist of a three-part message: a factual statement about the present or incoming hazard; the signs and symptoms used for recognizing the hazard; and the actions that the entire community and/or individual citizens can take to prevent or at least ameliorate the dangers and difficulties involved. In other words, public health communications are not limited to providing information but also changing behavior.

Delivering the Message

Menino's 9 January declaration did not unlock any additional political powers, seek or add any new funds, or even request any assistance from the state of Massachusetts or the federal government; instead, it served as a mechanism for emergency messaging – and pushed the risk of influenza immediately into the public consciousness. By pairing the declaration of emergency with a message about the availability of free flu vaccine clinics, the City of Boston was able – with its private-sector partners – to vaccinate approximately 7,000 people in the course of a single weekend.

Prior to the emergency declaration, only 12,000-15,000 Bostonians had been vaccinated to meet the possibility of an outbreak during the 2012-2013 flu season, according to Nicholas Martin, director of communications for the BPHC. The key features of the city's messaging plan are brevity and staying on message. Perhaps the most important essential, though, for using an emergency declaration as a communications tool is the credibility of the executive.

That condition was met in this case, as Martin pointed out. Menino is widely respected and highly believable, and was therefore "the right person" to deliver the unpleasant message of warning. Lesson learned: A declaration of a public health emergency, or any other imminent danger, is not only an essential tool for responding to a disaster and/or providing recovery support, but often can be much more than that.

Joseph Cahill is a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

NANORAIDER™
Personal Spectroscopic Radiation Detector (SPRD-CZT)
for under than $10k

BECAUSE IT'S NOT JUST YOUR JOB, IT'S YOUR LIFE.™

The difference between life and death is in your hands. FLIR CBRNE threat detection products provide lab-caliber analysis where you need it most – in the field. When lives are at stake you need fast, accurate results you can trust.

FLIR®

www.FLIR.com/gs

Partnering: A Key to Effective Preparation & Response

By Thomas Moran, Private Sector

The All Hazards Consortium (AHC), headquartered in Frederick, Maryland, is a nonprofit organization focused on issues related primarily to homeland security, emergency management, and business continuity. Established in 2005, AHC started as a state-guided, vendor-supported organization. Over the past several years, the organization expanded its efforts to engage the private-sector owners and operators of the nation's critical infrastructure more effectively in order both to integrate planning efforts with the states and to enhance business continuity following a major natural or human-caused disaster.

The Regional Integrated Systems and Planning Initiative was launched by AHC in January 2011 and focused on integrating – into federal, state, and local government planning processes – the private sector from a broad spectrum of important "lifeline" communities: energy, transportation, telecommunications, food, water, finance, medical, chemical, and information technology.

To begin the building of a better integrated planning process, six AHC workshops were held in 2011 and 2012 attended by numerous representatives from those lifeline communities. More than 150 companies, most of which are owners and operators of critical infrastructure, were represented at the workshops, helping to further expand the association's new business-continuity efforts. Later, at the AHC's Annual Board Retreat in July 2012, a joint planning meeting with owner operators and state representatives continued to polish and upgrade the short- and long-range plans for building and carrying out an even more long-term integrated planning framework and joint exercise program needed to build sustainability.

Super Storm Sandy: A Massive Disaster & Unprecedented Response

A major and unscheduled real-life test of what has been accomplished to date started with only a few days' warning in October 2012 when so-called Super Storm Sandy barreled up the East Coast of the United States, making landfall in several Northeastern states and leaving one of the largest geographic footprints in the nation's history. Most of the state and local governments in the "target area" were quickly overwhelmed with requests for support. Private-sector organizations and businesses also needed government assistance during their own response efforts.

In New Jersey, the State Emergency Operation Center quickly activated its Private Sector Help Desk, an action that proved to be particularly helpful in coordinating efforts between the companies and agencies that were responding and those that were in need. Fortunately, the AHC had already worked with the Private Sector Help Desk and was engaged in several integrated planning programs and projects, so it was able to work more effectively with its own members and partners to quickly provide the broad spectrum of donated services needed to support both the private and public sectors in their own response efforts. Following are a few examples of the specific actions taken:

- Daily private-sector resource reports were issued that included "open/closed" status reports on the location and availability of thousands of food, fuel, pharmacy, and hotel accommodations;
- Regional rail alerts were provided – by the Association of American Railroads (AAR) – to keep states, local communities, and owner/operators informed of rail-related incidents and operational status;
- Citizen protection measures were initiated to provide a pro-bono social media service that alerted New Jersey's emergency operations center/fusion center, and more than 50 companies, to a broad spectrum of helpful information that could be used to save lives, rescue stranded citizens, and protect property;
- Power/utility fleet movement was significantly expedited through toll stations by using a jointly developed process created by state agencies and private-sector companies; and
- The "housing crisis" created by the super storm was addressed in emergency meetings that identified thousands of potential housing units that might be available to support local citizens and emergency workers.

A Widespread Disaster & The Public/Private Response

All of this information, and more, was provided by private-sector partners to the AHC, which then resolved many if not quite all of the business/legal/competitive issues involved. It then was able to distribute the upgraded information to the correct people and organizations in government and/or the private sector. To cite but one example: In the daily private-sector resource reports, Hughes Network Systems – a major provider of satellite broadband – provided data on the "power up/power down" status of their customers in the pharmaceuticals, fuel, fast food, and lodging businesses. The Hughes data was first compiled and inserted into a basic spreadsheet. Thousands of data points were then created, each of which indicated the "potential" availability of services at specific locations.

The new upgraded information then was distributed to officials throughout the affected region – by the second day of the response efforts to the super storm. Significantly, the same data also was used by the Federal Emergency Management Agency (FEMA) in its daily White House briefings and for the pre-positioning of federal assets.

By using established programs and the skills and resources of existing relationships and partners that had been developed over more than seven years, the AHC was able to coordinate assistance and services for many agencies, organizations, and individuals – without interfering with the operational efforts of various states. This private-sector effort helped significantly to reduce the heavy workload suddenly imposed on government response agencies – and, not incidentally, to provide a liaison service that could assist government agencies and private-sector companies in a number of other ways, including the following:

- Delivery companies used the power outage reports to determine which stores could receive shipments and redirect the truck drivers accordingly;
- Major employers used private-sector resource reports to assist essential personnel in getting to work;
- Power crews used the same reports to determine where they could purchase fuel and/or find hotel rooms;
- To ease traffic congestion on toll roads, power company vehicles traveling from outside the region were directed by government officials to use the right-lane tollbooths and simply leave a business card for billing at a later time; and
- Working with housing database firms, thousands of potential housing units were identified for citizens who had been displaced by the storm throughout the two states hardest hit: New Jersey and New York.

Future Outlook: Additional Programs & Services; Better Communications

Secretary Janet Napolitano of the U.S. Department of Homeland Security telephoned the AHC, the month after Sandy made landfall, to thank the members for their outstanding support and continuing assistance during the storm.

But that is not, of course, where the story ends. Looking forward, the AHC is now making plans to: schedule annual exercises with its private-sector partners; leverage its relationship with FEMA more effectively; promote the further integration of public and private partners; launch a new membership program for individual citizens and small businesses; offer a broader spectrum of owner/operator services; and further develop the multi-state "enabling framework" the association has been working on since 2005.

Collectively, all of the 2013 goals of creating a low-end membership program, providing sustainable services, and building better communications between and among stakeholders address a desirable goal that has resonated not only in the states directly affected by Sandy but also across the entire nation over the past few years: economic resilience.

Thomas (Tom) Moran serves as the Executive Director for the All Hazards Consortium, a regional 501c3 organization focused on multi-state homeland security and emergency management issues in the mid-Atlantic and North East regions. He spent more than 20 years in the communications and technology industry working in the areas of marketing/sales, customer service, and organizing national user groups. Before retiring, he spent nine years serving as the corporate executive liaison to state government leadership on all matters including strategy, contracts, legal, and operations. Educated in mechanical engineering at the University of Maryland, he has been a Maryland resident all his life and has owned several businesses.

Preparing Health Professionals & Emergency Managers in 2013

By Jack Herrmann, Public Health

For four days (12-15 March 2013), public health and healthcare professionals, emergency managers, and other leaders from across the nation will convene in Atlanta, Georgia, for the 2013 Public Health Preparedness Summit. The eighth annual Summit will provide a national forum for attendees to collaborate, learn, and share best practices to enhance their preparedness work long after the Summit concludes. As this difficult budgetary climate persists, the challenge has become not only doing more with less, but implementing innovative strategies and integrated systems to protect the nation's public health. These challenges will be addressed with this year's conference theme, "Strengthening Public Health and Healthcare Preparedness Through Innovation, Integration, and Implementation."

The Summit will offer an exciting and informative agenda. Twenty-nine hands-on workshops will provide in-depth training from experts in the field and continuing education opportunities for attendees. "Sharing," "Interactive," and "Ignite" sessions will cover a wide range of topics from disseminating risk communications to incorporating vulnerable populations in planning to developing strong and varied partnerships. Three engaging plenary sessions will provide a strong foundation for the Summit and will reinforce lessons learned.

Tuesday's opening plenary session, entitled "A Community United: An Integrated Response to the Aurora Mass Shooting," will feature officials from the Tri-County (Colorado) Health Department, the University of Colorado Hospital, and the Aurora Mental Health Center, who responded to the mass shooting on 20 July 2012. The speakers will highlight the key areas necessary to facilitate the response, including ESF-8 (Emergency Support Function #8 – Public Health and Medical Services Annex), behavioral health, patient tracking/family reunification, and partnerships with state and local authorities.

Wednesday's plenary session, entitled "To Stay or Go? What Sandy Taught Us About Hospital Evacuation and Healthcare Preparedness," will be sponsored by the Center for Biosecurity at UPMC. Officials from the U.S. Department of Health and Human Services' (HHS) Office of the Assistant Secretary for Preparedness and Response, Inova Health System, and Harris County (Texas) Public Health and Environmental Services will discuss the questions and lessons learned from hospital evacuations during Hurricane Sandy in October 2012. The speakers will highlight the importance of preparing for medical surge, onboarding additional medical staff, and resolving credentialing and insurance issues.

Lastly, Friday's closing plenary session, entitled "Great Expectations: Maintaining Public Trust and Instilling Confidence Before, During, and After a Disaster," will be moderated by ABC News' Chief Health and Medical Editor, Dr. Richard Besser. Panelists include: Dr. Nicole Lurie, Assistant Secretary for Preparedness and Response at HHS; Richard Serino, Deputy Administrator at the Federal Emergency Management Agency; Dr. Ali S. Khan, Director of the Office of Public Health Preparedness and Response at the Centers for Disease Control and Prevention; Jerry DeFrancisco, President of Humanitarian Services at the American Red Cross; and Marisa Raphael, Deputy Commissioner of the Office of Emergency Preparedness and Response at New York City's Department of Health and Mental Hygiene. They will discuss how federal, state, and local officials can shape public expectations prior to a disaster and take control of the messages after a disaster, even in light of the increasing role of traditional and social media.

Conference attendees will have the opportunity to acquire the tools, resources, and networks needed to advance their work and to integrate and implement innovative strategies into future preparedness activities. Additional information on the 2013 Public Health Preparedness Summit can be found at www.phprep.org.

Jack Herrmann is the senior advisor and chief for public health preparedness with the National Association of County and City Health Officials (NACCHO). In this role, he oversees the organization's public health preparedness portfolio, which is aimed at strengthening the preparedness and response capabilities of local health departments. He also serves as the organization's chief public health preparedness liaison to local, state, and federal partner agencies, and chairs the annual Public Health Preparedness Summit. He has extensive experience in disaster management and response and has participated in numerous disaster relief operations with the American Red Cross. He holds a bachelor's degree in sociology from St. John Fisher College, and a master's degree in counseling from the University of Rochester (New York).

Implementing the National Health Security Strategy

A Five-Part White Paper Series by

RADM Craig Vanderwagen, M.D.

Founding Assistant Secretary for Preparedness and Response,
U.S. Public Health Service - Retired

The strategic goal of delivering needed supplies and people to populations during disaster events, natural or manmade, is to save lives, reduce the burden of suffering and to speed recovery to a new normal after an event. This white paper series explores the role and requirements for a system of information management in directing and utilizing medical and public health assets in preparation of and responding to events.

White Papers Now Available for Download:

Part 1: The Role of Logistics in Public Health Practice
Part 2: The Role of Patient Tracking in Public Health Practice
Part 3: The Public Health Challenge in Mass Evacuation & Shelter Care
Part 4: Event Management: Visibility in the Fog of Response
Part 5: A National Strategy: It Is Time For Action

Watch Dr. Vanderwagen in a video preview of each white paper at **upp.com/vanderwagen**

From August 2006 until July 2009, **Dr. Vanderwagen** was the founding Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services.

White Paper Series Underwritten by:

Upp Technology, Inc.

800.777.6092 | upp@upp.com

innovative technology solutions

Download the White Papers today at **upp.com/vanderwagen** or scan this code.