domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 8 Issue 11, November 2012

BIOTHREATS

MAKE THE TRANSFORMATION FROM

CHAOS TO CONTROL

Broken

Waiting for Parts

Unknown

Recalibrate

Software Error

Need Training

Out of Service

Check Failed

Missing

Maintenance Management for HazMat/CBRNE Instruments

READY

- FTIR including HazMatID™ & TruDefender
- Raman including FirstDefender
- PID including MultiRAE
- SCBAs
- Gamma spectroscopy including IdentiFINDER™
- GC/MS including Inficon HAPSITE
- IMS including Sabre 4000™ & RaidM
- ECL including M1M

Reduce service costs without compromising readiness.

Do you have HazMat/CBRNE instruments in multiple locations and vehicles? Backlogs of repairs? Missing equipment? Dozens of vendors and maintenance contracts? Does your success depend on knowing that mission-critical instruments are 100% operational and ready to go? **How do you manage?**... Sticky notes? A spreadsheet?...It's time to take control.

Now, with KD Analytical Instrument Maintenance Management, CBRNE/HazMat teams and fire service personnel can ***take control of instrument chaos for as little as $100 per month!***

- **Receive one-call support** for all instruments in your kit.
- **Reduce maintenance and repair costs up to 30%.**
- **Increase availability of equipment up to 60%.**
- **Resolve issues quickly** with **ReadiTrak™, a web-based instrument maintenance management system** that provides unprecedented visibility and accountability for equipment status as well as instant access to the most complete library of instrument maintenance and repair documentation and FAQs available.

KD ANALYTICAL

Learn more at kdanalytical.com/mm or call 1-866-308-7102.

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

Staff
Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

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

Catherine Feinman
Associate Editor
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

American Military University (AMU)

AVON Protection

BioFire Diagnostics Inc.
(Formerly Idaho Technology)

Booz Allen Hamilton (BAH)

FLIR Systems Inc.

KD Analytical

PROENGIN Inc.

Upp Technology Inc.

Witt Associates

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

In the second half of the 20th century, the primary and most urgent concern of military and civil defense planners was the possible outbreak of a nuclear holocaust. Today, there are a growing number of nations, and even a few terrorist groups, that already possess or might soon have access to what are generically described as weapons of mass destruction (WMDs) or more commonly known as chemical, biological, radiological, nuclear, and explosives (CBRNE).

Biological weapons pose a special challenge to today's emergency planners. In the Middle Ages, the bubonic plague killed anywhere from one quarter to one third (even today the estimates vary) of the population of the entire world. In the 20th century, the biggest killer was not the bloody wars and insurrections that took tens of millions of lives, but the so-called Spanish Flu. The biggest killer of all, though, has been smallpox. Fortunately, smallpox has been totally eradicated. Or has it?

Eight highly knowledgeable contributors address that literally life-or-death question in this month's issue of *DPJ*. Craig Vanderwagen leads with a comprehensive discussion of biological weapons in general, focusing particular attention not only on smallpox and the plague but also on anthrax. The prevention of and/or recovery from anthrax or other biowarfare weapons, including the spread of infectious diseases, he points out, is possible – but is by no means guaranteed, primarily because the advance planning carried out so far has been woefully inadequate.

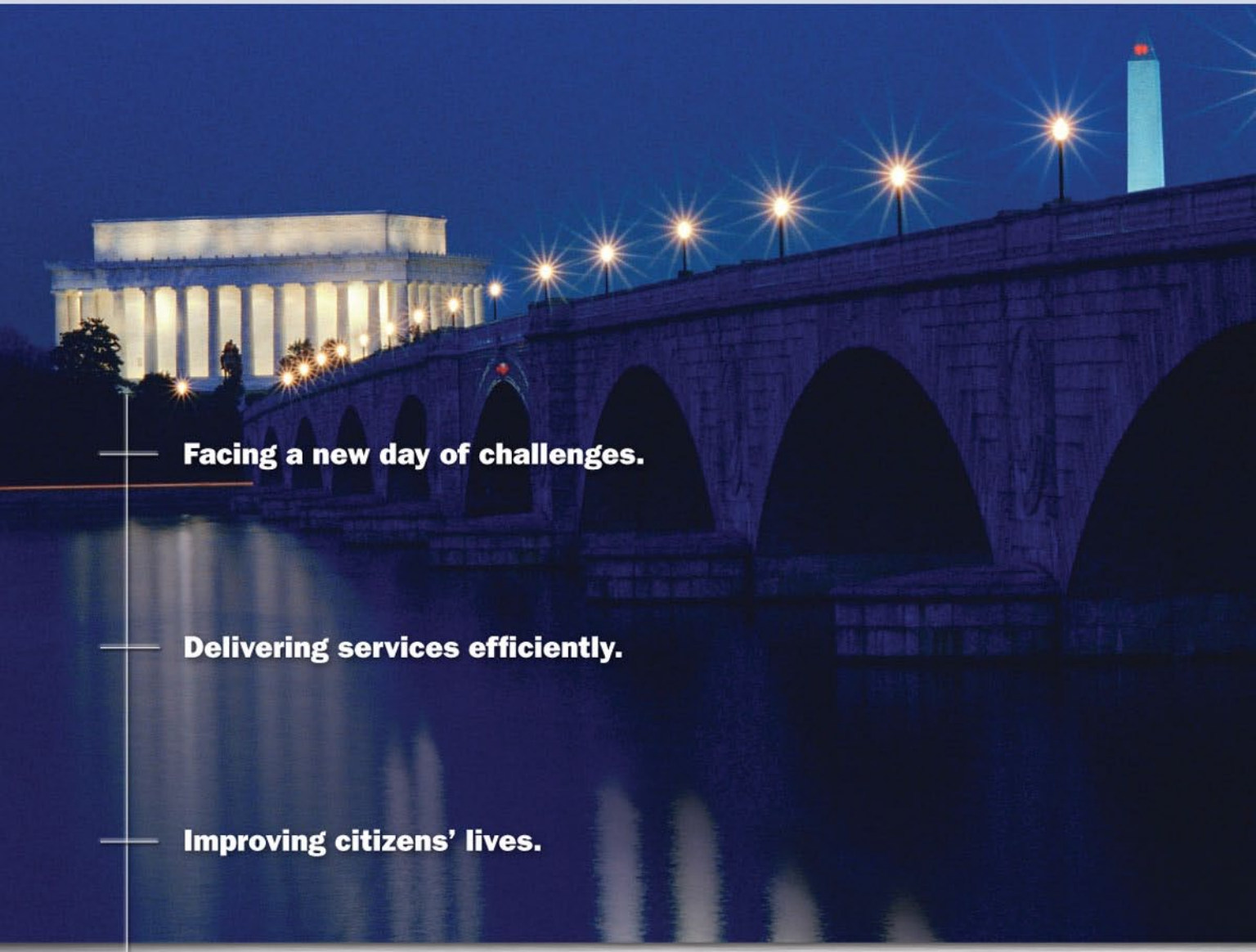
James J. Augustine agrees, and points out that it is possible, even with current high-tech systems, to detect infectious diseases in their earliest stages, but the purchase and use of such equipment has not been a high priority for the U.S. government. Perhaps the greatest need of all, says Patrick Rose, is an effective, highly sophisticated, and extremely reliable early warning system.

Even after the 9/11 attacks, Richard Schoeberl notes, several reports were written and comprehensive legislation was enacted – but with little lasting effect, primarily because of funding cuts and leadership failures that led to failing grades from the WMD Commission. Dennis Schrader gives special attention to the need for national resilience – a perhaps impossible dream in the immediate aftermath of a biological-warfare attack.

Rounding out the issue are closely related articles/reports/commentaries by: (a) Craig DeAtley, who discusses the supply and logistics problems related to the OPODs and CPODs (open and closed points of distribution); (b) Joseph Cahill, who uses a gridiron example to point out that the equally important support-staff requirements also are given less attention than is or should be mandatory; and (c) Raphael Barishansky, who is brave enough to point out that – as Hurricane Sandy recently proved – the best articulated, most effective, and "most likely to succeed" contingency plans are seldom fully funded.

About the Cover: This iStock photo of a laboratory assistant about to enter a quarantine area serves as a timely reminder that the protection of support staff personnel is and must be one of the highest priorities of emergency planners at all levels of government.

STRATEGY & ORGANIZATION | TECHNOLOGY | ENGINEERING & OPERATIONS | ANALYTICS



Facing a new day of challenges.

Delivering services efficiently.

Improving citizens' lives.

Ready for what's next. The most important challenge today is the mission of government—from national defense and economic security to health, citizen services, and international development. For nearly a century, the strategy and technology consultants of Booz Allen Hamilton have partnered with clients to nurture innovative ideas and drive them forward to tangible results. Today, we're proud to help government prevent cyber attacks, reform the financial system, and modernize infrastructure. Our 25,000 dedicated people do important work, with exceptional colleagues, where a spirit of service thrives. Booz Allen understands your toughest problems, and with collaboration and deep technical expertise, we're bringing solutions to help you meet your mission. Whether you're managing today's issues or looking beyond the horizon, count on us to help you be ready for what's next.

Ready for what's next. www.boozallen.com/rfwn

Booz | Allen | Hamilton

delivering results that endure

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Bruce Clements
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

Theodore (Ted) Tully
Health Systems

Biodefense: Eliminating the Threat

By Craig Vanderwagen, Emergency Management

In the biowarfare field, effective preparedness is the key to mounting a successful response, and preparedness begins with a strategic assessment of the threats and risks involved and a clear focus on the means available to counter those threats. Today, there are numerous agents – anthrax, smallpox, plague, and a broad spectrum of other organisms – that can be used as weapons of terror, either by state or non-state actors. That same list includes infectious agents that not only are highly lethal but also may be spread in a variety of ways that can affect a large number of people within a very short time frame. There are also toxins, such as botulinum toxin, associated with infectious agents that pose major threats.

By accepting the facts that these threats are real and that delivery of these agents is not only feasible but also a deliberate goal of those who want to do harm to the United States, appropriate planning and training processes can be developed to robustly address the threats. Marshaling the human and material assets needed, and training and exercising them for probable use if and when an attack does occur, are essential aspects of an effective preparedness posture, which also should include the development and acquisition of the specialized medical countermeasures and equipment systems needed to protect the population. Fortunately, significant progress already has been made in the development of: (a) the newer vaccines required to prevent illness; (b) the improved treatment modalities – monoclonal and polyclonal antibodies, for example – that can protect against toxins as well as organisms; and (c) new generations of antibiotics that will be more effective than their predecessors. Many of these resources are now in the Strategic National Stockpile, but more sustainable means of assuring their quick and continuing availability must still be developed and implemented.

The current U.S. planning process is, however, predicated on the ability to know when and where to deploy these capabilities and material resources. To begin with, there must be an identified "trigger" – that is, a clear signal that a specific known infectious agent is already in the environment and has been released – before action can be initiated. For that reason alone, early biodetection is a critical aspect of the preparedness planning and implementation process and can be achieved by a variety of means (some of them more timely than others).

Biodetection to Initiate Action

Ideally, early detection will lead to a swift intervention that provides the maximum protection for the affected population. This is particularly true in situations involving anthrax, because it is well known that the provision of antibiotics and vaccine within the first 48 hours after exposure to anthrax spores reduces both the number of cases that develop and the number of probable deaths. Again, in an ideal world, detection within a very short time frame – ranging from several minutes to only a few hours after release of the spores – would be of significant benefit.

New technologies already exist that permit the remote sampling of environmental air needed not only to identify the presence of threatening organisms but also to transmit that information within three hours of the sample collection. This is a major improvement over the current 24-36 hour limit required for environmental detection. The new technology, however, has not yet been deployed because: (a) there are legitimate questions to be answered about false positives and negatives; and (b) certain other (non-technical) issues also must be resolved.

Among the other means used to detect the presence of a threat are clinical syndrome surveillance and the analysis of clinical laboratory information. The term "clinical syndrome surveillance" relates to the monitoring of certain clinical signs and symptoms, reported from emergency rooms and other medical care facilities and typically associated with the identified threat. The "signs and symptoms" refer to a relatively late set of events indicating that a particular threat agent has been in the environment long enough to cause clinical illness.

In practice, though, any responses generated in these circumstances usually would not be as effective as desired in preventing future illnesses and deaths, primarily because activation of the response system would by definition be much later than the emergence and dissemination of the disease-causing agent. Nonetheless, with many diseases and in many communities, this information might well be the first indicator that an infectious-agent event has begun. Various clinical laboratory tools may provide specific identification of the agent or agents involved – and these tools, even when used late in the exposure process, would still be useful in confirming and measuring both the time of exposure and the specific agent(s) identified.

Response, Recovery & Protecting the Protectors

After an infectious agent has been identified in the environment, an effective response should be directed and the assets needed quickly deployed. The effectiveness of any given response may vary considerably, depending upon the agent itself. In some cases (usually associated with bacterial diseases), antibiotics should be the first line of response. In other cases (usually viral illnesses), the use of vaccinations is the most effective approach. In all cases, though, medical surge assets are urgently needed and require the deployment and distribution of people, medicines, medical supplies, and other tools and equipment – ventilators, for example.

The effectiveness of medical surge responses is highly dependent upon the effectiveness of the planning and exercising phases of the long-term preparedness plan. The anticipation of probable needs, combined with the identification and training of the systems of care likely to be involved, are the usual determining variables that lead to saving lives and reducing the overall burden of illness. To some degree, the protection of healthcare workers themselves, and their families, is also a critical factor that must be taken into consideration to ensure that the response personnel needed are both healthy and quickly available. Specifically *how* the protection of healthcare workers is or should be provided is another major issue that has not yet been resolved.

Lastly, recovery to a new, higher, and more complex definition of "normal" offers significant challenges – for example, how the potential lingering effects of certain agents are or should be mitigated or remediated. Perhaps the most significant example, particularly in anthrax cases, involves the removal of remaining spores – a huge challenge, obviously, when a major metropolitan area such as New York City has been the target of a terrorist attack. The removal techniques may be simple in some cases, but in other cases not only very expensive but also very time-consuming.

Deterrence: Critical Questions & Assumptions

Another critical question that must be considered is whether the level of spores remaining in the local environment has returned to an acceptable level – one that is safe for the return of the local population. Working on the assumption that 100 percent removal may be required, in most if not all situations, that complex question still requires a major policy answer at all levels of government. Whatever the answer, though, the adverse impact on the economy, and to the American people at large, may be so great that any pre-event assumptions would be of little or no practical use.

If all of the above elements are demonstrated to be in place and effective response and recovery operations might reasonably be expected – and, in fact, demonstrated through drills and exercises – then the goals of saving lives, reducing the burden of illness, and recovering to a new standard of normal can be achieved. In addition, and of perhaps greater importance, the threat itself may be deterred. In other words, the demonstration by any community, large or small, of a much improved ability to respond and recover from an infectious-agent attack might in itself reduce the possibility of an attack such as that described here.

The heightened preparedness and response posture and capabilities of communities throughout the nation therefore would serve as a deterrent, and that would be another important reason for undertaking the considerable and difficult efforts involved. By lessening the probable impact of biothreat attacks, the nation thereby would also lessen the attractiveness to would-be terrorists of using biowarfare weapons. The ultimate goal of the national strategy for biodefense, therefore, should be not merely to respond to and counter the threat, but to eliminate it completely.

Craig Vanderwagen, M.D., is a Senior Partner with Martin, Blanck, and Associates (MBA). His most recent government post prior to joining MBA was as Assistant Secretary for Preparedness and Response, 2006-2009, for the U.S. Department of Health and Human Services (HHS). Dr. Vanderwagen has a special interest and significant experience in biodefense, domestic disaster preparedness and response, international humanitarian and disaster response, federal health delivery systems, innovative organization development and evaluation, and cross-cultural healthcare.

Designing a National Infectious-Agent Detection System

By James J. Augustine, Health Systems

Local hospitals often serve as the focal point of health preparedness and response programs in communities across the nation. During and after most crisis situations, therefore, a hospital's emergency department (ED) becomes the epicenter for the diagnosis and treatment of survivors. This status gives them the ability to design the hospital-centered surveillance programs and detection technologies needed to cope with future biologic incidents. As a corollary, the incorporation of additional detection, analysis, and reporting tools into the hospital ED resource inventory can serve as a valuable pathway to build the more effective incident management system needed to deal with all types of biologic threats – both natural and manmade.

The design elements of such a program are already used in such medical incidents as trauma or hazardous materials contamination, and typically encompass most or all of the following elements:

- A threat to community health;
- A facility designed for the management of information relevant to the patients involved, whether presenting themselves one at a time or in groups;
- A reliable method to provide accurate and timely diagnoses of the health threat;
- A reliable system of analysis (often linked with a regional healthcare coordination system);
- The medical systems needed for the safe management of patients contaminated by and/or exposed to the specific health threat involved;
- Links to the community's overall emergency system and to timely public health education systems; and
- The other systems of various types needed to mitigate the adverse impact on the community.

The principal component or step lacking in the current system is a reliable method for the timely, accurate, and reliable detection of diseases related to biologic agents. It seems likely, though, that evolving technology will resolve this issue, if and when applied in a uniform manner to EDs throughout the nation.

Critical Components of the Biologic Threat-Prepared Hospital

In contrast to the visible immediacy of a plane crash, a bombing, a nuclear incident, or a chemical exposure, a biologic incident can, for an extended period of time, be rather difficult both to detect and to specifically identify. It is crucially important, therefore, to reduce the identification time as quickly as possible when clinical cases start to appear.

Unfortunately, the early symptoms caused by many infectious agents can be and often are mistaken for relatively common clinical ailments. If a large number of patients are seen and quickly released before the first "identifiable case" is recognized, several opportunities both to initiate treatment and to quarantine contacts may be missed.

Because very few people can secure a medical appointment with their doctors on a "same-day" basis, it is very likely that the unsuspecting survivors of a natural event or a bioterror attack will seek care in the EDs of local hospitals. For that reason alone, it makes sense to concentrate a community's diagnostic, surveillance, and treatment resources at these facilities. As previously indicated, however, the time frame needed to successfully recognize and quarantine a bioterror agent may be rather short, so the capacity to mount an effective public health response should not depend on a fortuitous diagnosis by an overworked clinician.

Infectious Agents, USPS Precedents & Computerized War Rooms

To address this specific, but likely, problem, there are two measurably effective operational tools that would be particularly valuable: (a) an infectious-agent detection system; and (b) a data-analysis system to measure ED flows. Following is a brief summary about how each of these tools could be used.

First, a simple but effective infectious-agent detection system could be created, using polymerase chain reaction (PCR) identification, by tapping into the tools already being used for environmental surveillance. More specifically, three types of detection devices could be developed: (a) a "breathalyzer" for patients exhibiting any respiratory symptoms; (b) a "sniffing" system to examine the skin and clothing of persons known or believed to have been exposed to airborne agents; and (c) various analytical devices that could be used to examine

body secretions for the detection of agents that predictably would be excreted during the typical disease process. Many if not all of these systems would use detection-device technology – similar to what is used by the United States Postal Service (USPS) – to trigger alarms and activate automatic notification systems that would immediately alert operational and supervisory authorities.

The second "operational tool" mentioned above would require more widespread use of data analyses of ED flows, particularly those relating to specific symptom complexes and/or laboratory tests that indicate the presence of an infectious disease. The electronic patient-tracking systems of EDs, therefore, should be arranged to feed data into a public health "war room" at regional departments of public health. Over a relatively short period of time, computerized analyses would yield both hour-to-hour and day-to-day "profiles" of the normal ebb and flow of patient visits to the EDs.

If and when medical workers detect a sudden increase in ED visits related to a particular complaint or diagnosis, they can contact emergency staff, request additional information, and require all personnel involved to approach such cases with a higher degree of suspicion. If a particular pattern is sufficiently worrisome, additional staff may be dispatched to examine and, if necessary, quarantine not only the patients involved but also their visitors and other contacts.

Funding Challenges, But a Unique Opportunity

The application of these tools and technologies should and usually would result in the building of an ED biologic-agent sentinel surveillance system. It is clear that combining public and private funding resources has in recent years become a critical factor in preparedness planning, but a system such as that described here would provide the budgetary framework needed to justify the investment required.

More important, though, is the fact that there is a unique opportunity now available for joint investments by the nation's federal, state, and local governments that can be carried out in conjunction with the many businesses, charitable organizations, and individual citizens who also want a higher level of emergency preparedness within their communities. In that context, it seems obvious that any federal funding provided for more effective emergency systems should be used to support the central roles of the emergency care system not only in overall community preparedness but also in syndromic surveillance and healthcare forecasting.

The time-sensitive need for technology upgrades related to the detection of biologic agents would modernize emergency departments throughout the nation to not only receive and process everyday patients but also to develop the physical, processing, and procedural changes required to develop and improve the all-hazards preparedness capabilities of all levels of government. In today's world, the term "hospital preparedness" means that all citizens have early access to critical medical services during a time of need. The development of a national ED-based surveillance system matches the need to further develop and improve the health and prevention efforts of all of the healthcare communities involved.

There have been times in the past when emergency physicians were either praised for their surveillance work or, in other situations, justifiably criticized because of their failure to detect or alert the community in a timely manner about a known or suspected health emergency. A program that applies advanced technology to quickly detect biologic agents, used in concert with an active surveillance and analysis program, would result in a time- and cost-efficient preparedness national network – one that could be used on a day-to-day basis.

James J. Augustine, M.D., is an emergency physician who serves with the Atlanta Fire Rescue Department and Hartsfield Jackson Atlanta International Airport. A Clinical Associate Professor in the Department of Emergency Medicine at Wright State University in Dayton, Ohio, he previously served as Chair of ASTM Task Group E54.02.01, which developed ASTM Standard E2413 on Hospital Preparedness, under Committee E54 on Homeland Security Applications. He also served as Chair of the Atlanta Metropolitan Medical Response System.

Building Resilient Regions
For a Secure and Resilient Nation

SPECIAL REPORT

Booz | Allen | Hamilton

delivering results that endure

KD ANALYTICAL

Save time. Save money. Guarantee readiness.

Upp

WITT ASSOCIATES

Download the full report,
Building Resilient Regions for a Secure and Resilient Nation

http://www.domesticpreparedness.com/userfiles/reports/dpj13nov12.pdf

On 13 November 2012, DomesticPreparedness.com hosted the "DomPrep Action Plan – Building Resilient Regions for a Secure and Resilient Nation" Executive Briefing at The National Press Club, in Washington, D.C. With a keynote by Thad Allen, Vice President of Booz Allen Hamilton, DomPrep40 Advisors led a discussion on gaps and synergies uncovered at six regional resilience workshops and through regional surveys.

Key points addressed include:

- A common language and a new way of thinking are needed between the public and private sectors;
- Resilience is a long-term goal that requires a change in the cultural norm; and
- There must be clear leadership to facilitate the sense of capability at the local and regional levels.

Attendance for this by-invitation-only event included representatives from various government, firefighter, law enforcement, and hospital agencies, as well as other private and public officials. Discussions and presentations were made, followed by questions and comments from the audience.

Planning Needs for Staff Medication Dispensing

By Craig DeAtley, Health Systems

Hospitals and other healthcare facilities order, receive, and administer medications to patients on a daily basis. However, not as routine is the issue of how to acquire and administer drugs to staff and their families during a biological incident. To address this potential response issue, a well thought-out plan is required. Healthcare facilities in Washington, D.C., have recently partnered with the District of Columbia Health Department to address this important response need.

Fortunately, the U.S. Centers for Disease Control and Prevention (CDC), working in coordination with local and state health departments, has already been encouraging local jurisdictions to develop comprehensive medical countermeasure programs for their own communities. A critical component of such programs is Points of Distribution (PODs), of which there are two types: (a) Open PODs (OPODs); and (b) Closed PODs (CPODs).

Healthcare facilities must be ready to provide medical countermeasures to their staff and family members in case of a biological incident. Creating a closed point of distribution is one way to accomplish this task.

Most OPODs are operated by health departments to provide medications to the general public during a biological incident. During and after such incidents many OPODs would be operated simultaneously to facilitate the distribution of medications as quickly as possible to adults and children in the community. Citizens coming to the OPOD can obtain oral antibiotic/antiviral medications for themselves and their family members – vaccinations/immunizations, however, require that each individual comes in person to receive the injection. Public messaging directs citizens to an open nearby OPOD. The availability of the OPOD streamlines the distribution of medications while at the same time minimizing the need for citizens having to go to a hospital in person to receive the medications.

CPODs are typically operated by businesses to distribute medications to their own staff and a designated number of direct family members. The purpose of using CPODs is to ensure that, to preserve their health, staff could receive needed medications in a timely manner and, therefore, would not have to go to a hospital or OPOD to receive the medications.

An important question frequently asked is: "Where do hospitals and skilled nursing home staff and their families receive their own medications?" Over the past two years, the District of Columbia Department of Health (DOH) has effectively fostered the development of PODs within D.C. Those efforts have been very successful both in creating and exercising the two types of PODs. More recently, an intense effort has been initiated to encourage D.C. healthcare facilities to become CPODs.

Public-Private Partnership Planning

To assist healthcare facilities in developing a CPOD, a four-step process has been described in a *Closed POD Dispensing Planning Guide*. The *Planning Guide*, created and distributed by the DCDOH, outlines – in a comprehensive but easy-to-read format – all of what a healthcare facility needs both to understand and to do in establishing a CPOD.

The first step involves executing a memorandum of agreement (MOA) with the local DOH – information on the MOA document is included in the *Planning Guide* materials. The MOA, which outlines the responsibilities of both parties involved, includes a stipulation that, in return for completing the outlined steps, the healthcare facility will, in an emergency, be provided the number of medications requested to cover its own staff and designated family members.

Managing the Process

The second step involves the facility devising a Closed POD Site Plan by using a planning template included in the *Planning Guide*. The same plan addresses a number of closely related topics, including outlining the incident command structure both to provide leadership to the CPOD operation and to integrate that operation into the healthcare facility's overall incident command system. The principal

positions assigned to provide the leadership needed are those of the Closed POD Coordinator and the leaders of three principal units: Forms and Queuing Unit; Dispensing Unit; and Logistics Unit. Job Action Sheets are written for each command position and provide suggested actions and outline reporting relationships. The Site Plan also spells out the throughput design – which encompasses, among other important duties and responsibilities: Greeting and Form Distribution; Form Screening; Medication Dispensing; and Special Assistance.

The number of lines established to maximize client throughput at any given healthcare facility is usually dependent on both the number of staff members available and the space needed to allow a redundant line design; ideally, of course, the greater the staff size, the greater the number of process lines that can be formed. Facility planning must also address such ancillary management issues as staff rotation, resupply, documentation, communications, and security.

To help familiarize the healthcare facility planners responsible for managing that facility's CPOD, the D.C. DOH has created and made available a series of training sessions described as "Step 3" in the overall process. These sessions help participants both to understand and to use the guidance materials available and to discuss the lessons learned from other facilities that have previously completed the CPOD process – specifically including the conduct of an exercise. After the healthcare facility has completed its CPOD plan, the plan is submitted, along with the signed MOA, to the DOH for its review and comments.

Training and Exercising

The final step of the CPOD process requires that the specific facility involved provides training to the healthcare staff designated to operate the CPOD. That training includes reviewing the plan, the incident command system (ICS) – and the individual roles and responsibilities assigned by the ICS – as well as the throughput system design and various documentation requirements.

Following the in-house training required, each healthcare facility conducts a full-scale operational exercise. During that exercise, the plan is implemented from the beginning and encompasses such important actions and responsibilities as: (a) the alert and notification process; (b) the system "set up" process; (c) medication receipts from DOH; and (d) the distribution of medications to the volunteer staff members arriving to receive them.

Following the exercise, all of the parties involved participate in an after-action discussion that not only leads to a comprehensive report being written but also lists various changes that should be made to the plan. Ideally, such exercises would be conducted annually to ensure adequate staff familiarization and implementation capabilities.

To briefly summarize, the potential for a community to encounter a biological incident requiring the distribution of medical countermeasures is a major planning concern for health departments across the country. No less important is for hospitals and other healthcare facilities to be ready to open a CPOD to provide medications to their staff and family members, thus optimizing staff responsibilities and capabilities by: (a) focusing on doing their own jobs during the crisis; (b) building confidence that their individual family needs also have been met; and (c) reducing the number of persons waiting in line at an OPOD.

Craig DeAtley is Director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region's largest hospital; he also is the Emergency Manager for the National Rehabilitation Hospital and co-executive director of the Center for HICS Education and Training. He previously served as an Associate Professor of Emergency Medicine, for 28 years, at George Washington University, and now also works as an Emergency Department Physician Assistant for Best Practices, a large physician group that staffs emergency departments in Northern Virginia, and has been both a volunteer paramedic with the Fairfax County Fire and Rescue Department and a member of the department's Urban Search and Rescue Team. He also has served, since 1991, as the Assistant Medical Director for the Fairfax County Police Department.

Not All Components Are Equal, But All Are Essential

By Joseph Cahill, EMS

Surprising facts are learned about even a relatively uncomplicated system when a small "piece" or component of that system is removed or not working as it should be. Without being privy to the discussions, the nation's football fans will probably never fully understand the thrust of the many closed-session talks between owners and on-field umpires and referees leading up to the recent "lockout" of National Football League (NFL) officials. It is now clear, though, that the owners reached the erroneous conclusion that experienced referees are not needed in the football "system."

The principal "components" of a professional football game include: (a) the players, of course; (b) the coaches and owners; and (c) the fans, certainly – not only those in the stands, but also the much larger number watching the game on television. If asked last year, many fans might have discounted the value of the referees; however, a very different answer would be given during the current season.

Most Emergency Medical Services (EMS) systems cannot simply shut off an essential support function – as the NFL tried to do. However, various vital components of all types of systems, both electronic and mechanical, sometimes fail of their own accord – or must be interrupted for upgrade or repair. During even a temporary cessation of a support function, the goal is to continue providing services and to keep the disruption virtually invisible to the end user. As with any other change, permanent or temporary, several steps must be taken for the change process to be successful.

The Starting Lineup – Computer-Aided Dispatch

For individual components of computer-aided dispatch (CAD) operations, for example, planners must begin by thinking through and documenting every step of the process needed to stay operational. Planners must work through the loss and/or malfunction of each part of the entire system to create many seemingly small plans that can be combined into what is sometimes a surprisingly large "playbook."

In today's high-tech world, interruption of the current support system often means falling back on earlier technology. When a CAD system fails and EMS assignments cannot be quickly and easily entered into a computer, pen and paper are usually the most obvious and sometimes only "replacement parts" immediately available.

The screens of most CAD systems may initially have been designed to emulate existing paper forms, but it is unlikely that this is still the case. In today's much more complicated high-volume support systems, it is often necessary to reduce, to the absolute bare necessities, the services provided to the end user(s).

In the case of CAD, there are a series of questions that must be asked as well as a parallel series of answers – many of those answers, though, lead to additional, but different, sets of follow-up questions. The end result is or should be an improved and, usually, more complete understanding of the medical emergency the caller might be reporting. For software programs with built-in logic that prompts the next question, even while answers are being recorded, this is a relatively simple matter – but does not always seem so on paper. When switching to paper, therefore, the decision "tree" may have to be shortened to maintain the speed necessary to cope with a major emergency of any type.

The Backup Quarterback – Pen and Paper

Paper backup forms should be upgraded to make the flow of the paper version – of a standard "form" of various types, for example – more like that of the on-line version. By doing so,

the operators working with the paper will become acclimated more readily if and when a breakdown occurs. The ultimate goal is to make the paper process as similar as possible to the electronic process.

It is not enough, therefore, simply to emulate the computer screens on paper and pack all of the backup components into a handy nearby box marked "break seal in case of emergency." Staff members *and* supervisors must be trained and exercised to promote a full and complete understanding of, and comfort with, such materials. For working purposes, this means that procedures that have been written but not trained functionally do not exist.

The final step in the process is review. Any loss-of-service event or incident should be written up as an after-action report in a format similar to that of any other major response event that occurs in the field. By enumerating the positive as well as negative lessons learned, planners can revisit and improve the backup plans previously developed. Similarly, every time the system is changed – to accommodate an upgrade of the CAD software, for example – the plan must be reviewed and modified as needed.

In short, by recognizing – as early as possible – that support services play a significant role in the successful operation of a system, and that detailed planning is critical to operational success when (not if) essential services are unavailable, leaders and managers can provide the guidance necessary to make not only the system as a whole but also each and every one of its vital components operationally successful at all times.

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 the 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.

Smallpox – Still a Viable Bioterrorist Threat

By Richard Schoeberl, Law Enforcement

The 9/11 terrorist attacks against the United States and, shortly thereafter, the mailing of anthrax spores to several news agencies and the offices of two U.S. Senators became evidence of the need to improve U.S. homeland security in general and the nation's biosecurity capabilities in particular. Congress and then-President George W. Bush responded to the national outcry by passing the Public Health Security and Bioterrorism Preparedness and Response Act of 2002 – also known as the Bioterrorism Act, which was signed into law on 12 June 2002. That Act, and other legislation since then, has significantly upgraded the federal government's capability to prevent, prepare for, and respond to future national health emergencies and unforeseen bioterrorism incidents.

The bioterrorist threat itself continues to spawn new federal programs, additional legislation, and even increased funding – approximately $60 billion since 9/11 – to combat what previously had been considered a relatively unlikely danger. However, despite these efforts, new intelligence reports and the concerns voiced by congressional commissions about the growing threat of bioterrorism attacks have brought significant attention to the level of security and preparedness needed – but still lacking.

Following the terrorist attacks of 9/11, it became apparent that even the most "unlikely" threats could in fact actually happen. For that reason alone, effective plans must be in place to prevent a remotely possible smallpox attack from becoming a reality.

On 12 February 2003, Central Intelligence Agency Director George Tenet said, in testimony before the Senate Armed Services Committee, that "We continue to receive information indicating that al-Qaida still seeks chemical, biological, radiological, and nuclear weapons." More recently, documents recovered from al-Qaida facilities in Afghanistan indicated that al-Qaida still "has a sophisticated biological weapons capability." Terrorists also continue to acquire bioagents – e.g., various types of bacteria, viruses, fungi, and toxins – all of which are valued by terrorists not only for their psychological impact on the public, but also for their potential to kill thousands of people quickly and easily, their ease of distribution, the difficulties involved in detecting them, and the maturation period of the infectious agents themselves. For numerous reasons, therefore, an authentic bioterrorism threat poses unique challenges for those responsible for preparedness, protection, and – perhaps of the greatest importance – an effective and timely response against such an attack.

Failing Grades From the WMD Commission

Despite the strong efforts already made to upgrade the nation's counterterrorism capabilities, numerous authorities – including congressional commissions, governmental and non-governmental organizations, and private industry – have identified the need to further improve the nation's biodefense strategies. The U.S. Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism – formed by Congress in 2004 to evaluate the U.S. government's readiness for a terror attack – warned the House Committee on Homeland Security in 2010, in fact, that "The threat of bioweapons being used by terrorists or rogue states has continued to worsen."

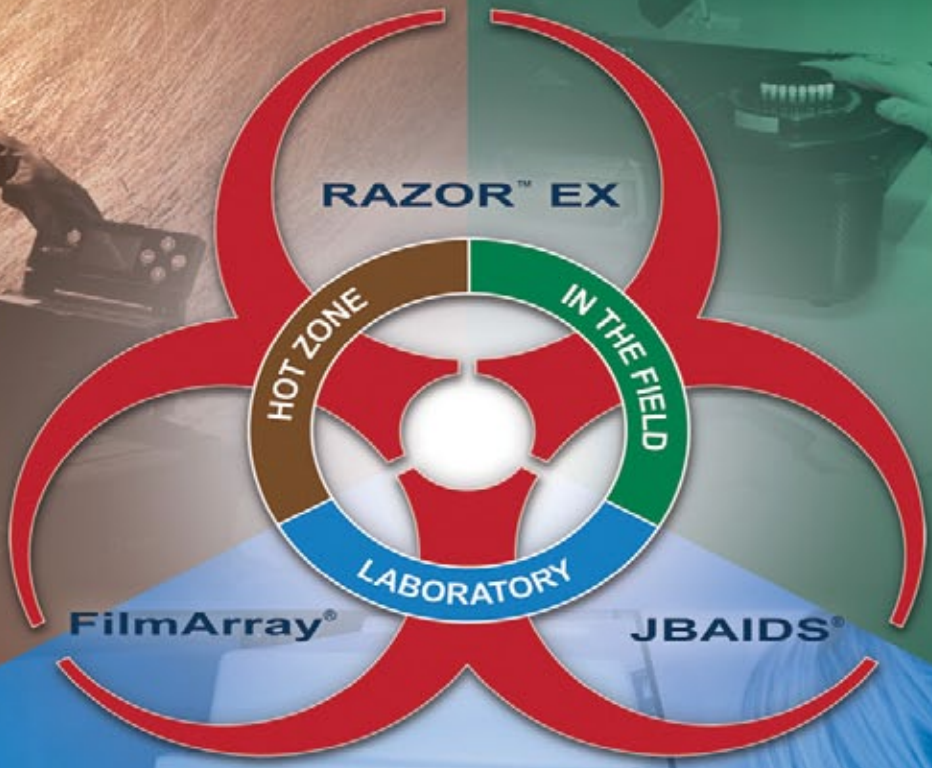
The Commission, co-chaired by former U.S. Senators Daniel Robert Graham and James Matthes Talent, also issued a "Report Card" (on 26 January 2010) on the efforts made thus far to address several of its earlier (2008) recommendations. In that report, the Obama administration's failure to "enhance the nation's capabilities for rapid response to prevent biological attacks from inflicting mass casualties" received a failing grade ("F" – meaning that no action had been taken on this recommendation). For its inadequate oversight of high-containment laboratories, the administration received an almost failing "D+."

"We no longer have the luxury of a slow learning curve," the Commission also warned, as yet another indication that the Obama administration is not addressing urgent threats, including bioterrorism. "Especially troubling," the Commission said, "is the lack of priority given to the development of medical countermeasures – the vaccines and medicines that would be required to mitigate the consequences of an attack."

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

Despite the failing grades and missteps – of Republican as well as Democratic administrations – the U.S. biodefense efforts of the past decade have, if nothing else, led to a greater understanding of both the lack of preparedness and the actual biothreat itself. That understanding has not only spurred the development and placement of new detection technologies, but also expanded the provisions in place for effective countermeasures. Nonetheless, the enactment of additional legislation, some of it still pending, to implement other Commission recommendations is needed to further enhance the nation's current biosecurity capabilities.

Smallpox Disasters – Still a Threat?

Largely because of a worldwide smallpox vaccination campaign carried out by the World Health Organization (WHO), naturally occurring smallpox has been successfully eliminated. According to the U.S. Centers for Disease Control & Prevention (CDC), the last reported smallpox case occurred in Somalia in 1977, and the virus has not infected anyone within the United States since 1949. Nonetheless, and primarily because of recent security concerns in embattled nations such as Libya and Syria, the use of biological weapons against civilian populations has once more become a real and present danger to the national security of the United States (and, of course, other nations throughout the world).

Currently, samples of the smallpox virus – an airborne virus that is extraordinarily contagious and extremely lethal – are now stored in only two laboratories, one in the United States and one in Russia, which are both closely guarded. Nonetheless, there are also some understandable concerns that a few other nations and/or organizations – including terrorist groups – might also have acquired samples of the virus at one time or another in the recent past. Moreover, even though naturally occurring smallpox seems to have been effectively eradicated, it might still be inexpensively replicated, both technologically and synthetically, and used as a terrorist weapon of choice.

Making smallpox an even more attractive bioweapon is that the maturation period of the virus ranges from 7 to 17 days. A human carrier of the virus thus could travel to numerous countries around the world without exhibiting any warning signs, while possibly spreading what could lead to an international pandemic. Even if the overall likelihood of a bioterror attack remains relatively low, the historical record shows that *any* use of the smallpox virus as a bioweapon would become a major international concern.

According to the CDC, the most common type of smallpox, variola major, had an approximately 30 percent death rate – and millions of other victims suffered major disfigurements. In the 20th century alone, smallpox killed an estimated 300 million people – more than the total number killed in all of the wars fought in all countries throughout the entire world during that century. Also, because there is no specific treatment for smallpox – beyond treating the visible signs and symptoms of the infection – the foremost concern is to stop the spread of the virus before it reaches epidemic proportions. In nations that do not possess the types or quantities of immunization to the virus that would be needed, stopping the spread of disease can be an even greater challenge.

Developing a National Plan

Securing and preparing the United States (and/or any other nation) to cope with the threat posed by bioterrorism requires that several additional actions are needed. The same WMD report that issued less than complimentary grades also recommended five steps the U.S. government itself should take to combat the threat of bioterrorism:

1. Conduct a comprehensive review of the current domestic programs already in place to secure dangerous pathogens;
2. Develop a national strategy for advancing the ability to conduct forensic analyses of bioterror attacks;
3. Tighten government oversight of the private-sector as well as government laboratories that deal with dangerous pathogens;
4. Promote a culture of security awareness among scientists; and
5. Enhance the nation's current rapid-response plans to prevent biological attacks from inflicting mass casualties.

To connect experts and build interoperability, the government should also continue to pursue a national biosurveillance strategy, including but not limited to: (a) sharing laboratory information; (b) investigating and researching the use of such unstructured data as information from the internet and social networks; (c) incorporating biosurveillance information where it is important and

reasonable to integrate; and (d) developing and promoting a global disease detection network.

On 31 July 2012, the Obama White House released a National Strategy for Biosurveillance, which stressed that a "well integrated, national biosurveillance enterprise is a national security imperative." The essential goal of that national initiative is to save lives by guaranteeing that key personnel have the correct information to make judicious decisions during a public health emergency. In addition, the National Strategy also calls for an interdisciplinary approach to biosurveillance in order to combine and integrate the information and knowledge available from areas beyond public health – e.g., law enforcement, the intelligence community, and the private sector.

In August 2007, the U.S. Congress established the National Biosurveillance Integration Center (NBIC) within the Department of Homeland Security to enhance the nation's capability to integrate all U.S. biosurveillance efforts. NBIC's biological common operating picture is a manually updated Google Map application that tracks biological events worldwide. The biosurveillance common operating network supports DHS's Google Map system and also monitors, tracks, and disseminates relevant information through a system called Global Argus – a global early detection and tracking system for biological events – which depends heavily on public information sources such as newspapers and the internet.

The mission of the NBIC further includes the ability to enhance the capabilities of the federal government to: (a) rapidly identify, characterize, localize, and track a biological event of national concern; (b) integrate and analyze data relating to human health, animal, plant, food, water, and environmental domains; (c) disseminate alerts and other relevant biothreat information; and (d) oversee the development and operation of the National Biosurveillance Integration System (NBIS) interagency community.

To briefly summarize, the threat of bioterrorism is real and smallpox is the most viable bioagent that might be used as a WMD. It is conceivable, in fact, that terrorists might reproduce and deploy various infected bioweapons because the educational materials needed are widely accessible throughout various public documents and internet resources. Moreover, although the likelihood of a bioterrorist attack seems to be very small, so too was the possibility that passenger aircraft would be used to fly into buildings and/or that makeshift bombs would be smuggled inside shoes or underwear.

As with any other type of terrorist threat, the U.S. government must find a safe and reasonable equilibrium between being prepared for a possible attack and effectively managing the financial and logistical costs associated with the preparations involved. Building partnerships, especially with other countries, is a critical step in building a higher level of biosecurity.

For additional information on:
The June 2002 Bioterrorism Act, visit http://www.fda.gov/RegulatoryInformation/Legislation/ucm148797.htm

The February 2003 Hearings Before the U.S. Senate Armed Services Committee, visit http://www.gpo.gov/fdsys/pkg/CHRG-108shrg91721/html/CHRG-108shrg91721.htm

The January 2010 "Prevention of WMD Proliferation and Terrorism Report Card," visit http://www.pharmathene.com/WMD_Report_Card.pdf

The July 2012, National Strategy for Biosurveillance, visit http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Biosurveillance_July_2012.pdf

CDC's Smallpox Fact Sheet, visit http://www.bt.cdc.gov/agent/smallpox/overview/disease-facts.asp

The NBIC, visit http://www.dhs.gov/national-biosurveillance-integration-center

---

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.

Early Warning: The Front Line of Biodefense

By Patrick Rose, Health Systems

Even before the post-9/11 "anthrax letter" attacks against the United States, some experts believed that a bioterrorism attack was not merely possible but highly probable. Since then, significant improvements in U.S. recognition and mitigation strategies have emerged, several different attack scenarios have been written and analyzed, and thousands of planning documents have been drafted to prepare the nation for another potential biowarfare attack. One result of these efforts is that the nation's biological threat-reduction and medical countermeasures capabilities have improved significantly during the past decade.

Whether the resulting technological advances and/or improved intelligence-gathering capabilities have dissuaded terrorists from launching another biological attack against the United States, though, is still not clear. Nonetheless, significant progress has been made at the federal and state levels of biodefense, thanks in large part to several initiatives establishing new and more effective response standards for potential biological disaster situations. However, the 2009 H1N1 influenza pandemic severely tested the nation's efforts, revealed serious gaps in the response system, and identified significant areas where additional planning and preparedness measures still must be developed.

Moreover, although several federal agencies and organizations – primarily the National Academy of Sciences' Institute of Medicine of the National Academies, the U.S. Department of Health & Human Services (HHS), the Food and Drug Administration (FDA), and the U.S. Centers for Disease Control and Prevention (CDC) – play key roles in supporting the capabilities needed to detect and respond to a bioterrorist event, past and pending budget cuts may impair the current biosecurity countermeasure efforts made by these and other agencies.

Early Detection Vs. the Surprise Element

Improving the technologies needed for predicting, detecting, and identifying a biological attack is only one component of the nation's overall biodefense process. During the response phase of a biological attack, doctors, nurses, and other healthcare providers must not only have available to them the effective medical countermeasures systems and equipment needed, but also should be properly trained to mitigate the spread of an infection – and thereby decrease the morbidity and mortality rates. It is particularly important during periods of scarce resources, though, that investments also be made to raise awareness among healthcare workers, who individually and collectively must be well versed in recognizing the signs of possible contagion among arriving patients.

Although most current bioterrorism efforts focus on anthrax and other toxic agents, the ability to recognize the early visible signs of these agents is of critical importance to keep the "surprise element" from overwhelming the nation's disease-surveillance systems. However, addressing the numerous challenges involved in incorporating preparedness training into the nation's healthcare-delivery system would be a daunting task, primarily because of the time, personnel, and funding required for such training. Nonetheless, when an ill person seeks assistance from a medical professional, that healthcare provider is in a strategic position to recognize the onset of what might well be a developing and more widespread problem. He or she therefore must fully understand and be able to take the proper steps needed to effectively address the serious risks involved.

At present, although most current medical practice involves the one-on-one patient care provided during a typical day, little if any training is required for recognizing unusual symptoms, implementing the treatment and isolation protocols required, and preparing for the crisis standards of care mandated should a medical surge or pandemic situation arise. After seeing 20 or more patients in a given day, a physician or nurse may not

Remote **BIOHAZARD** Detection

MAB
Portable Biological Alarm Monitor

Our MAB Portable Biohazard Detection System sends an alarm immediately upon detecting any evolution to the atmospheric background. It works on a continuous real-time basis and responds in only seconds. Easily used by untrained people, it has a very low power consumption rate and is especially designed for harsh environments.

MAB has a fast start-up time and can quickly analyze atmospheric particles for chemical signatures of bacteria or toxins such as anthrax, plague, Botox, legionella, etc.

MAB has already been selected by several military forces and is used by several NBC reconnaissance vehicles, as it is not sensitive to diesel vapors and smokes. Test reports are available.

Characteristics

- Size of the box (LxWxH): 300mm x 160mm x 470mm (11.8" x 6.3" x 18.5")
- Total height: 850mm (33.5")
- Weight: 14 kg (31 lbs)
- Operating temperature: -10°C to +50°C (14°F to +122°F)
- Storage temperature: -39°C to +71°C (-38.2°F to +160°F)
- Autonomy: 10 days (refillable hydrogen cylinder included)
- Power supply: 12 - 32 V DC / 110 - 220 V AC
- Can be remote controlled
- Remote data by RS 485 outlet
- Response time: less than 1 minute
- Field tested / Report available

www.proenginusa.com

PROENGIN

140 South University Drive, Suite F, Plantation FL 33324
(954) 760-9990 • FAX (954) 760-9955 e-mail: sales@proenginusa.com

readily remember the specific symptoms encountered earlier in the day, or over the past few days, thus missing an organophosphate poisoning, for example, or a case of toxic gas inhalation.

Compounding this problem is the fact that specific training in disaster management for students in most U.S. medical and nursing programs is, for most practical purposes, nonexistent. Numerous task forces have been formed, and their recommendations have been published – and some training programs developed – in the aftermath of several catastrophic events that have occurred over the past decade. But those resources are not necessarily being well used, or even implemented, throughout the nation's entire spectrum of healthcare agencies and organizations.

The Training Gap & Some Possible Solutions

To close this training gap, several forward-looking suggestions for rigorously implementing existing programs have been made, including the following:

- Using initiatives similar to the crisis-management training programs developed and used by the American Red Cross to train its volunteer healthcare workers and raise awareness in the use of crisis standards of care;
- Integrating the rotation of medical residents into existing programs that will expose them to public health and emergency preparedness education/experience; and
- Putting greater emphasis on early training and awareness programs to help healthcare workers understand their responsibilities and identify symptoms that might be out of the norm.

Greater investments in identifying early warning signs at the healthcare level would greatly mitigate the consequences of, and possibly even help deter, future bioterrorist attacks. Raising awareness also can reduce the "terror" factor that undermines the public's trust in the government's ability to protect the American people. When everyday citizens do not know how to react during an attack, the first place they usually turn to is the nearest healthcare facility. For that reason alone, and because healthcare workers are usually among the first to see those victimized by a biological attack, it obviously would be advantageous for them to be able, among other things: (a) to identify that an attack may have occurred; (b) to initiate the appropriate response mechanism required; and (c) to notify the appropriate government agencies.

Subsequently, those same citizens can develop greater trust and confidence in the care and advice received from healthcare workers, which in turn will help abate public fears related to the attack itself. According to a 2007 report from the Center for New American Security, "Many will ignore federal inputs if they are inconsistent with comments from state, local, and private officials, or from personally trusted individuals such as their doctors, their ministers, and their friends." With the efficacy of existing detection systems such as Biowatch – an "early warning" program managed by the Department of Homeland Security Office of Health Affairs – the next logical step would be to both augment and expand current syndromic surveillance systems and, at the same time, develop and train a new generation of healthcare workers with the aptitude to detect and respond to a bioterrorism attack.

For additional information on:
The Center for New American Security, 27 June 2007, "After an Attack: Preparing Citizens for Bioterrorism," visit http://www.cnas.org/node/127

The U.S. Centers for Disease Control and Prevention (CDC), visit http://emergency.cdc.gov/bioterrorism/

The U.S. Food and Drug Administration (FDA), visit http://www.fda.gov/BiologicsBloodVaccines/default.htm

The National Academy of Sciences' Institute of Medicine, visit http://www.iom.edu/

The U.S. Department of Health & Human Services (HHS), visit http://www.phe.gov/emergency/terroristthreats/Pages/default.aspx

---

Patrick Rose is a Senior Policy Analyst with the Center for Health & Homeland Security and a Fellow in the 2012 class of Emerging Leaders in Biosecurity Initiative at the Center for Biosecurity of the University of Pittsburgh Medical Center (UPMC). At the Center for Health & Homeland Security, he is part of the Exercise and Training Division working on the Homeland Security Exercise and Evaluation Program with various state and federal agencies. He also provides subject matter expertise to international delegations through the Senior Crisis Management Training, working in cooperation with the U.S. State Department Office of Anti-Terrorism Assistance. He has a Ph.D. in Microbiology and Immunology and is Adjunct Assistant Professor at the University of Maryland School of Medicine, Department of Epidemiology and Public Health.

Additional contributions to this article were made by:
Moulaye Haidara of the University of Maryland School of Medicine, a fourth-year medical student at the University of Maryland School of Medicine, who has been actively engaged in international public health initiatives on the epidemiology of infectious diseases such as malaria and tuberculosis. Haldara also has been heavily involved in matters related to the building of competent public health systems in West Africa, with special focus on unprepared and still developing healthcare systems. He plans, after graduation, to continue his medical training with a residency in Ophthalmology.

Biodefense – Protecting Public Health

By Raphael M. Barishansky, Public Health

For many citizens, the term "biodefense" conjures up images of suited-up response personnel looking into cracks and crevasses for potential threats, long lines of civilians awaiting medication, and worried public health officials addressing the nation as events unfold. The reality of planning for a biological attack is quite different. Nonetheless, a wealth of information must be analyzed not only for the past and present state of readiness to cope with such an attack but also for the future level of biological preparedness needed.

In the aftermath of the "anthrax letters" mailed shortly after the 9/11 attacks, U.S. public health and emergency management officials worked quickly to better understand the realities of the chemical, biological, radiological, and nuclear (CBRN) threats against the U.S. homeland. Special emphasis has been placed since then on planning for, and responding to, biological attacks. However, many biological agents – e.g., anthrax, plague, smallpox, and ricin – are extremely difficult to detect and may not cause discernible illness for periods ranging from several hours to several days. For that reason, as well as the potential of those and other agents to cause mass panic and disruption of the infrastructure throughout an entire city or state, biological agents also would be a particularly attractive weapon of choice for would-be terrorists.

Recent Developments And Presidential Mandates

In 2006, the Strategic National Stockpile (SNS), a division of the U.S. Centers for Disease Control and Prevention (CDC), began developing more robust detection tools and other resources to help state and local health departments increase their capacity to receive, distribute, and dispense SNS assets in the event of another major emergency or national disaster. In 2007, the CDC's

Technical Assistance Review (TAR) also started: (a) to collect and report data, as viewed from the federal level, of state and local readiness to receive SNS materiel; and (b) to analyze the plans, in accordance with the Cities Readiness Initiative (CRI), of numerous "Metro Statistical Areas" and use that data to upgrade the ability of such areas to ensure the prompt delivery of prophylaxis to their populations within 48 hours after the start of a significant public health emergency – an anthrax attack, for example.

The TAR also provides reviews of other critical criteria – including, but not limited to, the following: (a) the availability of the personnel needed to staff SNS point of distribution (POD) sites; (b) the percentages of the population covered by open PODs as opposed to closed PODs; (c) site security requirements; (d) POD site management; and (e) existing memoranda of understanding. The TAR scores are updated annually and made public.

Clearly, the use of biological agents by terrorists is still a major concern for the nation's public health and emergency management personnel. Some additional recent analyses and reports have addressed other aspects of the ever-expanding world of biological agents and the need to defend against them. The WMD Prevention and Preparedness Act of 2011, for example, requires, among other things, that:

- The President assign a member of the National Security Council to serve specifically as Special Assistant to the President for Biodefense;
- A national biodefense plan be developed;
- The Administrator of the Federal Emergency Management Agency (FEMA) assist state, local, and tribal authorities in improving and promoting their individual and community preparedness against – and their collective responses to – terrorist attacks involving CBRN materials; and
- Guidance and modeling to enhance the ability of emergency response providers to respond to an attack, including guidance for the dispensing of medical countermeasures, be developed.

Numerous challenges remain in both the U.S. public health infrastructure and the working relationships, at all levels of government, with the private sector. Through better cooperation and communication, the efforts underway should lead to an improved homeland security framework.

Fundamental Goals: An Interdisciplinary Approach Is Required

On 31 July 2012, President Obama, in his introduction to the National Strategy for Biosurveillance, focused on several important issues that must be addressed in the near future.

Two significant foundational themes, among others, were stressed in that document. First, the fundamental goal of the national biosurveillance enterprise should be to save lives by ensuring that leaders have the information they need to make timely decisions during a public health emergency. However, biosurveillance products are virtually useless if they are not also distributed and shared in a timely fashion, particularly at the local level.

Second, an interdisciplinary approach must be used to build a successful biosurveillance program – one that incorporates information and knowledge from sectors beyond health, such as law enforcement, intelligence, agriculture, the private sector, and others. Although there have been previous calls to better integrate existing federal biosurveillance efforts, there also have been several daunting challenges. This specific articulation by the White House of the importance of sharing and integrating information across all sectors is intended to help improve coordination and cooperation between and among the many private- and public-sector agencies and organizations. Future advances in technology, the advent and use of social media, and new scientific breakthroughs all provide additional opportunities to strengthen national biosurveillance capabilities.

The Highest & Most Difficult Hurdle: Funding Cutbacks

Although it is clear that biodefense is a critical area of concern for the nation's leaders, there also are other issues related not only to implementation and operationalization but also to cooperation and communication that must be addressed. First, there is a continuing need for sustained funding of the programs at the local, state, and federal

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

levels of government that support biodefense activities. More than two years ago, in fact, the Trust for America's Health – a non-government private-sector organization headquartered in Washington, D.C. – reported that there have already been numerous funding cutbacks adversely affecting this vital element of the public health infrastructure. More specifically, the Trust said, such cuts had been made on three levels, and included the following:

- *State cuts:* Of the 33 states and Washington, D.C., that cut funding for public health from FY 2009 to FY 2010, more than half were cutting public health preparedness funding for a second year in a row.
- *Local cuts:* In January 2010, 53 percent of the nation's local health departments reported that their core funding had been cut from the previous year, and 47 percent anticipated additional cuts in FY 2011. These and other reductions have resulted in a weakening of the "boots on the ground" capabilities of the public health infrastructure and led to the loss of approximately 23,000 jobs – an estimated 15 percent of the local public health workforce – in the two years since January 2008.
- *Federal cuts:* Since FY 2005, federal support for public health preparedness had been cut by approximately 27 percent.

Past & Current Difficulties, But Future Strengths

Clearly, in the years that have passed since the 9/11 attacks, there has been significant forward progress in building and improving the nation's biodefense capabilities. There was significant stakeholder cooperation, for example, specific to the National Strategy for Biosurveillance that helped outline some excellent points related to that doctrine's guiding principles and core functions. At the same time, the actual biosurveillance efforts taken at the local, state, and federal levels have been effectively "combat-tested" by such events as the 2009-2010 H1N1 flu pandemic.

Another consistent issue not yet adequately addressed is the true integration of public health emergency preparedness and response efforts into the homeland security framework. The role of public health at the federal, state, and local levels has become an important component of the nation's overall emergency preparedness efforts. As has been evident during other disasters in the post-9/11 era – the response to Hurricane Sandy, for example – no single agency of government seems to be fully prepared and/or equipped to independently mount an effective response to a major disaster or other mass-casualty emergency. It seems clear, therefore, that any response to a *biological* event will require close and continuing cooperation between public health and emergency management agencies at all levels of government.

As the newest agency – in at least some respects – on the scene, the public health sector is still working hard on integrating more effectively with other first responder agencies such as police and fire departments and emergency medical services agencies. A continuing challenge impeding such integration is that the public health landscape differs in several respects at the federal, state, and local levels. Failure to take into account limitations at each level almost ensures that there will be a continuing cascade of problems as responses become more complex. A true and more detailed national strategy in this area, therefore, must be developed based on the weakest link in the chain, not the strongest.

For additional information on:
Bill Summary & Status, 112th Congress (2011-2012) H.R.2356, visit http://thomas.loc.gov/cgi-bin/bdquery/D?d112:46:./temp/~bssb9ZB

The National Strategy for Biosurveillance, visit http://www.whitehouse.gov/sites/default/files/National_Strategy_for_Biosurveillance_July_2012.pdf?goback=%2Egde_2060384_member_141908766

The 2011 TAR scores, visit http://www.cdc.gov/phpr/pubslinks/2011/documents/SEPT_UPDATE_REPORT_9-13-2011-Final-appendix2.pdf

Trust for America's Health December 2010 report, visit http://healthyamericans.org/assets/files/TFAH2010ReadyorNot%20FINAL.pdf

---

Raphael M. Barishansky, MPH, is the Director of the Office of Emergency Medical Services (EMS) for the Connecticut Department of Public Health. Prior to establishing himself in this position, he served as Chief of Public Health Emergency Preparedness for the Prince George's County (Maryland) Department of Health and as the Executive Director of the Hudson Valley Regional EMS Council, based in Newburgh, New York. He is a frequent contributor to the DomPrep Journal and other publications and can be reached at rbarishansky@gmail.com.

A Practical Approach to Achieving Resilience

By Dennis R. Schrader, Viewpoint

The time has come to address the ongoing concern that the private sector does not understand nor accept the concept of resilience. The key question: Is it a relevant strategy or simply the latest fad in homeland security?

To be useful as a security outcome, resilience should become a process that is both: (a) characterized by a set of operational practices that are easily understood and applied; and (b) described in the context of day-to-day corporate jargon. These practices include:

- Business continuity
- Risk analysis and management
- Engineered systems
- Supply chain management

In addition, adapting the government concept of "whole of community" to the private sector through processes in the National Incident Management System (NIMS) provides the integration necessary to achieve resilience.

The benefit of incorporating these practices is that a common language can be developed to bridge public and private sector efforts in the Homeland Security Enterprise without adding new overhead costs to the enterprise. Currently using these practices as an organizing principle, thousands of certified continuity professionals in the private sector already are improving their businesses' resilience each and every day.

The Evolution of Resilience

The Federal Emergency Management Agency's (FEMA) website defines "hazard mitigation" as "sustained action taken to reduce or eliminate long-term risk to people and their property from hazards and their effects." It could be argued that the practice of mitigation is the first generation of the resilience concept.

As cited in a book entitled "Emergency Management: The American Experience 1900-2010," hazard mitigation was first recognized as a concept in the 1950s and 1960s. The first reference in Congressional language to hazard mitigation appeared in the 1974 Disaster Relief Act. By 1988, the Stafford Act authorized mitigation projects through post-disaster federal assistance.

A National Academy of Public Administration report in 1993 advocated more aggressive and integrated mitigation efforts, which led to the establishment of the Federal Insurance and Mitigation Administration (FIMA) in 1993.

In 1997, after Congress first approved funding for pre-disaster mitigation, FEMA established a pilot program called "Project Impact." Since then, FEMA has continued to build a national mitigation program – Pre-Disaster Mitigation Grant Program – which is a practice that analyzes and reduces risks to engineered systems in the built environment and land use policy.

In the Post-9/11 era, by the time resilience was first officially adopted as a national homeland security strategy in the February 2010 Quadrennial Homeland Security Review (QHSR), there was a reluctance to spend too much time defining the term "resilience." In fact, a November 2010 study by the Homeland Security Institute identified 119 different definitions of resilience. Unfortunately, the word "resilience" has become a mantra or marketing strategy rather than an operational reality. At conferences and in articles, for example, the concept of resilience currently is discussed as if it were a well understood "black box" that can be "plugged in" to solve the nation's security problems.

Rather than using a simple buzz word, the ultimate goal is for the national enterprise to achieve resilience as an operational outcome. In effect, resilience would become an "umbrella" concept for practices that are well established and understood in both business and government. Public safety and public health professionals would then be able to apply these practices to focus on one or two key operational metrics as a *measure of resilience* – "reduced recovery time," for example – and coordinate those metrics with their private sector counterparts.

Changing the Culture

To achieve a long-term culture for "whole of community," there is a need to foster existing low-cost networks and encourage professional development in the practice of collaborative leadership. This notion is embedded in the NIMS doctrine, which envisions a scalable system of resources that can be rapidly applied on a regional basis. By doing so, NIMS potentially serves as a resilience tool that can be applied to whole of community preparedness.

Another step toward resilience is linking engineers to the public safety community for the preparedness mission. For example, the American Society of Civil Engineers (ASCE) has developed a set of Guiding Principles for Infrastructure to improve the resilience of engineered systems. The principles advocate resilience in the capital investment decision process through risk management, systems design, and lifecycle analysis.

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.

ASCE also has recently developed response task forces in partnership with the American Institute of Architects (AIA) and the National Council of Structural Engineers Associations (NCSEA) that can support local emergency operations and integrate local engineers into the homeland security enterprise. With pilot teams organized in Seattle, Boston, and Utah, the first deployment was made in July 2012 to support those fighting the Utah wildfires. ASCE is also working with FEMA to develop engineering resource types – that is, the categorization and description of resources that are commonly exchanged in disasters via mutual aid – to allow engineers to participate in NIMS through Emergency Management Assistance Compact (EMAC) requests, which are national interstate mutual aid agreements.

Examples of efforts related to the supply chain are evident in the ongoing Superstorm Sandy response. The state-sanctioned All Hazards Consortium, for instance, was able to provide indicator data to the emergency response agencies in New York and New Jersey. That support, in collaboration with Maryland-based Hughes satellite services, has helped create situational awareness by providing the status of gas stations, pharmacies, hotels, and food outlets.

Rather than reinventing the wheel, achieving resilience will require that nontraditional relationships be built and innovation applied to practices that are used in everyday operations. Of course, there may be a period of trial and error to determine the best tactics for effective application of these practices. Without changing the culture, however, resilience will continue to be a great idea with limited utility.

For additional information on: The ASCE Guiding Principles for Infrastructure, visit http://www.asce.org/Infrastructure/Guiding-Principles-for-the-Nation-s-Critical-Infrastructure/

The ASCE response to Utah wildfires, visit http://www.asce.org/ascenews/shorttakes.aspx?id=25769810876

Claire B. Rubin's 2012 book, "Emergency Management: The American Experience 1900-2010," visit http://www.crcpress.com/product/isbn/9781466517530

Dennis R. Schrader is President of DRS International LLC and former deputy administrator of the Federal Emergency Management Agency'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. He currently provides Senior Consulting services at Integrity Consulting Solutions, LLC.

Witt Associates offers a complete range of planning, mitigation and prevention consulting services to better prepare your organization before a crisis strikes. Whether its a public facility, business, municipality, or private non-profit, Witt Associates offers expertise, technical assistance and access to the latest technology and mitigation practices. Our team conducts a complete risk analysis, identifies vulnerabilities and designs solutions that will provide the greatest benefits to you and your organization. Our highly skilled staff also coordinates activities with local, state and federal government agencies and supports and leverages resources from public and private communities to ensure the success of these mitigation efforts.

The benefits are clear. The results, tangible.

Witt Associates makes a difference.

MITIGATION | PREPAREDNESS | RESPONSE | RECOVERY | STRATEGIC ADVICE

WITT
ASSOCIATES

www.wittassociates.com