domestic preparedness .com
T.I.P.S. Total Integrated Preparedness Solutions
$5 Per Issue
Volume 1, Issue 9, May 4, 2005

This Issue:

Interview: Department of Homeland Security, Matt Mayer

By John Fass Morton
Interviews

On May 3, 2005, DomPrep's John F. Morton, Martin Masiuk, and James D. Hessman visited with Matt A. Mayer, the acting executive director of the Office of State and Local Government Coordination and Preparedness in the Department of Homeland Security.

For the complete audio download of the interview, please go to www.DomesticPreparedness.com

Mayer, the DHS Office of Domestic Preparedness (ODP) official in charge of the rollout of *Homeland Security Presidential Directive 8 (HSPD-8) on National Preparedness*, discusses the process of recent regional rollout conferences and encourages first-responder participation as critical to the "transformational" nature of the HSPD-8 document.

Mayer also discusses *Capabilities-Based Planning* and the process involved in identifying the HSPD-8 Interim Goal's 15 National Planning Scenarios, 200 Critical Common Tasks, and 36 Target Capabilities.

Mayer highlights the importance of information sharing, providing background on the ODP's *Lessons Learned Information Sharing (LLIS) Service*, or *LLIS.gov*, the national network of lessons learned and best practices for emergency-response providers and homeland-security officials. Finally, Mayer encourages state, local, and tribal government entities to take advantage of the ODP's *Homeland Security Preparedness Technical Assistance Program* to help them write equipment requirements and define standards for preparedness assessments and strategies.

Dirty Bombs: The Impossible Becomes Probable

By Neil Livingstone
Smart Security

For many years in popular fiction and in films – not to mention in scores of academic and government publications – the same question has been asked: Will terrorists go nuclear? Until the collapse of the former Soviet Union it was an article of faith among experts that there was no known black market in fissionable material – and, therefore, that it would be virtually impossible for a rogue state or a terrorist group to build or acquire nuclear weapons. There also were some obvious problems related to assembling the equipment, technology, and skills required for the task. Finally, there was a presumed need not only to test the device but also to develop an effective delivery system. (However, numerous scenarios were quickly dreamed up about ways in which a bomb could be smuggled into the United States – in the hold of a ship, for example, or hidden inside a boiler or even in a shipment of machine tools.)

Continued on the Next Page

Editorial and Circulation Office
517 Benfield Road, Suite 303
Severna Park, MD 21146
www.domesticpreparedness.com
(410) 518-6900

Editorial Staff

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

Channel Masters

Rob Schnepp
Fire HAZMAT
rschnepp@domprep.com

Joseph Cahill
Emergency Medicine
jcahill@domprep.com

Colonel (Ret.) Robert Fitton
Military Support
bfitton@domprep.com

Ashley Moore
Standards
amoore@domprep.com

Bonni Tischler
Customs & Border
btischler@domprep.com

Jay Kehoe
Law Enforcement
jkehoe@domprep.com

John Morton
Interviews
jmorton@domprep.com

James D. Hessman
Coast Guard
JamesD@domprep.com

Neil Livingstone
Smart Security
nlivingstone@domprep.com

Anthony Lanzillotti
State Homeland News
tlanzillotti@domprep.com

Business Office

Susan Collins
Circulation Director
subscriber@domprep.com

Sharon Stovall
Copy Manager
sstovall@domprep.com

Martin Masiuk
Advertising & Sponsorships
mmasiuk@domprep.com

Subscriptions
$50.00 annually 26 Issues for single user, delivered via web or email. To order, visit www.domprep.com and click on subscribe.

Published by IMR Inc.
Martin D. Masiuk, Executive Director and Publisher, mmasiuk@domprep.com

All of this changed with the fall of the Soviet Union and its fragmentation into eleven successor states. "The breakup of the Soviet Union left nuclear material scattered throughout the newly independent states and increased the potential for the theft of those materials, and for organized criminals to enter the nuclear smuggling business." So said President Clinton in a speech at the U.S. Air Force Academy in 1995.

The Russian government, it rapidly became apparent, did not have an accurate inventory of either its weapons – especially the relatively small and easily concealable "backpack nukes," as they are sometimes described – or its stockpiles of fissile and radiological material. Most Russian nuclear plants, it seems, never placed a high priority on fully accounting for their nuclear fuel; a ninety-seven percent reconciliation score was considered full accountability. Plants also tended to hoard any surplus to make up for possible future shortfalls. The Tomsk-7 facility in Siberia, moreover, is believed to have somehow "lost" a large amount of plutonium. Rebels even overran a nuclear storage site in Azerbaijan in 1990 – the site was quickly retaken by Russian troops, but the fact that one site had been captured one time suggested that the same thing could happen again, with a less favorable outcome.

As a result of these and other problems with Russian nuclear materials, the United States passed the Nunn-Lugar legislation to help the Russians and other USSR successor states control and protect such materials.

Strontium Capsules and Well-Guarded Potatoes

Despite its noble goal, that program has had, at best, only a mixed success to date. The U.S. National Intelligence Council recently forwarded a report to Congress wherein it was stated that Russian officials "have reported that terrorists have targeted Russian nuclear weapon sites. Security was tightened in 2001, after Russian authorities twice thwarted terrorist efforts to reconnoiter nuclear weapon storage sites. "We find it highly unlikely," the report continued, "that Russian authorities would have been able to recover all the material reported stolen. We assess that undetected smuggling has occurred. And we are concerned about the total amount of material that could … [have been] diverted or stolen in the last 13 years."

Russian efforts to safeguard their nuclear weapons are generally considered to have been more successful than the steps they have taken to protect their stockpiles of fissionable and radiological materials. U.S. teams found sites where radiological material was stored behind doors with no locks, only seals – which, if broken, would have indicated that someone had violated the site. At another site, the United States paid for elaborate security enhancements, including detection devices that were removed after the visit of an inspection team – incredibly, out of fear that the security systems themselves might be stolen by thieves. At yet another site, a new pipeline was built directly through the facility, rather than around it, rendering meaningless the millions of dollars of security enhancements that already had been paid for. According to a Russian special investigator, "potatoes are guarded better than radioactive material" in contemporary Russia.

And the incidents continue. Just two years ago in Tbilisi, Georgia, authorities arrested a man driving a taxi in which there were a number of boxes marked "Danger: Radiation."

Continued on the Next Page

Inside the boxes, which were emitting a dangerous amount of radiation, were capsules of strontium and cesium. The taxi driver had been hired to take the boxes by train to Adzharia, Georgia. Authorities speculate that the boxes were then going to be shipped to either Turkey or Iran.

High Priorities and Public Announcements

Given that Russia and other Soviet successor states are believed to have hemorrhaged both fissionable/radiological material as well as nuclear know-how over the past decade and a half, the threat of a terrorist or rogue state carrying out an attack on the United States is now more than a reality; some would say it is a probability. For that reason alone there probably is no higher priority, from a homeland-defense perspective, than the development of the systems, procedures, and capabilities needed to protect this nation and its citizens from the threat of a catastrophic attack on one or more American cities. In a variation on the Mutually Assured Destruction (MAD) strategy that prevailed during the Cold War, the first step the United States should perhaps take to prevent such an attack is to publicly announce that it would launch a nuclear counterattack against any nation that either directly or indirectly aids and abets any rogue state or terrorist group in carrying out a nuclear or radiological attack, "incident," or other event against the United States. Such an announcement would be a logical extension of President Bush's several previous statements that any nation that harbors, financially supports, and/or helps terrorists in any other way would be held just as accountable as the terrorists themselves for acts of terrorism against the United States. Included in the aiding-or-abetting category, therefore, would be countries that provide assistance to nations – or to "non-state actors," as terrorist groups are sometimes called – in obtaining fissile or radiological material, scientific know-how, and/or the delivery system used in the attack.

Detection of fissile or radiological materials remains a serious problem. Although the federal government has installed more than 400 radiation monitors over the past two years at U.S. border crossings, in the nation's airports and seaports, and even in U.S. post offices that process international mail, new and more advanced detection technologies are needed, and detection instruments and devices based on those technologies will have to be installed on a massive scale, and used on a continuing 24/7 basis.

Other difficulties also remain. Despite the seriousness of the problem, administration spending on Russian nuclear transition initiatives and other efforts to reduce the threat posed by unsecured nuclear warheads, materials, and technological expertise has remained static – or, in some cases, has declined – in recent years. The program also has been slowed down not only by friction with Russian authorities but also at times by weak and/or inattentive leadership on the part of U.S. government officials.

Hiroshima Times 182,000

Meanwhile, nuclear stockpiles continue to grow as Cold War weapons inventories are dismantled around the world. Experts estimate that, by 2010, there will be enough surplus uranium available from dismantled warheads to make 70,000 Hiroshima-sized bombs, enough HEU (highly enriched uranium) from dismantled bombs to produce another 65,000 nukes of the same size, and enough Plutonium-239 – from civilian-sector stockpiles in Japan and Western Europe – to build 47,000 Hiroshima-sized nukes. It seems clear that more effective, and much more *aggressive*, efforts are required to protect this material before it is too late. America's first line of defense cannot be at its borders but must focus on denying rogue states and terrorists the nuclear materials, equipment, and scientific technology required to build fissile weapons.

However, even if all orphan high-order radioactive materials are ultimately secured, a major threat will still remain in the form of RDDs (radiological dispersion devices – which can even be constructed of radiological medical waste). The International Atomic Energy Agency (IAEA) announced in 2002 that the alleged "controls" of more than a hundred countries were at that time inadequate to prevent the theft of radioactive materials – and, therefore, that almost any nation in the world was (and still is) capable of creating so-called "dirty bombs." Intelligence officials believe that a number of terrorist organizations, including Al Qaeda, can be added to the IAEA list.

An RDD uses conventional explosives to disperse radiological material. An RDD attack carried out in lower Manhattan – even one that produced only "limited" casualties, however that term is defined – might cause the stock market to implode, and also might require a billion dollars to clean up. Some people, fearing residual radiation, would probably never return to New York. Indeed, fear is the most likely byproduct of an RDD attack.

It seems clear that – in addition to focusing more time, attention, and resources on the detection and prevention of nuclear or radiation attacks – the United States must put greater emphasis on the nation's emergency response and mitigation capabilities in the event that the unthinkable occurs nonetheless.

America has been lucky so far. But, as all sports fans know, the longest winning streak on record cannot last forever.

~

SNL and Merlin: A New Way to Look at Decontamination

By Rob Schnepp
Fire/HAZMAT

In 1997, the Department of Energy (DOE) received a mandate from Congress to develop improved technologies for use in the "Global War on Terrorism." One purpose of that mandate was to find a more effective way to decontaminate (decon) potential biological and chemical agents – in other words, something better than the traditional water-based decontamination agents employed by most fire agencies at the time.

Fast-forward to the New Mexico desert, home of the Sandia National Laboratory (SNL), where a new decontamination solution, DF100, was developed as an initial response to the mandate. A peroxide-based foam solution, DF100 proved to be quite effective at rapidly deactivating nerve agents as well as destroying all conventional biological pathogens considered to pose a credible threat.

Fast-forward again to the current version of the SNL solution, called DF200. "Right now, it's the top dog in decon," said Dennis Smagac, founder and director of business development at Intelagard Inc., a company based in Broomfield, Colorado. "The U.S. military and the Capitol Hill police are using Intelagard's Merlin™ system, a compressed-air foam delivery system, with DF200 as the decon solution," Smagac said. "It's a very efficient combination. It's mobile, and not dependent on having water available." DOE has licensed two companies to manufacture the SNL solution, Smagac said: Modec, in Denver; and Envirofoam Technologies in Huntsville, Alabama.

"Spectacularly Effective" – Fast, Too

Intelagard specializes in the design of compressed-air foam (CAF) systems for the deployment of liquid-based solutions, like the SNL DF200 solution, and various firefighting and hazardous materials foam concentrations. It was Intelagard's Merlin CAF system, using DF200, that was used to clean the U.S. Senate office buildings that were discovered, not long after the 9/11 terrorist attacks, to be contaminated with anthrax.

The SNL formulation is spectacularly effective at deactivating chemical warfare (CW) agents, biological pathogens, and many toxic industrial chemicals (TICs). In studies conducted by Modec, DF200 achieved a 99 percent neutralization rate against nerve agents such as soman (GD) and VX, with a 15-minute contact time. Within one hour, the nerve agents were completely destroyed, without the formation of any toxic byproducts. Sulfur mustard was broken down with equal effectiveness, and many TICs – including sodium cyanide, butyl isocyanate, carbon disulfide, phosgene (gas), chlorine (gas), and anhydrous ammonia (gas) – were 99 percent neutralized within one minute of contact time with SNL DF200.

DF200 also proved to be a highly effective decontamination agent against biological warfare agents when tested against simulants for anthrax and plague, achieving a "7-log" kill – i.e., 99.99999 percent – within 15 minutes of contact time (further testing on live warfare agents confirmed the effectives proven on the simulants). The Bovine Corona Virus, a surrogate for Severe Acute Respiratory Syndrome, aka the SARS virus, was successfully inactivated after a one-minute exposure to a 10 percent concentration of SNL DF200. (For additional information on technical specifications of the DF200 foam solution, visit www.sandia.gov/SandiaDecon/.)

"DF200 can be applied in any fashion and still be effective," according to Mark Tucker, technical contact at Sandia National Laboratory. "The solution may be applied through compressed-air foam systems, or as a liquid in a paint sprayer or even a bug sprayer. It could even be put into a fire-engine water tank and sprayed through a hose line.

"The purpose of using DF200 is two-fold," he added. "It's intended to be used for remediation efforts [e.g., the decontamination work at the U.S. Senate buildings], or for decon."

Environmentally Friendly, and Approved by EPA

When the DF200 is applied through a CAF system such as Merlin, the resulting foam enhances the contact time between the decon solution and the substance. Contact time is a critical factor in deactivating or neutralizing the hazard. "Essentially," Tucker said, "the foam holds the agent, and the peroxide, which is a little stronger than what you have at home, breaks the chemical bonds. To activate the foam solution, a surfactant, a fortifier, and a booster are mixed inside a five-gallon bucket. Once the components are mixed, the foam solution is ready to go – with about an eight-hour pot life."

A bucket of DF200 foam solution

DF 200 also has been proved to have no compatibility issues with materials such as wood, paper, plastic, concrete, or asphalt – typical construction materials found at hazardous materials incident sites. But it may, according to Tucker, be mildly corrosive to ferrous materials such as iron and steel.

Continued on the Next Page

"The SNL DF200," Smagac said, "is environmentally friendly, and has received approval from the U.S. Environmental Protection Agency for use on chem/bio agents.

The partial components of the DF200 decon solution

The Merlin system, along with the SNL DF200 foam solution, is used by all Federal Emergency Management Agency-sponsored urban search and rescue teams in the United States. The combination is an effective one, allowing both for portability and for rapid decon in the field – important advantages when a team is operating in potential collapse areas and/or in other places where water may not be available.

The Merlin, during a training exercise, functions as a fully independent handcart, capable of delivering a variety of liquids from twin 7.5-gallon tanks.

When dispensing foam, the Merlin has the ability to expand the DF200, or standard firefighting foams, in ratios ranging from 1:1 all the way up to 70:1, depending on the type of foam used and the configuration of the nozzle. High-pressure self-contained breathing apparatus cylinders provide the "power" that makes the Merlin a truly portable compressed-air foam-dispersal system.

This shows an example of DF200 training foam being applied through a foam aspirator nozzle.

For additional information about compressed-air foam solutions and the Merlin system, visit Intelagard at www.intelagard.com.

~

The What and Wherefores of Bio-Terrorism

By Joseph Cahill
Emergency Medicine

Bio-terrorism is covert by its very nature. It is unannounced and it is hidden – it has to be. Moreover, by its nature, it can stay hidden – for at least a while – adding to its destructive power. Every minute of every hour that a biological-warfare attack continues without being detected means that much more time to infect that many more victims.

An explosion happens. It does its damage and is finished, and its energy is expended. Chemical or radiological dispersion device (dirty bomb) attacks kill, wound, or destroy within the given volume of contaminant, and therefore have a finite destructive power.

Biological agents are unique, though. Given the right conditions, they can and will – through the natural process of reproduction – increase in the volume of space and number of persons affected. In addition, if the disease caused by a specific bio-agent is person-to-person transmissible, every victim is a potential ally in spreading the effect of the weapon.

The effects are cumulative. The more time passes the sicker the patients will be when they reach care providers. In addition, in this time, more people will be infected, and the circle of damage caused by the attack will continue to widen. Conversely, the sooner any victim starts treatment the more likely it will be that he or she will survive.

Fundamentally, a bio-weapon causes an artificial outbreak of disease. Historically, the accepted method of detecting any outbreak of a disease is to make it reportable – by doctors, hospitals, or laboratories. On the federal level the process is embodied in the National Notifiable Disease Surveillance System (NNDSS), which depends on doctors, hospitals, and laboratories to fill out disease case reports and pass the information forward to public health officials. These well educated professionals, experts in diagnosing diseases, are license holders and often are regulated by the same public health officials who are tasked with the identification of outbreaks.

One Case Does Not an Outbreak Make

In practice, the reporting model tracks instances of a known, reportable disease – the plague, for example. There are some instances of plague every year, so a few cases do not necessarily signify an unusual or unnatural outbreak. However, if three times the annual national average number of cases occur in a city over the course of just a few weeks, it is reasonable to suspect that something unusual is going on.

The diseases caused by traditional bio-weapons (anthrax, botulism, brucellosis, cholera, plague, tularemia, western equine encephalitis, and eastern equine encephalitis) are rare enough that a single case can be considered significant depending on its geographic location. A study by the Centers for Disease Control and Prevention (CDC) explains the situation this way: "Even with such low incidence, we identified patterns in disease incidence that better prepare us to identify potential bio-terrorism events.

Continued on the Next Page

In this analysis, certain diseases appear to be endemic in certain geographic areas. A case of smallpox, which has been eradicated from the natural world, will always be considered an act of terrorism or war unless otherwise explainable. Similarly, the incidence of naturally occurring anthrax is so low that any and all cases – particularly outside of sheep/goat-raising areas or the wool industry – should raise the index of suspicion.

Improvements in data technology have made paper reporting of diseases nearly obsolete; on-line reporting is now the norm. Reporting professionals can easily add their data to the greater public-health picture without leaving their offices. This advance is more than just a convenience, though. Electronic reporting improves the amount of reports actually filed. Electronic reporting also increases the number of reports actually filed. Further, the information is immediately available to public health analysts.

Symptoms, Syndromes, and Surveillance

According to the CDC, the term "syndromic surveillance" applies to surveillance "using health-related data that precede diagnosis and signal a sufficient probability of a case or an outbreak to warrant further public health response." In other words, it refers to the collection of data on clusters of symptoms that do not depend on the final diagnosis.

The New York City Department of Health and Mental Hygiene (DOHMH) has established a number of symptom clusters that hospital emergency rooms (ERs) in New York City report daily. There are eight syndromes they track: Common cold, Sepsis, Respiratory, Diarrhea, Fever, Rash, Asthma, and Vomiting. As is evident, the syndromes are defined more by their symptoms than by the actual causes of the symptoms.

During the early phase of an outbreak, the symptoms reported are identified only as unusual activity. An increase in the number of patients complaining of the symptoms of a common cold is identified in the data by the DOHMH as evidence that something unusual may be going on. The information does not, though, identify precisely what is going on – that still has to be determined. The next step would be for a DOHMH investigator to determine the cause; it might be, for example, that there has been an outbreak of anthrax.

The initial onset of symptoms of inhalation anthrax is nonspecific, though, and similar in certain respects to the symptoms of a common cold. For that reason, the first indication of a real anthrax attack might be a rise in treatment for and complaints of nonspecific symptoms at hospital ERs and in the offices of private providers.

Later symptoms of inhalation anthrax become more specific and can be diagnosed clinically. Public health officials can use reports of patients with the specific diagnoses to identify actual cases. At this point, remedial and/or preventive actions can be taken based on the specifics of the disease. The public health officials can issue critical information to care providers, for example, or to the general public. Parallel to the case investigations, the law-enforcement community can – if appropriate – start criminal investigations.

A primary goal of syndromic surveillance, therefore, is to recognize that something unusual is going on – and, for that reason, to start field investigations early. Today, because of the increased risk of terrorist attacks, this sequence of events might well be, literally, a matter of life and death.

Size, Seasons, and Suspicions

Among the several factors affecting syndromic surveillance and its usefulness are the following:

1.*Size:* the event has to reach a statistically significant threshold level. If there are 55 cases of a particular disease in an average year, an outbreak of six cases in one month may not be enough to sound the alarm.

2.*Population Mobility/Commuting:* A population that moves from one jurisdiction to another means two things to the syndromic surveillance system: Those infected spread a contagious disease across a larger geographic area; and the population of infected victims is now part of a larger overall population pool. In today's commuter age, an attack that originates in New York City could quickly spread to a four-state region just by being carried by daily commuters across state lines (or it could become worldwide if the attack were to take place in an international airport).

3.*The Level of Suspicion Within the Health-Care Community:* Among the principal factors determining success or failure in this type of system is the alertness of the health-care community. Providers must understand the need to complete the reporting procedures both fully and accurately. A lack of awareness of both the requirements for and the value of reporting – along with confusion resulting from changing requirements that do not always take into account the threat posed by bio-terrorism – has led in some instances, unfortunately, to incomplete reporting. The index of suspicion within the patient-care community will affect the success of the syndromic surveillance system because the members of that community who are required to report events have to understand both what has to be reported and why the reporting is important.

Continued on the Next Page

4.*The Seasons of the Year:* A bio-terrorism attack will take longer, and will be harder to detect, during the seasons when there are natural upswings in disease. Asthma cases increase every fall, for example, because of seasonal increases in natural irritants. The system has to allow for such known causal relationships. Raw daily tallies of a specific syndrome should not be compared to an annual daily average in any case. Instead, they should be measured against statistics that have been controlled and adjusted to remove as many known natural variables as possible.

5.*Syndromic Surveillance System Design:* The components of the syndromic surveillance system will affect the speed and accuracy of any warning that might be issued. Among these components are the source and quality of the data provided. In addition, the speed at which the data can be received and processed will directly affect the usefulness of the results. A data collection and processing system that provides 100 percent accuracy, but returns results in 30 days, would be useless in countering bio-weapons, which almost always have a "working life" – i.e., the time from infection to the end of the disease – of only two weeks or less. During the 2001 anthrax attacks, the time between infection and onset of specific symptoms was 4-6 days.

The thresholds for alarm also will help dictate the usefulness of the system. Like any other alarm system, from radiation meters to smoke detectors, the point at which a bio-terrorism alarm is sounded is very important. If the threshold is set too low the alarms become routine and will be discounted, remaining un-acted upon; if it is set too high the threat is too advanced by the time the alarm sounds.

The human factor always has to be considered. The time when the last false positive was received directly affects the success of the system. The more recently a false positive was received – and the more negative the fallout for those raising the alarm – the more wary those managing the system will be.

Other Data Being Considered

In addition to the hospital ER data on the number of patients complaining of one syndrome or another, several other sources of data have been studied and are being used. Two examples are the number of patients admitted to emergency rooms, and the volume of calls to EMS (emergency medical services) units and agencies. It seems evident that an unusual increase in the number of people coming into the emergency room, and/or in the number of ambulance runs on any given day, may be evidence of a possible outbreak.

Fortunately, EMTs (Emergency Medical Technicians) and Paramedics collect much of the same information about patients and their reasons for calling an ambulance – and it is well within the ability of the qualified Paramedic and/or EMT to describe a patient's symptoms, which means that these patients can be sorted into the same syndromes as ER patients.

There are, though, certain factors that might affect the validity of this data source. The first is that the jurisdictions of many public health agencies receiving and analyzing this data often are serviced by a large number of EMS agencies – which do not necessarily use the same standardized written reports. Also, they may or may not be required to turn in their reports.

Finally, even if there is a centralized report recipient, there may be a built-in time delay and/or no effective way of entering and/or analyzing the data in a timely manner.

In general, it seems to be the administrative bottlenecks that make data received from EMS units less timely – and, therefore, less useful. However, there are a number of electronic ambulance reporting systems now available that either record information into a hand-held device (such as a palm top or tablet computer) or scan handwritten documents to make them available as electronic data as rapidly as they are scanned.

Laboratory case reports also can be useful. Kansas City (Mo.) has studied the use of data from the main labs used by hospitals and private physicians to track the types of complaints reported by patients. This provides an indirect indicator of the specific syndrome from which a patient might be suffering. For example, if test "A" is the standard of care for patients with an unidentified rash, and is used for little else, then an increase in requests for test A should be indicative of an increase in unknown rashes.

An increase in gross numbers also can tell the disease tracker that something is amiss when the number of requests for lab tests climbs. There is, though, a general problem in relying too much on either the number of EMS calls or the volume of lab test requests, because there are several variables that may affect either or both.

Unfortunately, all three of these sources of data – EMS call volume, ER visit volume, and lab test volume – are indirect methods for extrapolating the same information that is provided by the ER syndrome data. As such, it is more reliable to collect this information directly.

Blood, Dollars, and Confidentiality

Approximately four million people give blood each year. The donors represent all demographic groups and come from all areas of the country. In theory, if a small sample of each unit of blood donated were sent to a lab to be tested the general

health of the community could be determined, more or less, by the results. Real-life experience, though, shows this seemingly logical plan to be unworkable.

There are numerous complex legal issues – involving consent and/or confidentiality, for example – governing any medical testing. There also are a large number of laws and regulations governing testing practices and the control of results. In addition, the agencies that collect blood may not be enthusiastic about participation in any data-collection effort. Concern about confidentiality of the test results may keep people away who otherwise might be willing to donate. The need for blood donations grows every year, and the agencies filling that need are not likely to do anything that might reduce the number of potential donors.

There are other factors to be considered. One is that even a blood test that is sensitive enough to identify an infected patient in the first three days of infection would yield only a 26 percent chance of successfully detecting the disease. In addition, the time it takes for that detection would almost certainly be longer than the time it would take for the disease to manifest itself through the outbreak of symptoms (at which time the disease could be identified by other means). Finally, the overall cost of testing samples of all blood donated each year would be astronomical.

It is clear that the complicated amalgam of data and data sources, laws, regulations, and practical factors that come into play in fighting bio-terrorism presents a formidable challenge. Meeting that challenge is mandatory, though, because it presents the best hope for shortening the time between disease attack and disease discovery – and, therefore, for improving the chances for survival of those who are the victims of an attack. It should be understood, though, that efforts in this area can and should be complemented by improvements in the gathering of intelligence, more vigorous law enforcement, traditional diagnosis-based case tracking, and aggressive use of other homeland-defense assets and resources.

~

States of Preparedness

By Anthony Lanzillotti
State Homeland News

MISSOURI

Funeral directors seek help with PPE funding

Funeral home directors in Missouri have asked the state to help them obtain federal funding for the purchase of personal protective equipment (PPE). The request came after a recent meeting of the directors to discuss the need for the PPE, which would limit their exposure to biological or chemical agents left on a cadaver after a terrorist incident. Don Otto, executive director of the Missouri Funeral Directors Association, has initiated talks with the Missouri State Emergency Management Agency about the funding request.

The State Emergency Management Agency previously provided various state and local agencies with PPE and other equipment needed to respond to incidents involving the use of biological or chemical agents.

Susie Stonner, a spokeswoman for the State Emergency Management Agency, indicated that, because it is an organization "representing private businesses," the association might not be eligible for homeland-security grant money. She said, though, that the state will wait for a formal request from the association before reviewing the issue. The agency already has plans to provide free training to funeral directors later this year. Included in the training will be discussions about precautionary measures available and "resource management" for and within possible disaster areas.

Related Notes: The city of Columbia's police department and Office of Volunteer Services have started to invite members of the public to attend free training sessions devoted to the subject of terrorism awareness.

The first two-hour session, held at the city council chambers, covered both domestic and international terrorism, discussed possible indicators of terrorist activity, and spelled out the procedures to be followed in reporting suspicious activity. Attendees also were encouraged to participate in and/or otherwise become involved in programs sponsored by such groups as Volunteers in Police Service (VIPS), the Citizens Emergency Response Team (CERT), and the Health Department Volunteer Corps.

RHODE ISLAND

Responds to bio-terrorism in mock Q Fever outbreak

Brown University served as the real-life stage for a six-hour public health drill carried out in cooperation with state and local law-enforcement and public-health agencies.

The scenario for the drill was a bio-terrorist attack that released Coxiella burnetti, an airborne pathogen, inside the university's Rockefeller Library. The Coxiella burnetti bacteria causes Q Fever, a disease that affects approximately half of those exposed to it and causes high fever, headache, nausea, and vomiting as well as a number of dangerous respiratory ailments.

Continued on the Next Page

The purpose of the drill, carried out on Friday 22 April, was to test the university's ability to manage a bio-terrorism incident. Because Q Fever has an incubation period of two to three weeks, the actual time of release could not be determined, according to the scenario, which meant that all individuals who had been inside the library over a period of three weeks would have to be diagnosed. A mock clinic was set up at the campus's Pizzitola Center, where volunteers had their vital signs checked and their simulated symptoms diagnosed.

Antibiotics were "administered" to all potential victims, and those exhibiting symptoms of the disease were "treated" by doctors.

Students from Brown's Emergency Medical Services team also took part in the drill, which was carried out during the various festivities that are part of the university's Spring Weekend.

The timing of the drill limited the number of volunteers to some extent, but those who did participate were taught the real-world lesson that an attack or outbreak similar to, or worse than, the simulated Q Fever incident could occur at any time.

NEVADA
Continues focus on grants and communications interoperability following acquisition of mobile command center

Grant programs, mutual-aid agreements, training needs, hazard mitigation, and implementation of the National Incident Management System (NIMS) were among the principal topics discussed earlier this week at a Nevada Emergency Management Conference in Las Vegas. Among the attendees at the conference, hosted by the Nevada Department of Public Safety (DPS), were representatives from the Federal Emergency Management Agency (FEMA) and a number of state agencies.

Many of the same topics were on the agenda of a meeting on 21 April sponsored by the Nevada Commission on Homeland Security. The principal topics of discussion at the earlier meeting, which was video-conferenced between the Nevada Division of Emergency Management in Carson City and the Southern Nevada Area Health Education center in Las Vegas, were an overview of all of the U.S. Office of Domestic Preparedness (ODP) grant applications received by the state, and the approval of fiscal year 2005 ODP grant applications. Also on the agenda were a discussion of the status of a statewide vulnerability assessment now being carried out and an update on the Nevada State Communications Interoperability Plan. The latter, which is being implemented by the Nevada Communications Steering Committee, is intended to facilitate the planning and development of interoperable communication systems designed for use between government officials and the state's emergency-response agencies.

Related Notes: In large part because of similar grant conferences and meetings carried out last year, the Nevada DPS was able to deliver a customized mobile command center earlier this year to the department's Homeland Security Unit. The command center, named S.T.A.R.T. (State Tactical Assessment and Response Team), is expected to have a number of uses statewide, including but not limited to serving as a base of operations for crime-scene communications, the support of narcotics investigations, and responses to terrorist incidents. S.T.A.R.T. is equipped with a number of advanced equipment systems, including radiological/chemical/biological detection instruments, video-monitoring devices, and various communications systems. Nevada also has been successful in using ODP grant funding both for training and for the purchase of other essential equipment.

Do you have the best response tools?

MultiRAE Plus

PID plus multi-gas equals protection from the unexpected

- Toxic Industrial Chemical (TIC) vapors
- Flammable gases and vapors
- Oxygen concentrations

HazRAE

Chem/Bio/WMD Decision Support

- A 6-foot stack of HazMat references in your hand
- Identifies unknowns using signs and symptoms
- Speeds the transition from detection to decision

PlumeRAE

Plume Measurement and Prediction

- Down-range wireless monitors tell you where the plume is located
- Easy-to-use complete system
- Quick toxic threat evaluation

GammaRAE II

Personal Radiation Detector

- Prominent visible, audible and vibration alarms
- Water-resistant for easy decon
- Fast response to radiological threats

RDK Gamma

Toxic Gas/Radiation Perimeter Monitoring

- Rapid Deployment Kit with wireless monitoring
- Remotely monitor threats up to 2 miles away
- Includes 4 down-range monitors for quick, adaptable response

www.raesystems.com

Hazardous Environment Detection Solutions

RAE SYSTEMS