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

This Issue:

For more details, visit:
DomesticPreparedness.com
Since 1998, Integrating Professional Communities of Homeland Security

Rosie the Riveter and Homeland Security

By Martin Masiuk
Publisher

Everyone knows of Rosie the Riveter. During World War II, she represented America's "real" secret weapon–the U.S. private-sector defense industry and the hundreds of thousands of dedicated and intelligent people who work for it. After Pearl Harbor was attacked, Rosie rolled up her sleeves and outfitted the nation's war fighters with the equipment needed to ensure a successful outcome of that terrible conflict. Today, Rosie is still hard at work, innovating the cutting-edge technologies, systems, and equipment that will be required to win the global war on terrorism.

Last week, the DomPrep.com T.I.P.S. team exhibited at Equity International's Homeland Security Summit at the new convention center in downtown Washington, D.C., where there was on exhibit a dazzling array of products, some of them already fielded, based on the several new technologies that can be used to protect the nation's land and sea borders, U.S. ports, nuclear plants and other "high-interest" facilities, and the American people. In addition, America's first responders are being equipped for their roles in consequence management as they prepare to respond to an attack.

Interestingly, Rosie and her co-workers are being helped by products offered from Finland, Israel, Russia, and the United Kingdom, all of which also were represented at their own pavilions in this important trade show. The lesson was clear: The global marketplace is hard at work developing the solutions needed to win this new global war.

Continued on Page 2

Interview with Amit Yoran, Former DHS Cyber Security Chief

By John F. Morton
Interviews

On March 3, 2005, DomPrep's John F. Morton and Martin Masiuk visited with Amit Yoran, until last fall the head of the National Cyber Security Division in the DHS Information Analysis and Infrastructure Protection Directorate.

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

Mr. Yoran gave the government a C- in his report card on the public-private cyber security partnership and spoke of the challenges to information sharing with the private sector and state and local governments—in particular the shortfalls in classified sharing.

Continued on Page 3

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

Robert Schnepp
Fire HAZMAT
rschnepp@domprep.com

Joseph Cahill
Emergency Medicine
jcahill@domprep.com

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

Ashley Moore
Standards
amoore@domprep.com

Bonni Tischler
Customs and Borders
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
Facility Protection
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 e-mail. To order, visit domprep.com and click on subscribe.

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

Rosie the Riveter and Homeland Security

Continued from page 1

Genius is obviously at work, as has been clearly demonstrated by the hundreds of thousands of hardworking engineers, technicians, scientists, office workers, and other members of the homeland-industry teams designing, testing and bringing to market products that not only will be used in war, but also can serve a dual purpose in a broad spectrum of peaceful uses.

DomPrep.com plans to bring readers periodic updates and special reports on this new bow wave of technology in the WebChannels of Industry Update, Online Exhibit, WebConference, and soon-to-be-relaunched Buyer's Guide. These reports will not endorse any specific product, but it is obvious that that there will be some winners and some losers as the marketplace develops and as standards evolve. It will be DomPrep.com's mission to report these competitions to its readers, sometimes with an accompanying analysis, and at other times raw.

America's economy continues to grow at record pace by building products that are cheaper, better, faster, and delivered just in time. Now, as the nation retrofits "security" into the equation, some adjustments are being made. The National Response Plan, international and national cargo-security strategies, critical infrastructure protection, cyber security, all are being offered what the market place refers to as "product solutions." In addition, there are numerous management, training, and interoperability issues that must be addressed when integrating this technology into the system. This brings even more new opportunities to those companies known for their best practices, strong marketing skills, innovative sales programs, and reliable business plans.

The DomPrep.com T.I.P.S. team plans to attend and exhibit at future trade shows and similar events, and looks forward to providing more technology reports, focused on those shows, to T.I.P.S. readers. To learn more about these exciting developments, visit the Online Exhibit, register and attend the WebConferences, and click on the web banners, all of which present an innovative array of solutions.

Footnote: After World War II, the fall of the Iron Curtain over Eastern Europe, and the Cold War buildup, Rosie worked for many Department of Defense contractors. As the requirements for ships, planes, tanks, and armament changed, the builders and suppliers grew, merged, partnered, and acquired one another. Today there are only a few giants supplying what is still a major and continuing demand. Similarly, it is expected that, as the Department of Homeland Security and its numerous state and local counterparts define, then refine, their equipment requirements, the same evolutionary process will occur in the homeland-security sector. Watching and reporting on the winners and losers will be interesting, indeed. DomPrep.com looks forward to sharing new developments, as they occur, with its readers.

Finally, a personal note from the publisher: Please let me know by reply email, mmasiuk@domprep.com, not only if you think we are on track but also, and of greater importance, how you suggest we might improve and be of even greater value to you, the reader. Thank you. Marty

Interview with Amit Yoran, Former DHS Cyber Security Chief

Continued from page 1

Turning to cyber security and the Internet, Yoran touched upon Einstein, the Federal government's pilot program to help officials prevent future attacks, and its potential for information sharing with state and local governments and the private sector through US-CERT. He also noted the development of IT interaction mechanisms between DHS and state and local governments via the Homeland Security Information Network (HSIN).

Citing the work of the National Infrastructure Advisory Council (NIAC) in making recommendations on how to rate IT vulnerabilities across various industry sectors, Yoran stressed the need for a best practices analysis of how organizations are delineating the roles of chief information security officer (CISO) and chief security officer (CSO) in risk management. Lastly, he warned of the increasing security challenge posed by what he called network "de-perimeterization" that is the result of the reliance on outsourcing, mobile and wireless platforms, and the proliferation of XML infrastructures.

Materials Distribution in a Public Health Crisis

By Joseph Cahill

In the so-called Dark Ages, "emergency plans" focused on keeping invaders – Vikings, Visigoths, and Vandals, for example – or political enemies out of one's own fort, and on maintaining life for those within the fort. Much of what is now called emergency management focused, therefore, on management of the food supplies and other materials required to ensure self-sufficiency.

Much has changed in the many centuries that have passed since then, but those are still among the essential goals of emergency management in today's world.

In recent years, particularly since the 9/11 terrorist attacks, there have been several federal programs initiated that involve the distribution of materials during and/or immediately after a public health emergency. In addition, and as a logical follow-on, many local, state, and county-level planning efforts have been geared to provide a suitable framework for the delivery of those materials during and/or after a terrorist attack. Among the most important of these efforts has been creation of the Strategic National Stockpile (SNS) program initiated by the Centers for Disease Control (CDC) and a closely related subprogram called Chempack.

All of these efforts are or should be developed in accordance with certain basic concepts, one of the most important of which is called generalization. In any plan (developed for any task or situation) there are always a number of tasks that have to be carried out. Generalization is simply the common-sense recognition that the step-by-step process developed to carry out one plan, or one step in a plan, should ideally be applicable to as many other steps, or plans, as possible.

A second basic concept, also of the common-sense variety, requires using resources that already are available for everyday tasks to carry out other tasks that might develop during a crisis. One garden-variety example might be using a hose normally used to wash the car or water the lawn to put out a fire in the tool shed.

Tools, Skill Sets, and Competency Levels

In theory, every planning effort might usefully be considered to be a tool R&D (research and development) program. In many if not quite all situations the planning for the task determines the size and design of the tool. For example, the SNS program requires that specific localities develop their own plans for moving materials from a county-level site to individual clinic sites. That task might be broken down into several steps or components. It is how those components are viewed that determines how well (or how poorly) local planners apply the generalization concept.

The first step is to define each component in the general terms needed to accomplish the task at hand. In the SNS example, medical supplies would be delivered by the state to a county-level staging area. An inventory system would then be used to keep track of the supplies. By tapping into the system, clinical sites throughout the state would be able to request the specific supplies they need.

By defining each step, without reference to the SNS or to any specific type of materials (medical supplies, in this example), planners can apply the same plan to the receipt, inventory, and supply chain of any type of materials required by any end user in the state.

All offices and agencies at every level of government carry out certain tasks specifically assigned to those offices and agencies. Assuming that the personnel at those agencies are competent at their jobs the public has a right to expect that those jobs will be done correctly. The level of competency is likely to vary considerably, however, from job to job and from person to person. Any public health nurse, though,

Continued on Page 4

Materials Distribution in a Public Health Crisis

Continued from page 3

should possess a certain set of skills suited to the work he or she routinely does. In this case, his or her skill set probably would include varying levels of medical education, the knowledge needed to carry out pre-vaccine evaluations, and the ability to administer vaccines and/or medications of various types. Other government employees would not usually possess the same skill set. Nor would all other nurses, for that matter, because many nursing skill sets require licensure and/or board certification, but others do not.

Different jobs obviously require different skill sets. For that reason, even though the public health nurse might be the staff member best qualified to be in charge of patient education, he or she might not be the staff's best forklift operator. Recognition that blue-collar non-medical staff members possess their own valuable, and often unique, skill sets is not only an important lesson for planners but also a helpful intangible in building teamwork.

Ideally, staff members should perform the same tasks during an emergency that they do every day—using the same tools, and following the same work practices. That way, even the staff members who might be overwhelmed by the emergency per se can step back into the refuge of the familiar. The previously mentioned forklift operator, moreover, would probably do his or her everyday job not only better but also more safely than another person assigned to the job just for the emergency.

Specific Accountability for Everyday Tasks

There are several efficiencies that result from applying a "normal" everyday mechanism of government or business to a medical crisis or other emergency. Among the most obvious benefits is that the use of normal processes and staff personnel already in place eliminates, or at least significantly reduces, the need for any special training. Again, the SNS process helps to illustrate this point. Typically, the CDC will ship the materials needed to the state or states immediately affected by a public-health crisis or similar emergency. It will be the job of the individual states to break down the materials into the smaller quantities needed to supply the counties or cities within the state. The CDC, of course, requires that an accountability system be maintained that can show where specific materials have been delivered after they have been received by the state.

Because the process described involves public health, it frequently happens that state health departments are assigned the responsibility for distribution and inventory control. Here, the first step in the process is to unload the materials received from the CDC and transfer them to local facilities, maintaining a strict inventory control at all times.

All states have their own support and supply departments (by whatever name), the functions and responsibilities of which are similar to those of the federal General Services Administration. Most if not all of those departments have branches or divisions responsible for warehouses where state supplies – paper goods of various types, for example – are unloaded, counted into inventory, and later withdrawn from inventory for delivery to wherever they are needed.

The same warehouses, and the same inventory-control systems, can be used during public health emergencies. The receipt, storage, inventory-control, and delivery tasks are carried out efficiently and safely because those performing the tasks are familiar with the work from carrying out their day-to-day jobs. It should be obvious that the first time a person operates a forklift should not be during an emergency.

Effective emergency management means, among other things, that – rather than designing new forms and/or creating a separate inventory-control system to deal with a public health crisis – it is both less costly and less complicated to use the warehouse staff and other people involved in a crisis situation by assigning them, insofar as possible, to the same jobs they do every day.

The tasks involved have changed considerably, but whether the goal is to distribute medical kits to a smallpox clinic or lay in the supplies needed to withstand a Viking attack, the basic principles are the same: Plans should be generally focused, and day-to-day resources and processes already in place should be used to get the job done.

Port Security: A "Mission Impossible" For the U.S. Coast Guard?

By James D. Hessman

On 11 September 2001, nineteen Al Qaeda terrorists commandeered four large U.S. passenger aircraft, crashed two of them into the World Trade Center Towers in New York City, and one into the Pentagon. The terrorists who had seized control of the fourth aircraft, United Airlines Flight 93, crashed it into a field in Shanksville, Pa., after the passengers revolted and tried to take control back from the terrorists.

Continued on Page 5

Port Security: A "Mission Impossible" For the U.S. Coast Guard?

Continued from page 4

The four crashes killed more than 3,200 innocent people – more than died in the 7 December 1941 Japanese attack on Pearl Harbor. The crashes also cost the U.S. economy more than $500 billion, and led to the formal U.S. entry into the Global War on Terrorism.

Since that second date that will live in infamy, the U.S. armed forces, backed by an allied "coalition of the willing," have overthrown two tyrannical governments, helped install a democracy of sorts in Afghanistan, and – despite a discouraging number of setbacks – seem well on the way to doing the same in Iraq.

On the American home front, the White House and Congress joined forces to create a reasonably workable new Department of Homeland Security (DHS), formed from 22 previously separate offices and agencies, and have funded it generously. Differences between and within a broad spectrum of U.S. intelligence agencies are being gradually resolved, there has been a demonstrable improvement in security at U.S. airports, and the nation's land borders are better protected as well.

Several laws also have been passed that will facilitate additional improvements – e.g., the Aviation and Transportation Security Act of November 2001, which created the Transportation Security Agency (TSA), a major component of DHS.

Nonetheless, a number of "major vulnerabilities" still exist, according to the National Commission on Terrorist Attacks Upon the United States, more popularly known as "The 9/11 Commission." Many if not most of those vulnerabilities are in the field of port and maritime security – where, the commission noted in its final report, the opportunities for terrorists "to do harm" are "as great [as], or greater [than]" at the nation's airports. More than 90 percent of the approximately $5.3 billion appropriated annually for TSA, the commission also noted (with a strong editorial comment immediately following), "goes to aviation – to fight the last war."

By the Numbers – Missions vs. Dollars

The U.S. Coast Guard, which supervised the evacuation of hundreds of thousands of terrified citizens from lower Manhattan on 9/11 – a remarkable achievement that is not even mentioned in the commission's final report – is the DHS agency with primary responsibility for maintaining security in the nation's 361 ports, throughout the 3.4 million square miles of America's coastal waters, along the U.S. Atlantic, Pacific, and Gulf Coasts, and throughout the nation's extensive system of inland waterways.

In the best of times, that is a daunting responsibility for an agency with fewer than 40,000 men and women on active duty, even when augmented by the several thousand Coast Guard reservists who have been called up for varying lengths of time since 9/11. The fact that, at any given time since September 2001, four Coast Guard cutters and approximately 500 active-duty personnel have been forward-deployed to the Persian Gulf cuts into the service's homeland-defense capabilities. But that requirement has been more than offset by several major increases in funding over the past three years, and by the addition of more than 3,000 additional people to the active workforce.

Other offsetting factors include: (a) the requirement to train the enthusiastic and highly dedicated, but also inexperienced, young men and women now entering the Coast Guard; (b) the fact that, despite the increase in appropriations, it still will take several years, minimum, to upgrade and modernize the USCG's outdated and maintenance-intensive inventory of ships, aircraft, and electronics/avionics systems and sensors of all types; and (c) the discouraging recognition that, even when the Coast Guard's innovative Deepwater program – designed to modernize the service's complete hardware inventory across the board – has been fully implemented, there still might not be enough people and equipment to carry out all of the missions the Coast Guard already has been assigned and the even heavier workload it will be facing in the foreseeable future.

A Bullish Report, But Major New Challenges

Coast Guard Commandant Admiral Thomas H. Collins obviously had the latter "challenge" in mind when he commented, during his annual "State of the Coast Guard" address last year, that the service's "mission growth" had "outstripped, in many ways," its budget growth. He listed a few specifics, focused primarily on the service's port and maritime security mission, in what was otherwise a fairly bullish report.

From 2003 to 2004, Collins said, Coast Guard personnel had carried out "thousands of port-security patrols, air patrols, security boardings, and vessel escorts." In addition, he said, the service had established and maintained a number of "new security zones" around the country; developed several "new capabilities" by increasing the number of Sea Marshals on the personnel roster and by creating and deploying several new Maritime Safety and Security Teams (MSSTs, each of which consists of 71

Continued on Page 6

Port Security: A "Mission Impossible" For the U.S. Coast Guard?

Continued from page 5

active-duty personnel and 33 reservists); and had transferred a number of cutters and patrol boats, and their crews, to the port and maritime security mission.

All of those changes, several of which must be categorized as "major," translate into an increased overall workload. Some, a very few, of the service's other important missions have been reduced modestly, but none can be handed over to another service or another agency of government. No government official would accept a decrease in the USCG's lifesaving capabilities, and neither would the American people. A respite in the service's interdiction of illegal aliens, and/or of illegal narcotics, also is unlikely. For one thing, terrorist organizations are known to have used the revenues from illegal drugs to finance their own operations. In addition, some of the illegal migrants who have been stopped in the past have been identified as probable terrorists.

A Terrifying Fraction

Several of the "numbers" problems confronting the Coast Guard are simply overwhelming – and beyond the USCG's own organizational control. The illegal-migrants interdiction mission provides an illuminating example. The Coast Guard is becoming ever more efficient in stopping the flow of illegal migrants from the sea. U.S. air and ground ports of entry also are somewhat more secure than they were before the terrorist attacks. Nonetheless, as the 9/11 Commission pointed out, there are already "more than nine million people … in the United States outside the legal migration system," and "another 500,000 or more enter illegally [each year] … across America's thousands of miles or land borders or remain in the country past the expiration of their permitted stay."

No one knows, of course, how many illegal migrants are terrorists, or potential terrorists, but even a small fraction – one percent of one percent, perhaps – would be a terrifying number.

There are two other numbers, directly related to the Coast Guard's port and maritime security mission, of perhaps cataclysmic magnitude that the service must cope with as best it can. The first is the number of fishing vessels – approximately 110,000 – in the U.S. commercial fishing fleet. The second number is even more impressive: 16 million. That is the number of American "recreational craft" now distributed throughout the U.S. waterways system.

The point here is simply this: There already are tens of thousands, perhaps hundreds of thousands, of vessels now in U.S. waters that are as big as, or bigger than, the one used by Al Qaeda terrorists to attack, and almost sink, the guided-missile destroyer USS Cole in October 2000.

There also are thousands of potential targets in or near the water for terrorists. Approximately 8,000 large ships now call in U.S. ports each year. Some of them are cruise ships carrying as many as 3,000 passengers. Others are heavily laden with toxic chemicals or explosive substances of various types. A successful attack from the water on just one of those ships — or on an industrial complex or a large housing area ashore – could kill perhaps hundreds of people, and could cost the U.S. economy several billion dollars.

Several attacks, in different ports but all at the same time, could shut down the entire U.S. maritime system for an extended period of time and eventually cost far more, in both lives and dollars, than the 9/11 attacks on the World Trade Center and the Pentagon.

Following are a few specific examples, which Al Qaeda as well as the Coast Guard might already be considering as test-case scenarios, that illustrate the extent of the damage possible from just one attack:

--On 6 December 1917 a French ammunition ship, the Mont Blanc, which was carrying 3,000 tons of TNT, collided with the Imo, a Belgian steamer, in the port of Halifax, Nova Scotia. An estimated 1,600 people died in the resulting explosion, which destroyed one tenth of the city.

--Not quite 30 years later, on 16 April 1947, another French cargo ship, loaded with an explosive nitrate fertilizer, exploded in Galveston Bay, killing hundreds of people and destroying most of Texas City, Texas.

--On 17 July 1944, a huge explosion at the naval magazine in Port Chicago, Calif., killed more than 300 men, disintegrated the merchant ship E.A. Bryan, and even caused damage in San Francisco, almost 50 miles away. Less than three months later, on 2 October 1944, the accidental ignition (ashore) of liquefied natural gas leaking from a cork-insulated tank in Cleveland, Ohio, killed 130 people, injured several hundred more, and devastated a major industrial area of the city.

All of these were accidents. How much greater damage, including a considerable loss of life, might result from several well-planned and simultaneous deliberate attacks, either at sea or in port, on larger ships loaded with thousands of passengers, or laden with toxic chemicals or combustibles or both, can only be imagined.

The fact that Al Qaeda has already used small boats on terrorist missions is not comforting. Neither is the realization that the demonstrable improvement in security at U.S. airports probably would not have been funded if 3,200 citizens had not died not quite four years ago while the nation was looking the other way.

State Homeland Security News

By Anthony Lanzillotti

Oregon, Nebraska, Tennessee, and Kentucky

OREGON

City of Portland Selected for Terrorism Exercise in 2007

Portland, Ore., one of the fifteen cities that applied to the U.S. Department of Homeland Security (DHS) in 2004, has been chosen as one of two sites for the "TOPOFF4" exercise scheduled for 2007. The Oregon Office of Homeland Security (OOHS) is planning to use a combination of DHS grant money and corporate donations to fund preparations for the upcoming exercises that will be an essential part of TOPOFF4.

Miguel Ascarrunz, director of the Portland Office of Emergency Management (POEM), recently returned from meetings with DHS officials in Washington, D.C., related to the logistics of TOPOFF4. Ascarrunz advised that four full-time POEM officers are being assigned to preparatory duties for the 2007 exercises. Portland officials will accompany state officials on a trip to the New York, New Jersey, and Connecticut Tri-State Area next month as observers in the TOPOFF3 exercises.

The diverse Portland landscape includes bridges, port facilities, various businesses, and a large convention center. This diversity will challenge the interoperability of federal, state, and local agencies during the exercises, and should provide an excellent summary of lessons learned that OOHS and other states can benefit from.

NEBRASKA

Nebraska Medical Center Receives New Biocontainment Unit

On 7 March 2005, Nebraska Governor Dave Heineman unveiled the new Biocontainment Unit at The Nebraska Medical Center in Omaha. Dr. Julie Gerberding, director of The Centers for Disease Control (CDC), was present at the unveiling and was given a full briefing and tour of the center by Heineman. The governor proclaimed Nebraska to be "a leader in bioterrorism preparedness."

The Nebraska Health and Human Services System (NHHSS), The Nebraska Medical Center (NMC), and the University of Nebraska Medical Center (UNMC) developed the new Biocontainment Unit using a combination of federal grant money and contributions from NMC and UNMC. The unit will allow medical personnel to safely treat victims of contagious and dangerous diseases, whether related to an act of terrorism or some other type of outbreak. The NMC has pledged to assist any other state dealing with an outbreak by accepting patients who would need the specialized care provided by the Biocontainment Unit. Dr. Philip Smith, the medical director of the Biocontainment Unit, describes it as "a valuable regional, and potentially national, resource." The unit's staff includes fifteen nurses and fourteen respiratory technicians and therapists, all of whom are on call 24/7.

TENNESSEE

Additions to the SensorNet Threat Detection and Tracking System

Oak Ridge National Laboratory (ORNL) has been using various sites in Tennessee as test beds during the past year for the ORNL SensorNet technology. SensorNet is a prototypical early warning system designed to provide real-time alerts of potential chemical, biological, or radiological threats. Numerous sensors and communication devices have been installed at various sites in Oak Ridge, Nashville, Knoxville, Memphis, Chattanooga, and the Tri-Cities area.

The SensorNet mission is to detect and track a hazardous release in real time, predict its movement, and determine the possible effect on the local population. The I-40 intersection at Watts Road in Knox County, Tenn., is one of the busiest in the country, hence ORNL's recent decision to add more sensors to the system at this location. Among the more important equipment items are new radiation detectors, thermal cameras, license-plate readers, and wind-mapping systems. Mobile SensorNet equipment has also been implemented and tested at major sporting events in Tennessee.

The success of the SensorNet program is the result of collaboration between ORNL, the University of Tennessee (UT), and various Tennessee homeland-security and law-enforcement agencies. Tennessee is bordered by eight other states, has the I-40 major thoroughfare running through it, and is home to the nation's largest cargo airport (Memphis). These geographic and economic particulars, combined with the collaborative SensorNet effort, are establishing Tennessee as a major hub of homeland-security research, development, and training.

KENTUCKY

Exercises, Spills, and Drills

Last month, the Kentucky Office of Homeland Security and the Kentucky Division of Emergency Management sponsored two exercises testing the state's ability to respond to large-scale incidents. The first exercise, a live drill, took

Continued on Page 8

State Homeland Security News

Continued from page 7

place in Paducah at the U.S. Department of Energy's Gaseous Diffusion Plant, which contains nuclear fuel. The exercise was designed to test communications between the National Guard and state and local emergency responders during a radiological event. The Executive Inn in Paducah served as the command post, where a large computer screen tracked the position and movements of responders on the ground.

Members of the Kentucky Division of Emergency Management Region 2 Office met at Lake Barley Lodge for "Winter Spill" on February 23. Winter Spill, a tabletop exercise sponsored by the Kentucky Office of Homeland Security, was based on a Weapon of Mass Destruction attack.

The annual Statewide Tornado Drill for 2005, scheduled to begin on March 8 at 1007 hours, calls for schools, businesses, and local responders all to take part, performing the same actions they would take if it were an actual event. The Kentucky Division of Emergency Management expressed concern that some citizens might take the drill lightly, and encouraged all state residents to participate and test his or her own preparedness plans.

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