domestic preparedness .com

DomPrep Journal

Volume II, Issue 3 | Expanded Print Edition | Special Advertising Section

Secure the Perimeter

And Redefine the Border

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

Does your field bio-detection equipment measure up?

What *do* you look for when choosing a new device, or replacing outdated equipment?

Independently Evaluated

RAMP's market leading sensitivity and reliability has been validated by the US Army, the Canadian Department of Defense, and State Public Health labs.

View findings on-line at www.responsebio.com/downloads

Field Tested

Rugged and reliable, RAMP is relied upon by first responders, military personnel and public health officials across the US and around the world.

RAMP works where you need it. Test on-site for anthrax, ricin, small pox and bot tox.

Hands-on Training

FREE on-site training is included with every new RAMP System. Our trainers are experienced first responders who've been in your shoes.

Much, Much More

We can tell you lots more about RAMP's ease-of-use and 15 minute results. Call **1.888.591.5577** to learn all you need to know about the best in field bio-detection, by every measure.

RAMP®
WHEN ANSWERS COUNT

Call 1.888.591.5577 to order a FREE Demo CD.

visit www.responsebio.com/specials for special offers now available

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
Managing Editor & Interviews
jmorton@domprep.com

Susan Collins
Subscription Mgr. & Layout/Design
subcriber@domprep.com

Sharon Stovall
Web Content Coordinator
sstovall@domprep.com

Paige Dunn
Customer Service Coordinator
pdunn@domprep.com

DomPrep Journal is electronically delivered 26 times per year by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; 410-518-6900; fax 410-518-6020 and available at DomPrep.com

Articles are written by professional practitioners in homeland security, preparedness, and other 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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

Publisher's Message

By Martin (Marty) Masiuk

Prevention, Precautions, and Common Sense. That brief description fairly well summarizes the collective practical and policy recommendations provided by three distinguished authors in this issue of *DomPrep Journal*. Neil Livingstone's advice is possibly the most controversial: If the U.S. government is truly serious about keeping terrorists out of this country, it should build a "wall" or physical barrier of some type along the entire length of the U.S.-Mexican border. Chris Hawley steps up to the plate next with several practical suggestions about various WMD detection devices now on the market or in the R&D pipeline. And Brian Finch follows with helpful advice about the landmark 2002 SAFETY Act and how private-sector businesses and organizations can benefit from the many protections the Act provides to encourage the creation, production, and distribution of a broad spectrum of anti-terror instruments, devices, and technologies.

The implementation of Dr. Livingstone's suggestion would make it considerably more difficult not only for terrorists to enter the United States, but for illegal migrants as well – which is one reason it would be opposed by those who have vested economic and/or political reasons for encouraging (or at least ignoring) illegal migration. One rationale for "looking the other way" at illegal migration is that those coming into this country illegally "are only looking for jobs that Americans do not want." No evidence is ever offered for this naïve statement, always enunciated as a universal truth – nor, interestingly, has anyone ever provided a detailed list of such jobs. The fact that the building of a wall such as that suggested might well precipitate considerable controversy – both nationally and internationally – is not enough to quash the idea without at least a thorough and totally honest public debate.

There should be absolutely *no* debate about Chris Hawley's recommendations – which apply to the purchase and use not only of WMD detection instruments but of *any* high-tech products and services: Be informed; seek expert advice; ask questions; test before buying; compare with other products and services of the same type; and be aware of "associated" expenses such as maintenance costs and the cost of paper products and other consumables that might be required. Good advice for everyday shoppers as well.

Brian Finch's topic, the liability protections provided by the SAFETY Act, is one of major and increasing importance to decision makers at all levels of government, and in the private sector as well, particularly in an era when additional terrorist attacks are considered by most experts in the field to be not only possible but inevitable. As an article by William Cook in the May 2004 issue of *CSO* noted, one court already has ruled that the danger of a plane crashing into the World Trade Center should reasonably have been foreseen, and another court postulated that attacks by computer viruses or worms are "completely foreseeable events." Whether the same logic would apply to the "shelter in place" policies recommended by some counterterrorism experts has yet to be determined. In any event, businessmen as well as government officials would be well advised, as Finch recommends, to avail themselves of the numerous legal protections now provided by the SAFETY Act rather than to rely on the common sense of the U.S. court system.

Cover Photo of an intruder (terrorist?) scaling a fence to cross the U.S. border illegally may be simulated, but depicts a real and present danger to U.S. security - see Neil Livingstone's article beginning on page 5. One way to stop illegal entry, he suggests, is to build a long border barrier studded with electronic devices that will trigger an immediate alarm when an intruder has been detected. Photo provided by CCD Photonics Ltd. (www.kolumbus.fi/ccdphotonics).

Arriving first on the scene means you never know what you're going to encounter.

Today that could include life-threatening chemical nerve agents which may be lethal in seconds.

Immediate evacuation and wearing PPE is essential, as is being equipped with auto-injectors that are designed to administer antidotes in emergency situations such as these. Unlike a syringe which can be cumbersome and time-consuming, auto-injectors provide a quick and portable drug delivery in just two steps.

Hope for the best. Prepare for the worst.

You can't rely solely on antidotes for protection, but you can be better prepared for the worst. **Call today—Meridian can help you prepare.**

MERIDIAN
MEDICAL TECHNOLOGIES™

Protecting Those who Protect Us™

www.meridianmeds.com
800.638.8093

How to Build a Protective Wall Along The U.S.-Mexican Border

By Dr. Neil Livingstone, GlobalOptions

The 2,000-mile long U.S.-Mexican border represents one of this nation's key vulnerabilities to international terrorism. Figures are imprecise, but various authorities have estimated that eighty-five percent of the illegal immigration through that border is by Mexican nationals. It is the other fifteen percent, however, that most worries U.S. security officials. According to Michael Flynn, writing in the 11 December 2005 edition of *The Washington Post*, on any given day people from nearly 60 countries, "most of whom had hoped to use Mexico as a gateway to the United States," were being held in Mexico City's migrant detention center.

The border is so porous that illegal immigrants run little risk in entering the United States from Mexico. While the vast majority of all illegal immigrants may be seeking economic opportunity, as has been claimed, a small number, mostly of Middle Eastern background, also may be entering this country to set up sleeper cells and carry out terrorist attacks.

Those opposed to immigration reform reject the idea that there is any significant threat posed by the poorly defended southern border, alleging that there is little or no evidence that terrorists would use that route to infiltrate into the United States. But, contrary to such claims and misinformation, the inability of the United States to stop illegal immigration along the border has been recognized by U.S. adversaries for years and has been exploited in a variety of ways.

In the second volume of their monumental work based on the KGB archives, Christopher Andrew and Vasili Mitrokhin describe how Moscow Center used Sandinista revolutionaries to infiltrate the United States along the Mexican border and scout out potential sabotage targets. A KGB sabotage and intelligence group, they pointed out, was "formed on the U.S.-Mexican border with support bases in the area(s) of Ciudad Juarez, Tijuana, and Ensenada."

Sandinista operatives, disguised as illegal Mexican immigrants, the two authors continued, slipped into the United States and scouted "American military bases, missile sites, radar installations, and the oil pipeline (codenamed START) which ran from El Paso in Texas to Costa Mesa, California. Three sites on the American coast were selected for DRG landings, together with large-capacity dead-drops in which to store mines, explosive[s], detonators, and other sabotage materials. A support group codenamed SATURN was tasked with using the movements of migrant workers (*braceros*) to conceal the transfer of agents and munitions across the border."

While the U.S.-Mexican border is where mass illegal immigration potentially meets global terrorism, the Canadian border with the United States is also a problem, largely because of Canada's inadequate intelligence capability, the lax enforcement of its criminal statutes, and the regular abuse by Middle Eastern extremists of Canada's asylum program.

So what is the answer to improving U.S. border security? Some have suggested the use of more border guards and heightened enforcement, as well as a guest worker program that would seek to manage the flow of Mexican workers, in particular, into the United States. But would that be enough to stem the flow? Most knowledgeable observers say no. What is needed, they maintain, is a

barrier like the one Israel has constructed to prevent Palestinian infiltration.

Walls, Fences & Barriers

Israel's so-called wall is not really a wall but a multifaceted barrier. In some places it *is* a wall – designed primarily to prevent Palestinian sniping at cars traveling along Israel's major north-south axis road. In other places it is only a fence. The entire barrier, however, is equipped with sensors and alarms designed to detect any movement by infiltrators.

The Israeli barrier has been an unqualified success, virtually shutting down cross-border raids and infiltrations by Palestinian terrorists. In fact, it has exceeded the expectations of even its strongest proponents.

The United States could construct a barrier, not unlike the Israeli barrier, along its southern border that, if properly installed and administered, would almost completely shut down cross-border illegal immigration. It would not be extraordinarily expensive or time-consuming to do so, and the barrier would not constitute a particularly difficult engineering challenge.

In fact, there already is a high metal fence, nearly all of it in urban areas, along about five percent of the border between the United States and Mexico. However, because much of the border is protected by a wire fence only three feet high, illegal immigrants simply avoid the high metal fence and cross the border where it is less difficult to do so.

The barrier itself could be constructed of steel, concrete, chain link, or a variety of other materials. It should not be a passive fence but, rather, what is known as an "active" fence and designed to detect and delay illegal entry or even thwart it altogether. It also should be well-illuminated with light poles every sixty feet or thereabouts so that CCTV cameras could relay images of anyone attempting to breach the barrier back to monitors manned by border patrol agents.

Consideration should be given, in fact, to building a double fence, with the second fence electrified. The first fence (or barrier), which should be relatively high and topped with razor wire or concertina, would serve to delay the intruder/illegal immigrant(s) and, because it would be configured with sensors, to alert border response units. If an intruder/illegal immigrant nonetheless succeeded in breaching the first fence, he (or she) would be trapped between the two fences and usually unable to get through the second, electrified, fence.

The latter would be a non-lethal-pulse electric fence. Wires within the fence would transmit brief high-voltage pulses

of electricity that would shock an intruder but not cause permanent damage.

The area between the two fences should be about 15 feet wide and could be built in the form of a recessed concrete ditch twelve feet deep, broader at the bottom than at the top, with sloping sides. The walls of the ditch could be coated with a number of lubricants and/or other materials that would make them even more difficult to climb.

A Broad Spectrum of Sensors

Barrier planners could incorporate a variety of different sensors. Among those they could choose from are the following:

1. *Point Vibration Sensors:* Inexpensive and relatively easy to install, point vibration sensors could be mounted on the barrier to detect disturbances associated with climbing, sawing, cutting, or lifting the fence.

2. *Ported or "Leaky" Coaxial-Cable Sensors:* Ported coax or "leaky" cable detection systems generate an invisible electromagnetic field around two cables that are generally buried in the ground approximately three feet apart. One of the cables transmits signals; the other receives signals. Such sensors, which are most often used where covert detection is involved, could provide an additional level of detection, particularly when coupled with point-vibration sensors.

3. *Seismic Sensors:* Such sensors are particularly useful in detecting tunneling, which has been a continuing problem on both the Mexican and Canadian borders.

4. *Electrostatic Field Disturbance Sensors:* Electrostatic field disturbance sensors generate an electrostatic field between and around an array of wire conductors. These sensors, which detect changes or distortions in the field, could be mounted on the barrier parallel to one another, and to the ground, to provide uniform sensitivity along the entire length of the barrier.

5. *Microphonic Cable Fence Disturbance Sensors:* Sensors of this type are designed to protect fences and barriers against climbing, lifting, or cutting. They are quick and easy to install, comparatively inexpensive, and provide a high probability of detection.

6. *Advanced "Microstain" Fiber Option Sensing Systems:* A microstrain fiber optic sensor is an advanced in-ground or fence-mounted detection system that uses a multi-core fiber that can detect minute vibrations. With a sophisticated signal-processing and analysis system, different types of vibrations can be identified and those attributed to false alarms eliminated.

Larger Response Force Also Needed

President Bush recently told the American people that the United States will "return every single illegal entrant." But it seems obvious that it would make more sense to prevent illegal migrants from entering in the first place rather than having to chase them down and then expel them. A permanent barrier would be not only far more practical and effective, but also more humane.

An important key to the success of the barrier would be to have enough border patrol officers, stationed at intervals along the border, to respond quickly and effectively when anyone would try to breach the barrier. Without a timely response effort the whole project would fail.

The U.S. Border Patrol recently initiated the use of drones mounted with cameras to patrol the border. Continued use of the drones, combined with CCTV, sensors, and roving patrols, would make it extremely difficult and perhaps impossible for illegal migrants to circumvent the barrier.

If it is true, as is frequently alleged, that the U.S. economy needs what are currently described as illegal workers, mostly from Mexico and Central America, the creation of an effective barrier wall could be combined with a guest-worker program, such as the one President Bush has proposed, that would provide a suitable vehicle for legalizing the admission of foreign workers into the United States. Until that happens, though, stopping illegal immigration is perhaps the most important step the U.S. government can take to protect this nation, the American people, and the nation's economic resources.

Special Report

New Technologies for WMD Detection

Interview With Chris Hawley, Fire/HAZMAT

DomPrep Journal's John F. Morton met recently with Chris Hawley (left) to discuss the various systems, devices, and technologies now available, or in the development stage, that can be used by first responders to detect the presence of WMDs (weapons of mass destruction). Following are selected excerpts, slightly edited, from that discussion:

Morton: *Chris, you have been focusing a lot of your thought and training programs on the use of WMD detection technologies and their relationship to PPE (personal protection equipment). Remind us why, if you will.*

Hawley: You know, it goes without saying that it is particularly important for response agencies not only to understand but also how to use WMD detection devices – which are, in addition to protective clothing, the responders' primary protection against WMD materials. It also is critical to ensure that proper protective clothing is being used, and to determine whether proper isolation and protective measures are being employed.

Morton: *Among the wide variety of detection devices available, what type interests you most?*

Hawley: The type of handheld portable devices that could be used by response agencies.

Morton: *Such as?*

Hawley: Well, those that offer protection against a wide variety of hazards in the basic risk categories: fire, corrosives, and toxics, for example. And radioactive substances. Devices that alert response personnel to potentially hazardous situations. Devices that enable responders to take a risk-based approach to determine what protective clothing is appropriate, and how much.

Remember, though, that because terrorists have common industrial materials at their disposal and response agencies may encounter ordinary hazardous materials in many situations, these common risk categories I mentioned must always be monitored. A multi-gas instrument – such as one that detects and measures explosive [flammable] atmospheres,

oxygen content, carbon monoxide, and hydrogen sulfide – is an important instrument that should always be used.

But some WMD detection devices are not intrinsically safe, so a responder should always know if he or she is in a potentially explosive atmosphere. If response personnel are wearing air-purifying or powered air-purifying respirators, they have to know the oxygen content to ensure their own safety when they are using these respiratory devices.

Another device, which may be a part of the multi-gas instrument – or may be separate – is the photo-ionization detector, also known as a PID. This device will alert the user to potentially toxic materials in the air. It's a very sensitive device that can detect very low amounts of those materials. One PID in particular has the ability to detect materials in the parts-per-billion, while others are only at the parts-per-million level.

You also can use some simple pH papers, which will alert the user to potentially corrosive atmospheres and let response personnel know about aggressive acids and bases that might be present, which is what pH papers do.

The last risk category I mentioned is for the detection of radiation. Here, response personnel can use a pager-style device or a radiation-detection device. The pager-style device is easier to use, but responders have to make sure that they use a device that provides a dose rate.

Morton: *Have we gotten to the point where a handheld portable detection device will give you an on-site analysis comparable to what you get in a laboratory analysis?*

Hawley: Well, the current detection devices – even though they are becoming more sophisticated – cannot be replaced by laboratory testing. Laboratory tests are the gold standard of analysis – and, I would argue, the only tests that can be used effectively in court cases.

I also should mention another issue of importance – namely, that there is no single device that covers all risk categories. In other words, there are chemical and explosive and other types of detection devices, but none that detects radiation, *and* chemical, *and* biological [materials], *and* explosives.

No single device ... covers all risk categories

Morton*: Can you tell our readers a little more about biological detection devices?*

Hawley: The area of biological detection is a complicated one, because the current devices are not very quick, and some suffer from accuracy deficiencies. Some work is being initiated on a handheld device that has the potential to detect biological materials in the air, but a workable ready device is several years away. If you want effective biological detection, you should look at a range of devices and technologies. Devices such as a Fourier Transform Infrared Spectroscopy device – what is called an FTIR device – is a good one to start with.

A low-cost recommendation is to use a specific protein test. To save responders time and money, I advise going with one that uses a DNA match to perform its testing. To provide confirmation or additional analysis, a PCR [polymerase chain reaction] device is currently the best way to detect materials that are potentially biological in nature. Another option is to use a handheld assay [HHA] fitted with a reader to test for common biological materials – you *always* should use a reader with these assays.

When purchasing a PCR or HHA device, you should compare the current models that are on the market. Compare them, for example, by the number and ease of steps required to prepare and analyze a sample. Also compare the running times and the cost of the disposable supplies needed with each.

Remember: There is a wide variety of the ways in which samples are prepared for analysis in the machine. You should always divide the suspect material into two separate containers, following proper evidentiary processes. One container is for your field testing. The other one is for the laboratory testing that might be required for a court case.

Morton: *Is there any new cutting-edge biological-detection technology on the horizon that you think is particularly promising?*

Hawley: There is one very new device which uses micro-fluidic separation as its sensing technology. That technology could be compared to what is used in high-tech immunoassay testing, because it relies on the migration of impregnated dyes moving through the testing chip. Various biological materials have retention times in the testing chip that are already known. The chip is used to compare the retention times of the sample being tested. But the new device I just mentioned – I don't think I should name it at this time – still needs some additional evaluation to determine its true effectiveness.

Morton: *What about chemical detection devices? What breakthroughs do you see there?*

Hawley: In the chemical field, there are some new devices, and there are some devices that have been reformatted or reconfigured to enhance their capabilities. One device is a combination unit that has dual-sensing capabilities – it's equipped with both an ion mobility sensor, or IMS, and a surface acoustical wave or SAW sensor. Having both of these two technologies is advantageous, because they combine accuracy with the ability to detect low amounts of the product being analyzed.

Any device that uses a combination of detection technologies is on the right track, I think, because, considered alone, each detection technology has its own unique deficiencies. Combining two or more helps minimize the potential false-positive issues. A FTIR unit that is specific to detect unidentified gases is available and can be useful not only in WMD situations but also for more routine cases – sick-building investigations, for example. On the other hand, a standard FTIR unit may be very helpful in providing the potential identifications of liquids and solids, but it might not be able to detect gases in an easy fashion.

One manufacturer, I know, provides a Raman Spectroscopy unit that can Bluetooth – wireless – connect to their FTIR unit, which allows for the spectra of the two units to be compared fairly quickly. Raman Spectroscopy devices are new to the emergency-response market and I think will be useful tools in the WMD tool box. Used in combination with FTIR units, they can be of great assistance when dealing with an unidentified material.

The FTIR devices themselves have a big advantage in the number of materials they can detect, because they have large libraries. But the Raman devices have a different advantage in that the material [being detected and/or analyzed] can be read through a glass or plastic container. You have to remember: Like many other detection devices, the FTIRs and the Raman units both have slight limitations in the fact that they are not 100 percent accurate. They are important tools but should never be used alone.

Morton: *What do you consider to be the cutting-edge technology in chemical detection?*

> ***Any device that uses a combination of detection technologies is on the right track***

Hawley: There is one device that is fitted with a new variety of detection sensors and uses a miniature chromatograph column in combination with a SAW sensor. It has fairly low detection limits – in the parts-per-billion range, and that would be very useful. Much like its cousin, though, the biological detection device that uses micro-fluidics, this device needs some additional testing and evaluation before we can judge its true abilities.

Morton: *Chris, you have commented a couple of times about the need for responders to be smart shoppers. What specific advice can you give our readers in this area?*

Hawley: Always try before you buy. And remember: *You* are the customer. If you are going to invest thousands of dollars in a detection device, make sure it is one that your lowest-echelon people can operate. If only your best responders can operate the device, you are setting yourself up for failure. So step outside your normal purchasing box and look at all the vendors who are selling various devices and technologies. Compare the devices side by side, counting the number of steps required to prepare a sample, for example. In short, determine which device is the easiest to use and offers the best range of options.

One or two other things to remember: First, devices that can be used in everyday hazardous situations are usually better to buy than devices that have WMD capabilities only. Also, compare the set-up times and the cost of the disposable supplies needed, as well as the shelf lives of those supplies. Having a device in your tool box that does not require instructions for use is advantageous, and having one that requires only a minimal set-up should be a prime consideration as well.

Most important of all, though: Ask the vendors lots of questions. Call them on their claims. Ask about problems people may have been having with the device. Also, ask for references and follow up by calling those references. It also would be a good idea to study the independent test results that many manufacturers have available. Examine the raw data. Then go back again with this data and ask more questions of the vendor.

Morton: *Chris, that's really great advice. Thank you so much for your time, and for sharing your expertise with our DomPrep readers.*

Chris Hawley, a firefighter, a HazMat responder, and a former special operations coordinator for the Baltimore County (Md.) Fire Department, is now a project coordinator for the Computer Sciences Corporation with responsibilities for various WMD-related programs throughout Eastern Europe, Central Asia, and other parts of the world. The author of five texts on hazardous materials and terrorism response, he also has written numerous magazine and trade-journal articles.

ARE YOU PREPARED FOR A CHEMICAL CRISIS?

AP4C

Handheld Industrial or Military Chemical Alarm Detector

NEW

Our new AP4C detector is the most versatile portable detector available. It quickly and simultaneously detects a wide array of hazardous chemical agents. Constructed to rugged military specifications it starts quickly and has no "on-shelf" costs.

Advanced Spectro-Photometry Technology Detects

- Nerve Agents
- Blister Agents
- Blood Agents
- Homemade Agents
- Vomiting Agents
- Flammable Hydrocarbons
- TICs & TIMs
- Precursors

PROENGIN

405 N.E. 8th St.,
Ft Lauderdale, FL 33304
(954) 760-9990
FAX (954) 760-9955
e-mail: contact@proengin.com
www.proengin.com

The SAFETY Act and Preparedness

By Brian Finch, Safety Act

In order to be properly prepared for another terrorist event, homeland-security efforts at all levels of government and in the private sector must have access to safe, reliable, and effective anti-terror tools. Many companies have highly useful products or services to offer, but there often are significant barriers to bringing a product or service to the marketplace. In the U.S. homeland-security market in particular, the fear of devastating liability being imposed on products or services has caused many companies to reconsider their plans to sell their wares in the homeland-security marketplace.

Such fears are quite valid given the highly active plaintiffs' bar in the United States, as well as a number of decisions in U.S. courts holding that entities providing security in a number of events (the 9/11 terrorist attacks, for example, the 1993 World Trade Center bombing, and the 1996 Olympic Park bombing) could be or actually were liable for damages arising out of those events.

To lessen these concerns and at the same time encourage the development and deployment of anti-terror products and services, the U.S. Congress passed, and President Bush signed into law, the Support Anti Terrorism By Fostering Effective Technology Act of 2002 (usually referred to as the "SAFETY Act"). Under that Act, the U.S. Department of Homeland Security (DHS) was given the authority to award a number of liability protections to the sellers of anti-terror products and services. Understanding what the SAFETY Act provides and how it complements other anti-terror efforts is important for businesses and other entities engaged in preparedness efforts.

When they receive SAFETY Act protections, the sellers of anti-terror products and services, and their customers, are given a shield from liability arising out of terrorist attacks. For SAFETY Act-certified technologies, these protections include a presumption that the seller is dismissed immediately from such suits. Various provisions of the Act also postulate that: (a) The seller cannot be sued for punitive damages; (b) the seller cannot be sued in state court, only in federal court; (c) none of the seller's vendors, subcontractors, suppliers, distributors, or customers can be held liable; (d) these protections apply regardless of whether the sale of these technologies are to governments that are entitled to expedited reviews of their application; and (e) only the seller may be sued (customers and suppliers, however, may not be sued as a matter of law).

A Broad Blanket of Immunity

It is important to understand that the SAFETY Act's definition of "anti-terror technologies" includes not only products and services, but also training, information technology, and support services of various types. Essentially, therefore, when a product or service is considered to have some form of an "anti-terror purpose" (that purpose does not have to be solely to defend against acts of terrorism), it will be eligible for the protections provided under the SAFETY Act.

Among the many examples of products and services that have been awarded SAFETY Act approval are explosive detection devices, anti-terrorism computer data-basing software, airport security services, perimeter security services, vulnerability-assessment services, maintenance services, and night vision equipment.

The protections of the SAFETY Act apply regardless of whether the customer is a federal, state, or local government entity, or a commercial user. The protections are awarded, though, only after a thorough review of the seller's product or service has been conducted by DHS – more specifically, by the department's Office of SAFETY Act Implementation within the DHS Science & Technology Directorate.

The DHS review includes, among other things, not only an examination of what the specific product or technology is designed to do, how it works, and how the seller ensures the quality of the item, but also any evidence that demonstrates that the product or service is effective as an anti-terrorism instrument. After the review has been completed, the DHS under secretary for Science & Technology will make the final determination as to whether the subject of the application should be awarded SAFETY Act approval.

Comforts and Reassurances

For government as well as private-sector entities in the preparedness community, understanding the benefits of using SAFETY Act-approved products and services should be apparent. The most important benefit, of course, is that, by using SAFETY Act-approved products or services, preparedness entities at all levels of government will be giving themselves an extra layer of liability protection. This is important because many state and local government entities assume that being a unit of government protects them from all relevant liabilities.

That is not the case, however, and liability concerns have grown significantly since the 9/11 attacks. One of the most important recent examples is a decision in New York State holding that the Port Authority of New York/New Jersey was liable in connection with its security efforts related to the first (i.e., 1993) World Trade Center bombing. That decision has caused considerable concern across the country that security efforts conducted by government or quasi-government entities can and will be held liable for conducting inadequate security measures.

Using SAFETY Act-approved products and services can ameliorate at least some of these liability concerns. If, for instance, a state government entity were to contract with a SAFETY Act-approved company to provide security-guard services at public buildings, it would enjoy the liability protections offered by the SAFETY Act (e.g., the immediate dismissal of claims arising out of a terrorist attack related to the performance of the security guards). Obtaining such benefits would obviously then lower the liability concerns of a user, and that reassurance would bring with it some measure of financial relief as well.

Additionally, considering that SAFETY Act-approved products and services have gone through a fairly rigorous review process by DHS, contracting for and using those products provides an inherent measure of confidence in their ability to be used as effective anti-terror tools. Although SAFETY Act approval is not and should not be considered an endorsement or a "Good Housekeeping" seal of approval by DHS per se, it can be safely assumed that the department has thoroughly reviewed the item in question and determined that it has met the requirements of the SAFETY Act. This means in turn that the product or service, as it has been described by its seller to DHS, has been determined to be a safe and effective product that could be used in preventing, defending against, and/or responding to acts of terrorism.

... Anti-terror technologies include not only products & services, but also training and information technology ...

Stringent Protections, Judicious Choices

Preparedness officials at all levels of government, and in the private sector, may therefore want to consider the implications of such approval in determining what products or services to procure for their anti-terror efforts. Although a SAFETY Act award does not necessarily mean that the product or service is the best in its class, it strongly suggests that it is one that has been deemed to qualify for certain well defined and usually stringent liability protections.

Moreover, although it is not necessary for a product or service to be SAFETY

Act-approved on DHS grant lists (i.e., the Authorized Equipment List), SAFETY Act-approved items eligible for purchase through the use of grant funds would be judicious procurement choices for state and local governments, if only because the purchase of such items will not only convey to the customer the liability benefits provided by the SAFETY Act but also give that same customer the reassurance that the item has been thoroughly reviewed by DHS.

A Powerful Liability-Mitigation Tool

The SAFETY Act is, in short, a powerful liability-mitigation tool that preparedness officials should be well aware of when determining how best to equip themselves and their departments to cope with terrorist events. While government entities may not necessarily themselves apply for SAFETY Act approval, they can take advantage of the protection benefits provided under the Act by procuring SAFETY Act-approved items. By so doing, they will obtain numerous liability protections – and also take some measure of comfort in knowing that those items have already been reviewed in detail by DHS. The SAFETY Act, therefore, is a measure all preparedness leaders should be aware of and try to use to its fullest extent.

Brian Finch is a homeland security attorney at McKenna Long & Aldridge who focuses his practice on SAFETY Act matters and has already successfully represented many companies in obtaining SAFETY Act coverage. Brian is also a Senior Fellow at the George Washington University Homeland Security Policy Institute.

Michigan, Illinois, and Pennsylvania

By Adam McLaughlin, State Homeland News

Michigan
WMU Addresses Aviation Security Issues

Western Michigan University's College of Aviation, which has been quietly building an industry-research consortium, is now poised to pursue federal partnerships for work aimed at improving the nation's airline-security measures.

"We are putting together an amazing group of collaborators to enhance the significant strengths our college brings to the table," said Rick Maloney, dean of the WMU College of Aviation. "We plan to combine the resources WMU offers as a research university, the industry experience of our college leadership, and the security expertise of our collaborators to address specific areas in which we believe we can make a difference."

The college's pursuit of federal funding will concentrate on four areas of research that have been identified as of major importance in the post-9/11 world. More specifically, Maloney said, the college will focus on: (a) on-board communications between the cockpit and the flight attendants; (b) the use of in-flight video monitors and wireless communications; (c) cockpit defense and control strategies; and (d) the development of universal standards for air-to-air communications.

The proposed collaborators for research include a firm with extensive non-aviation homeland-security credentials, a second firm with significant experience in airline-security training, and a commercial airline that has a proven track record in the innovative use of technology for security purposes. Maloney said he also hopes to bring the faculty and staff of WMU's College of Aviation into the research process, particularly in the areas of criminal justice and law-enforcement training.

Illinois
Chicago Unveils New Emergency Management Center

The city of Chicago unveiled a new $4 million high-tech emergency management center early last week that is expected to dramatically improve the city's ability to cope with manmade as well as natural disasters of all types. The new City Incident Center (CIC) will greatly enhance the city's capability to streamline and coordinate response actions to everything from major snowstorms to possible terrorist attacks, officials said. "This is a logical step in our effort to effectively respond to emergencies on a citywide basis," said Andrew Velasquez, the director of the CIC.

The CIC is a 3,000-square-foot addition to the 9-1-1 center on West Madison in Chicago. Twenty-four computer workstations already are in place to assist the various city departments and agencies that would be coordinating their various activities in times of potential crisis. One of the center's principal features is a high-resolution digital-video unit capable of displaying images received from multiple sources. In addition, there are twelve big-screen TV units that individually and collectively can be used to display images received from weather services, news sources, and a large number of

surveillance cameras that are set up around the city.

Chicago Mayor Richard M. Daley said he would not be completely satisfied until there are even more surveillance cameras installed throughout Chicago to record incidents of potential significance and transmit the images to the City Incident Center. Daley and other city officials said that Chicago already has the most sophisticated emergency communications system in the country, but that the city could and would use more cameras over the next few years.

Pennsylvania
Altoona Plans to Use Fleas To Check Water Security

Much as coal miners have used canaries for many years to detect toxic gases in mines, the city of Altoona plans to use a special type of water flea to test reservoirs in the area for toxins that could be dumped by terrorists. The Altoona City Authority said it would use Daphnia water fleas to check the water in the city's reservoirs. The authority recently agreed to pay $4,450 for a Kingwood Diagnostics Q-Tox startup kit, and about $10,200 annually to maintain the system.

The authority's current testing seeks to detect mostly organic compounds that can leach into its 13 reservoirs, but does not now check for poisons such as cyanide, ricin, or soman. Use of the tiny brownish crustaceans, which are hypersensitive to poisons, will remedy that deficiency, officials said.

To test the water, examiners will add sugar that has been tagged with a fluorescent marker that does not glow while connected to the sugar. In non-poisoned water, the fleas will digest the sugar and, by so doing, break the marker away, after which the glow can be seen within the translucent bodies of the animals. In water that has been poisoned, though, the Daphnia become sick, are not able to digest the sugar, and therefore will not glow.

Altoona officials say the new system is not foolproof, because normal substances in the water also might interfere with the results. However, the system also gives municipalities a better overall picture of the chemical profile of the water, said Carlos Murawcyk, president of Kingwood Diagnostics. Authority officials said the city plans not only to test its water weekly but also to conduct emergency tests at various unspecified times.

BIOLOGICAL AGENT IDENTIFICATION

FIRST RESPONDERS – MILITARY – SECURITY

RESULTS IN 30 MINUTES

Proven Tools, Accurate Results–

Better Decisions.

The RAZOR systems small, rugged design and easy sample preparation make it the ideal instrument for first responders, homeland defense and security personnel.

It's a hand-portable, field hardened, biological agent identifier developed in support of the US Military. It simultaneously tests up to twelve samples in less than 30 minutes.

- Analyze up to twelve 100 µl samples
- Tests for Anthrax, Plague, Tularemia and other agents*
- Battery operated - rechargeable
- Freeze-dried reagents - just add sample and water
- Tested for accuracy by the US DoD
- Weight: 9.1 lbs. / 4.1 kg

RAZOR™ Instrument with pouch loading kit

Instrument Size
6.6 x 4.4 x 9.1 inch
17 x 11 x 23 cm

Visit us at **www.idahotech.com**
to learn more about this cutting edge capability.

Idaho Technology Inc.

*Check Web site for tests available.

390 Wakara Way, Salt Lake City, Utah 84108, USA | 1-800-735-6544 | www.idahotech.com

Don't Risk It!

There's a deadly chemical release. Why trust your safety – and the public's safety – to a product without a track record?

AreaRAE

Wireless HazMat Detection

- Remotely measures gas, vapor and radiation threats from up to two miles away
- See the entire threat from Incident Command
- With over 500 systems deployed, the AreaRAE is the standard for rapid deployment systems

Used by:

- Fire Departments
- Law Enforcement
- Industrial First Response Teams
- State and Federal Agencies

www.raesystems.com

Hazardous Environment Detection Solutions

RAE SYSTEMS