domestic preparedness .com
T.I.P.S. Total Integrated Preparedness Solutions

Volume 1, Issue 2, January 26, 2005

## This Issue:



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

# Hidden Dangers in the Use of Non-Lethal Technology

**By Jay Kehoe**
Law Enforcement

Six years ago, Capt. Sid Heal of the Los Angeles Sheriff's Department suggested, at a seminar on non-lethal technology, that the technology used by police to carry out their law-enforcement duties is likely to change more in the next ten years than it had over the past two centuries.

Today, slightly more than halfway through that ten years, his comments already have been validated. One result, though, is that law-enforcement administrators intent on protecting their officers, reducing injuries to suspects and any others on the scene of a crime, and keeping within ever-present budget limits are being bombarded with a broad spectrum of new, "improved," and "upgraded" items of equipment.

To understand the extent of what has become a major issue facing these administrators it is first necessary to specify what is meant by the term non-lethal technology. The answer depends on the definition one chooses. Most if not all progressive police administrators seem to have been gravitating to the definition used by the Department of Defense (DOD), which defines non-lethal weapons as "weapon systems that are explicitly designed and primarily employed so as to incapacitate personnel or materiel, while minimizing fatalities, permanent injury to personnel, and undesired damage to property and the environment."

*Continued on Page 2*

# Military Plays Unique Role in Consequence Management

**By Peter Menk**
Military Support

For the U.S. military, Homeland Security during the Global War on Terrorism consists of two major missions: Homeland Defense, and Defense Support to Civil Authorities (DSCA). The first mission consists of traditional military duties and responsibilities such as land defense, missile defense, and the protection of critical infrastructure. The second mission, DSCA, includes interagency support for consequence-management duties that, under the National Response Plan (NRP), usually would be coordinated by the Federal Emergency Management Agency (FEMA) of the Department of Homeland Security (DHS).

In any discussion of the military's role in consequence-management missions, attention has most frequently focused on highly trained and fascinatingly equipped high-tech military units such as the 55 National Guard Civil Support Teams throughout the nation.

*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

**Business Office**

**Susan Collins**
Circulation Director
subscriptions@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***


## Hidden Dangers in the Use of Non-Lethal Technology

**Continued from Page 1**

It is important to note that the DOD policy does not require or expect non-lethal weapons "to have a zero probability of producing fatalities or permanent injuries." It postulates, rather, that non-lethal weapons are intended to significantly reduce the probability of such fatalities or injuries, when compared to the number of fatalities or injuries that result from the use of traditional military weapons, which achieve their effects through the physical destruction of targets.
Understanding this definition puts the police administrator in the position of knowing that non-lethal weapons could indeed injure and—under ever-changing, dynamic, and unpredictable circumstances—might even kill. A simple pencil, designed and used as a low-cost and reliable writing instrument, could be a deadly weapon in the hands of a violent and determined suspect.

**A Growing Arsenal of Difficult Choices**

It is with those cautions in mind that today's police administrator must evaluate the growing variety of non-lethal weapons now available. Most of those weapons fall into several distinct categories, including the following:

Chemical/Irritant Devices: Among these are chemical agents such as OC (Oleoresin Capsicum), CN (Chloracetophenon), and CS (Ochlorobenzylidene malonontrite). It is safe to say that these products have reduced injuries—to suspects as well as to police officers—more often, and more effectively, than any other "non-lethal" in the history of modern law enforcement. Such devices give the police officer the ability to use non-injuring force at a safe distance from the suspect. Manufacturers tout effective ranges to distances beyond twelve feet. Police officers know from experience, though, the distance where sprays are most frequently used—at three to five feet. But those three to five feet have prevented numerous injuries and saved many lives.

Blunt Trauma Instruments: These include both batons and extended-range "impact" weapons such as wood, rubber, foam, and beanbag types of rounds that can be fired from a variety of platforms. Batons have been used in law enforcement for centuries. They have changed considerably in appearance, though, from the traditional, and extremely reliable, length of hickory to today's high-tech expandable metal shafts.

Hybrids: These use projectiles that not only have a significant impact effect but also carry a chemical/irritant payload, and can be launched from a distance.

Conducted/Directed-Energy Weapons: Conducted-energy weapons generate an electrical pulse, within the device, that is transferred through a wire onto and against the skin or clothing of a remote subject, affecting the individual's central nervous system; the intended result, almost always achieved, ranges from pain compliance to complete incapacitation. These devices, which are specifically designed to work without causing serious and/or lasting injury, are rapidly changing the way that modern law-enforcement agencies deal with combative suspects and/or emotionally disturbed persons.

In addition to the preceding, there also are under development—by various government agencies as well as private industry—a number of other non-lethal weapons and devices that use various forms of sound energy, light energy, laser energy, heat, and microwave energy to achieve their effects.

*Continued on Page 3*

Many of these technologies were initially explored by branches of the U.S. military during the Cold War. Several of them have been taken off the shelf in recent years and are now being modified and refined for potential use by law-enforcement officials.

**Homework, Research, and Careful Evaluation**

All manufacturers want police departments to buy their products. The careful administrator will keep an open mind, but should also remember whose name is going to be on the litigation—which is one reason why the idea of independent evaluation is making its way into the vocabulary of the police administrator.

There are various safeguards to keep in mind before making a final choice: credible medical studies, for example, as well as accuracy studies and, most important of all, training programs all will be needed. After these have been reviewed and evaluated, the real homework starts. A few large departments are blessed with research and development bureaus with the equipment and staff needed to conduct a thorough in-house evaluation. Other departments look to the various government and university agencies that have equivalent resources and are willing to carry out similar evaluations.

The first and foremost of these agencies is the National Institute of Justice, the research and development arm of the Department of Justice, which for over a decade has been conducting behavioral research and physical science research on non-lethal weapons used by the military and in law enforcement. Publications on all types of non-lethal option testing are immediately available at the NIJ home page: www.opj.usdoj.gov/nij

Other excellent resources include The Justice Technology Information Network (JUSTNET) home page www.nlectc.org and The Justice Information Center (National Criminal Justice Reference Service) home page www.ncjrs.org. In addition, the Applied Research Laboratory at the Pennsylvania State University, designated as the Marine Corps Research University, has conducted extensive independent research on various non-lethal devices available both to law enforcement and the military. Its home page is www.arl.psu.edu

**Media Reports and Other Hidden Dangers**

The careful administrator must be able to distinguish scientific data from popular opinion—usually created through news outlets. The misleading media coverage of the recent tragic event involving a non-lethal device in Boston during last year's baseball playoffs serves as a prime example. Law-enforcement departments received media reports that the death of a young woman had been caused by a beanbag round. Other reports said it was a Pepperball® round, and still others reported the Taser® as the responsible tool. None of these reports were accurate.

More recently (16 January 2005), an article in The Boston Herald said that the energy of a Taser's® "50,000-volt jolt" is "nearly 25 times that of an electric chair." That statement is preposterous on its face, but those who read the article without doing further research do not know that. So the administrator must base his or her knowledge on solid research, not on media reports—or the manufacturer's brochures.

The determination of the best and/or most effective non-lethals will vary by departments. One question that must be kept in mind is whether the device can be carried by the front-line patrol officer. It has been proven many times over that departments putting non-lethals into the hands of specialty teams do not always realize the potential of the devices they have selected. A reduction of more than 70 percent of officer injuries is possible when the right non-lethal is in the patrol officer's hands—and the patrol officers are the ones responding to and stopping incidents from escalating to higher degrees of violence.

The cost of a specific device, which is often deceiving, is frequently far below the actual cost of deployment. So the administrator also must determine the cost of the appropriate end-user training, and annual re-training, and compare those figures to the long-term likely savings that will result from the reduction of officer injuries, suspect injuries, and averted liability costs.

## Military Plays Unique Role in Consequence Management

**Continued from page 1**

Each team consists of 22 highly skilled full-time National Guard members who are federally resourced, trained, and exercised—and who have been fully instructed in the federally approved CBRN (chemical, biological, radiological, or nuclear) response doctrine. The mission of these National Guard teams is to use their unique expertise and capabilities to assist state governors, within each state's own emergency-response structure, in preparing for and responding to CBRN incidents.

*Continued on Page 4*

**A Division of Capabilities, Resources, and Responsibilities**

As important as the technological capabilities of the Civil Support Teams—or of such other Department of Defense (DOD) resources as the Army's Technical Escort Units and the Marine Corps Chemical and Biological Incident Response Force—might be, the military has an even more important consequence-management role to play in the hours, days, and weeks immediately following a terrorist attack.

To understand that role one must first recognize that U.S. national policy is to assign the bulk of technological consequence-management capabilities, and responsibilities, to the civilian sector. In 1996, the Nunn-Lugar-Domenici Act provided the federal funding needed to equip and train responders in the nation's 120 largest cities. Since passage of that act, the number of such federally funded programs has expanded significantly, both in the scope of the responsibilities assigned, and in the financial resources provided. DHS now funds an immense federal assistance program to ensure that state and local emergency-management personnel nationwide receive the equipment and training they need to carry out all of the duties they have been assigned.

Experience has proven the worth of this national policy. As tragic and devastating as the collapse of the World Trade Center Towers was, New York City's civilian responders did not require any significant assistance from DOD in carrying out their consequence-management operations. DOD retained all its resources for other missions, both in Homeland Defense and for its operations overseas.

**A Catastrophe of Unprecedented Dimensions**

However, the consequences of the 11 September 2001 attacks were not as catastrophic as future attacks may be. A close analysis of the response in New York City suggests, in fact, that a truly catastrophic attack, such as a contagious bioterrorism event, could overwhelm current civilian capabilities.

The biggest vulnerability in the U.S. civilian disaster-response system as it is now structured is that it does not have the depth needed to sustain long-term relief operations. Civilian capabilities were stretched to the limit, and beyond, less than a year ago in the attempts to sustain operations during four consecutive hurricanes—Charley, Frances, Ivan, and Jeanne—that struck the United States during the 2004 Hurricane Season. The operations most affected were not high-tech missions, but long-term, sustained, labor-intensive missions.

Today, the U.S. military, joined with the National Guard in operations coordinated through the Emergency Mutual Assistance Compact (EMAC), is uniquely capable of filling the requirement for sustained labor-intensive operations during, and following, major disasters of any type affecting almost any state or region of the country. EMAC serves in effect as a treaty—between the states, and ratified by Congress—that gives all participating states the ability to expeditiously request and/or provide emergency assistance to one another. At present all states except California and Hawaii are members of EMAC.

Although much of the role for the military in providing long-term labor-intensive consequence-management assistance may appear mundane, it is absolutely essential. The military is the nation's only current quick-access source of large numbers of disciplined and healthy young men and women who are both well trained and adequately equipped for sustained performance in stressful conditions under a unified command-and-control structure that is already in place. There is no equivalent resource in the civilian community. Among the typical roles requiring large numbers of personnel is the provision of traffic controls—e.g., the denial of unauthorized entry into a disaster area or, in the event of quarantine operations, the denial of exit from that same area.

**Thirty Seconds Times Five Million People**

If there were, in fact, a contagious biological attack in a large metropolitan area, current plans call for a "Push Package" of drugs and medical equipment—sufficient to treat up to 365,000 people—to be quickly delivered from the Strategic National Stockpile, with follow-on additional drugs and medical equipment arriving within the next 24 to 36 hours. Highly detailed plans and exercises, combined with the assistance provided by a Center for Disease Control Technical Advisory Response Unit, have significantly improved the nation's capabilities for initial distribution when the mass dispensing of antibiotics might be required.

However, a likely requirement in any catastrophic event of this type would be to distribute packets of drugs, to perhaps millions of people, within 24 hours, and to sustain that level of distribution for some time thereafter. If one assumes that distribution to five million people is required, the process just to hand over and track each bag—taking just 30 seconds to help each person—would take 3,472 people, all of them working 12-hour shifts.

*Continued on Page 5*

Only the U.S. military could do this job, and do it efficiently. The reason is that the U.S. military already is structured and equipped to conduct sustained combat missions overseas. The military also, of course, has carried out many consequence-management missions during and after U.S. domestic disasters, whether natural or man-made. For domestic missions, the military relies upon the same structure, discipline, equipment, and leadership it uses for its combat missions.

In short, the U.S. military's combat structure—which provides command-and-control capabilities for large numbers of disciplined forces operating, over a very large geographic area, in a stress-filled environment—already has proven its utility in countless humanitarian and disaster assistance missions, both at home and overseas.

The transformation of the U.S. military in recent years has made it an even more flexible and effective force. The lessons learned from such post-Cold War missions as establishing order, and starting and supporting the nation-building process, in disrupted states such as Kosovo and Iraq also are being leveraged to enhance the military's domestic-operations capabilities. Again, there is no civilian organization—federal, state, local, or private: sector—capable of carrying out the same missions.

## The Great Melting Pot of Domestic Preparedness

**By Rob Schnepp**
Fire HAZMAT

No single entity or agency can fight the war on terrorism—or handle the aftermath of any single battle–alone. Those tasked with response or recovery duties, at least the forward-thinking ones, understand that and embrace certain fundamental truths about U.S. domestic-preparedness policies and programs today, and for the foreseeable future—namely, that boundaries in and between agencies must be dropped; that operations exclusive to individual "kingdoms" or fiefdoms are no longer the most effective way to combat terrorism; and that, no matter what their history, all of the nation's preparedness agencies must be willing to share their own information, talents, and training with all other offices and agencies working in the same field.

This is the nature of the beast that is now driving the preparedness professionals, military as well as civilian–in the nation's entire domestic-preparedness/counterterrorism field—who are making the extra effort to reach across traditional boundaries and work with their counterparts in other agencies in not only traditional but also some nontraditional ways.

It might help, to more fully grasp what has happened over the past several years, to think of domestic preparedness as a giant kettle filled to the brim with varying-sized chunks of several different kinds of meat, as well as a dozen or so types of vegetables. The domestic-preparedness "kettle," perched above a roaring fire called terrorism, is filled with varying talents, skills, and fields of experience—in police work, firefighting, emergency medicine, matters related to public health, and other specialty areas. All are part of the nation's overall domestic-preparedness/military-response network.

**Numbers, Variables, and Fiefdoms**

Among the key players in that network are the 188,000 military and civilian employees of the U.S. Department of Homeland Security (DHS). But there are numerous other local, state, and federal agencies, as well as a number of private-sector organizations, also working in the fields of domestic preparedness and counterterrorism. These days, the heat generated just by the threat of terrorism will start the cooking process. Each ingredient would have different ideal cooking times and temperatures, of course, but with the proper care and attention, and sufficient cooking time, the resulting mixture would be as hot and fluid as the fire below. The kettle analogy may seem at first glance to be a bit forced, but it should be remembered that the United States, as a nation, frequently has been described as a vast "melting pot" of people of every race, nationality, religion, and cultural background from all over the world.

As with the nation, the melting pot of "ingredients" in the domestic-preparedness field includes numerous variables, including the prevailing political and financial climate as well as the internal cultures and perspectives of many different professions. If all goes well, though, previous fiefdom boundaries and attitudes will give way to a spirit of mutual trust and cooperation, and the end result will be an interrelated and truly interoperable system. Unfortunately, such a state of utopian preparedness cannot and will not happen overnight, or in the near future. There even is a distinct possibility that it may never happen, but that seems unlikely, given the mood of the American people and the seeming determination—in the fields of counterterrorism and domestic preparedness, if nowhere else—of most of the nation's political and military leaders to work together to make the nation, and the world, safer and more secure.

*Continued on Page 6*

There are some major obstacles to hurdle. Changes are required in certain federal regulations, the numerous political and cultural differences between and even within various professional disciplines will have to be reconciled, the vendor market has to be brought into the picture more completely, and a number of intangibles will undoubtedly crop up that also will affect the way that business gets done and relationships are forged.

Overall, the financial climate for domestic preparedness is improving, but not evenly and at the same pace for all first responders and/or for the other agencies involved. Most of the nation's hospitals, for example, are behind local police and fire departments in the amount of federal funding they already have received, and/or can expect to receive in the future. This disparity is a matter of considerable concern to hospital administrators.

Frank Califano, safety coordinator and network emergency manager for the North Shore Health System of Long Island, N.Y., commented as follows on the subject of hospital preparedness: "The hospital sector does not have [the same] access to federal funds that other responders do, but I think that is changing. Also, some hospitals work with public-sector responders in terms of personal protective equipment, respiratory protection, and decontamination, but that is not the case industry-wide, especially with smaller hospitals—many of which, it seems, are not sure what type of hazmat [hazardous materials] training is most effective, for example, or how to handle contaminated patients.

"But that, too, may be changing. In December of 2004, OSHA [the Occupational Safety and Health Administration] issued a 'guidelines' report [Best Practices for Hospital-Based First Receivers] that I think will help hospitals across the country understand what they need to do to handle contaminated patients."

First Receivers is a relatively new term in domestic preparedness and should not be confused with first responders. Historically, first responders are firemen and policemen—i.e., those men and women who throughout the nation's history have been called upon to work at the scene of an incident. First receivers, on the other hand, include doctors, nurses, clinicians, emergency services personnel, and other medical people charged with treating contaminated patients in facilities (hospitals, usually) and at distances away from the incident scene.

**Attitudinal and Other Problems**

Califano and other hospital professionals consistently mention a number of problems that must be overcome before major improvements in hospital preparedness can be achieved. Some hospitals are apathetic about preparedness in general, for example, and do very little training or planning. Others adopt the philosophy that the local fire department will take care of the victim-decontamination problem. Even when there are no "attitude" problems, there still may be a number of harmful misconceptions about the precise levels of hazmat training that are needed and the appropriate types and amounts of respiratory protection that should be available in the hospital setting.

"Before the OSHA Best Practices document was issued," Califano says, "federal regulations provided guidance for hazmat training. Those regulations [spelled out in the Code of Federal Regulations Title 29, section 1910.120 subpart (q)] are based on what is best for industry and public safety, not what is best for the hospitals."

For the most part, however, Califano said, the hospital community is improving overall, in terms of fitting into the big picture. "It is getting better, but even in hospitals with proper training and equipment there is still an issue with staffing. In a lot of places, an emergency department does not have enough staff both to do decon and provide care–they have to choose, and that creates an obvious problem. We learned a lot from the Tokyo subway incident and the World Trade Center.

"In Tokyo," he continued, "over 5,000 people went to hospitals–90 percent of them bypassed the first responders. The World Trade Center had the same profile. The downtown New York hospitals saw walk-ins well before the 9/11 patients started to arrive. Hospitals just cannot rely on the traditional method of receiving patients anymore."

It is this fact, Califano and others have suggested, that should drive hospitals and public-sector responders to work together and understand each other's strengths and limitations. A concept applicable to all members of the domestic preparedness community is to understand how their own agencies fit in, locally and regionally, and how they can contribute most effectively. Much of this, of course, is simply human nature: It is the relationships made *before* disaster strikes that will help the entire process work efficiently.

In that context, Frank Califano offers a basic but important bit of advice, germane to all players in the domestic-preparedness arena: "We should not be competitors–everyone must work together."

## Interview with Raytheon Vice President for Homeland Security Hugo Poza 24 January 2005

**By John F. Morton**
Interviews

John F. Morton: DomPrep.com is talking with Hugo Poza, vice president of Raytheon's Homeland Security business, a position he has held since June 2002.

The company's major programs, products, and initiatives under Poza's jurisdiction include Biometrics Identification, Cyber Security, Incident Command System, Explosives Detection, and Data Mining/Warehousing/Analysis/ Correlation. Previously, Mr. Poza was vice president and general manager of Strategic Systems in Raytheon's Command, Control, Communication, and Information Systems (C3I) business.

**JFM:** Mr. Poza, welcome to DomPrep.

**Hugo Poza:** Glad to be here and talking to you.

**JFM:** As the nation's fifth largest defense contractor, Raytheon is now in the homeland security business. How big an adjustment has that been for the company?

**HP:** Right after 9/11 we put together some of our best engineering talent to see how we could bring to bear our technologies, and the products we have in the defense industry, to play in the homeland-security arena. A lot of taxpayer money has already been paid for the technologies, and the products developed for our defense customers are now applicable in a different arena.

**JFM:** Now, have you got some specific examples, like what you do via JPS Communications? [Raytheon acquired JPS Communications in December 2002. http://www.jps.com/]

**HP:** Yes, you know communications interoperability, which was the basic reason for our buying JPS, is now not only a very important part of homeland security, but it's also becoming a very important part of the transformation of the military, so that the services are able to talk to each other. There's a particular example in the case of JPS. There are many others. I'll share with you the example of Red Wolf, a product line that we've had for a while. It's a telecommunications intercept. Two or three years ago, the idea was to use it to intercept drug communications and to be able to use it to convict. Well, gee, we thought, why can't you use that to intercept terrorist communication and convict?

**JFM:** Your procurements were with what department?

**HP:** Department of Justice. Can it be used by DHS [Department of Homeland Security] for grabbing and convicting terrorists? Absolutely. Now, it has to be geared toward a different type of environment, but the gearing is on the order of "ten percent" rather than starting from scratch. There's a lot that already comes from the defense and the intelligence world that can be used now, and all it needs is a little tweaking.

**JFM:** What division in Raytheon is doing the tweaking? I mean, how are you organized for homeland security?

**HP:** What we did in putting homeland security together was to designate it as a strategic business area, which I manage for the entire company. I do not have specialist engineers. I do not have specialist technology. But I do have perhaps the sharpest talent in my operational systems engineers. We add value by taking the products of the company and other companies and putting them together to give our customers the best solutions to their problems. So we are really mission systems integrators in the total sense of the word.

**JFM:** Now, if I am a law enforcement, fire and rescue, or emergency management procurement official, where is my point of contact at Raytheon?

**HP:** Your contact is here at Raytheon Homeland Security. Tom Hudson, our director of homeland security [Thomas_C_Hudson@Raytheon.com], will take you ultimately to the businesses—the engineers that design and produce the product that will be part of your solution. Raytheon Homeland Security combines all the products in the company.

Homeland Security does not sell products. We sell solutions. It is my responsibility to go into the rest of the company and get all the businesses to work together. In many of the programs, we are working three, four, five different businesses of Raytheon, in addition to working with other people and companies that provide things that Raytheon can't provide.

**JFM:** You talked about radio communications interoperability. What other kinds of homeland-security market segments are you focusing on?

*Continued on Page 8*

**HP:** The first segment parallels the Department of Homeland Security Information Analysis and Infrastructure Protection. We provide intelligence, cyber-security, things of that nature. So, for example, we are a member of the Northrop Grumman team for the Homeland Secure Data Network [HSDN]. We won HSDN with Northrop Grumman, and we provide Northrop Grumman with network security.

We do border security, transportation security, high-value-facility security, and access management. So, we are a team member of the Accenture team [http://www.raytheon.com/feature/static/node3543.html] for US-VISIT [United States Visitor and Immigrant Status Indicator Technology] and provide expertise in systems engineering, in biometrics, systems architecture, and deployment areas. And we are doing border security outside this country.

In the emergency-response arena, we have the first award of our incident command system [ICS] to be used by fire departments and police departments, and you are going to see a lot more of what we call e.ICS(tm) to provide hand-held equipment to communicate not only through satellites but also to the core of the building, basements, etc., etc.

**JFM:** When will that be announced?

**HP:** Launch customer should be announced within the next month.

**JFM:** What else?

**HP:** We also have tied to e.ICS(tm) another initiative called the Emergency Patient Tracking System [EPTS], which allows authorities to keep track of all the people who are hurt during a disaster, where people have gone, what hospitals, what the maladies are, their situation, and so on.

**JFM:** What about syndromic surveillance?

**HP:** The Emergency Patient Tracking System is actually being used in the City of St. Louis, where all 36 hospitals can communicate part of the syndromic status to start putting data together. EPTS is being used among the hospitals to keep the data going. And it's being tried out in the State of Michigan and other localities. It's being used right now as a test method for containment.

**JFM:** In the homeland-security market, you indicated that your customers at the moment are primarily in DHS, but with e.ICS(tm) and EPTS you're dealing with local law enforcement and hospital administration.

**HP:** I would say now that 90 percent of our customers are federal-level. I think that with the launch awards starting now at the local, city, and state levels, in the next year you'll see a tremendous growth in awards from big city fire departments, police departments, and state police departments. These are for equipment that allows them to communicate with each other and maintain a rational communications command scenario, as well as use intelligence to tell them about scenarios of criminals and terrorists. We have some competitions going on right now for equipment to enable state police to intercept communications and use intelligence on the people that they are going after.

**JFM:** What do you have to say about how Raytheon is addressing standards across all these different jurisdictions?

**HP:** You know, that is a very, very important issue. The City of New York has conditions of contracts that are different from those of the City of St. Louis. Trust me, we are just starting, but the way we are handling it right now is to define a product or system or solution that is standard, and then, to satisfy the particularities, we will modify, we will integrate differently. We bring 90 percent of a solution as a standard piece—with a standard price—and then we focus on the ten percent that needs to be modified to satisfy the particularities—which will have an extra price.

**JFM:** How are you rising to the challenge of developing relationships with 20,000 different procurement authorities nationwide?

**HP:** First and foremost, we are not trying to go after all 20,000. We are trying to look at the market leaders: New York, Boston, Los Angeles, Washington, Atlanta, Miami, Phoenix, Chicago. Those are the ones that the rest will look up to. To do that, we are leveraging the established relationships that JPS already has. We are using their example, their personnel, their knowledge.

**JFM:** Finally, I should ask what are you doing about the international homeland-security market?

**HP:** Our attention is focused principally on the areas of border security and access management. You know, the U.S. government is coming out with a program called America's Shield, which really refers to northern and southern borders with Canada and Mexico. In addition to that we have the US-VISIT program, which controls the access of visitors in and out of the country. We want to know when they come in and when they go out, and that's the information that US-VISIT will give us over a ten-year period.

*Continued on Page 9*

Well, the U.K. wants to have a U.K. e-Borders, which would be the English version of US-VISIT. Japan wants to have what they call Japan VISIT. Guess what? It's their version of US-VISIT. Same thing for China—the People's Republic. Countries in the Middle East—you can imagine how important border control is to them. So this is an international market. Absolutely, Positively.

**JFM:** Mr Poza, thanks very much for your time. I know that our T.I.P.S. readers will find your answers very interesting.

## Business Continuity Planning Standards: A Search for Normalcy

**By Ashley Paul Moore**
Standards Channel Master

*Acceptance of prevailing standards often means we have no standards of our own.*
*~ Jean Toomer (1894 - 1967) U.S. author, poet*

What is a standard? More specifically, what is a Business Continuity (BC) standard? In general, standards provide preparedness models that private-sector organizations can use when they want to establish their own "internal" organizational standards. In most cases, they are voluntary; this precludes the need, usually, for "regulatory" standards.

Most current process-oriented preparedness standards—such as the one prescribed for Business Continuity and Contingency Planning (BCCP)—are voluntary (unless they have been internalized by the corporate head). However, most "life safety codes"—i.e., fire and building codes—are deemed as regulatory standards. It is possible that some all-encompassing regulatory standard could be developed for buildings that serve as business headquarters, where people are employed who produce some viable output. But creating regulatory mandates for businesses might well pressure insurance companies, real estate owners, and the banking industry to become more directly involved in a BCCP balanced investment.

Because business interruptions range from catastrophic natural disasters like the January 2005 tsunami, acts of terrorism (e.g., the attacks on the World Trade Center), or technological malfunctions such as the 14 August 2003 Great Northeast Power Blackout, businesses providing services must have a broader view and understanding of BC standards. Sequentially, the services that they either support or produce must be recoverable within a short but narrow spectrum of time so as not to worsen the economic loss. Hence, BCCP standard developers could have used this momentum to force the development of a regulatory standard. However, U.S. history shows that legislative and/or regulatory changes are mandated only when the country is faced with, or has experienced, a major catastrophe—the attacks on the World Trade Center, and the Pentagon, for example. Fortunately, a National Fire Protection Association (NFPA) standard (NFPA 1600: Emergency Preparedness and Business Continuity) was already in place.

NFPA 1600 leads off with a strong and clear assertion: NFPA has no power, nor does it undertake, to police or enforce compliance with the contents of this document. Nor does the NFPA list, certify, test, or inspect products, designs, or installations for compliance with this document. Any certification or other statement of compliance with the requirements of this document shall not be attributable to the NFPA and is solely the responsibility of the certifier or maker of the statement.

Nonetheless, an interesting twist occurred in late April of last year at a Homeland Security Standards Panel meeting of the American National Standards Institute (ANSI). During that meeting, a recommendation was made that the "federal government" adopt standards consistent with NFPA 1600. Left unanswered was the important question of what department or agency was qualified to or would develop staff, establish policy, and manage a Business Continuity/Disaster Recovery Planning and Management program or process. Some agency or component of the U.S. Department of Homeland Security (DHS) seemed the most likely answer, and would be consistent with a Brookings Institution recommendation, in August 2004, that the DHS have an under secretary for policy. Creating a standard might well become one of the top ten items on that official's working agenda.

The need for workable standards also was addressed in the final report of the 9/11 Commission, which recommended that ANSI develop a "National Standard for Preparedness" for private-sector businesses to consider in making their own plans for emergency preparedness and its potential effects on business continuity. In response, ANSI assembled subject matter experts from the safety, security, and business continuity professions, as well as from industries and associations, and federal, state, and local government communities of interest.

*Continued on Page 10*

This extraordinary gathering of minds resulted in ANSI's recommendation that the Commission endorse the existing American National Standard on Disaster/Emergency Management and Business Continuity Programs—i.e., NFPA 1600—as strictly "voluntary." Embedded in the Commission's report was the following comment: "Private-sector preparedness is not a luxury; it is a cost of doing business in the post-9/11 world. It is ignored at a tremendous potential cost in lives, money, and national security."

**The Art of War and Business Continuity**

A number of forward-thinking public as well as private-sector agencies and organizations take very seriously the need for development, program implementation, and compliance oversight of Business Continuity "regulatory" standards.

In particular, the following have tackled the challenge with determination: the Department of Treasury, the Internal Revenue Service, the New York Stock Exchange, the National Association of Securities Dealers (NASD), and the International Standards Organization. Following are capsule summaries of what some of them have done:

Department of the Treasury: In December 2004, the department produced a report on "Improving Business Continuity in the Financial Services Sector." The report, ChicagoFIRST, which was conducted in Chicago, focused on a select regional coalition of financial institutions and local government organizations in that city. According to its mission statement, this collaborative effort came together to strengthen Chicago's financial services sectors and establish the framework to coordinate with local, state, and federal government agencies in the event of a potential natural or manmade crisis.

ChicagoFIRST also defined certain prerequisites for success, and provided this motivating conclusion: "By following the steps to adapt and apply the model, similarly healthy, robust communities can evolve elsewhere. These communities will strengthen the resiliency of the financial services industry as a whole."

The Treasury report is available at http://www.treas.gov/press/releases/reports/chicagofirst_handbook.pdf

New York Stock Exchange: In a memo dated 3 May 2004, the New York Stock Exchange distributed Rule NYSE 446 Business Continuity Plans to all members and member organizations. The rule states, among its general requirements, that members and member organizations "must" establish and maintain Business Continuity Plans (BCPs) relating to an emergency or significant business disruption. Rule 446(a) also requires that a member's or member organization's BCP be reasonably designed to enable it to meet existing obligations to customers, and address existing relationships with other broker-dealers and counter-parties.

The rule also provides the necessary framework for BCPs, which include but are not limited to the following:

- Annual Review of BCPs
- Minimum Requirements of a BCP
- Mission-Critical Systems and Back-Up for Such Systems
- Critical Constituent, Bank, and Counter-Party Impact
- Data Back-Up and Recovery (Hard Copy and Electronic)
- Prompt Access to Funds
- Disclosure Provisions
- Corporate-Wide BCPs
- Financial and Operational Risk Assessments
- Emergency Contact Information
- Implementation Dates

The NYSE rule is available at http://www.sec.gov/rules/sro/34-46443.htm

National Association of Securities Dealers: In April 2004, the association provided its members the rulings NASD 3510, "Business Continuity Plans," and NASD 3520, "Emergency Contacts." NASD members now are required to establish emergency preparedness plans and procedures. Rule 3510 requires each member to create and maintain a business continuity plan and enumerates certain requirements that each plan must address. The rule further requires members to update their business continuity plans upon any material change and, at a minimum, to conduct an annual review of their plans. Each member also must disclose to its customers how its business continuity plan addresses the possibility of a future significant business disruption and how the member plans to respond to events of varying scope. Rule 3520 requires members to designate two emergency contact persons and to provide this information to NASD electronically.

The NASD rules are available at http://www.nasdr.com/business_continuity_planning.asp.

*Continued on Page 11*

**The International Connection**

It should be obvious that attaching a regulatory standard to something that is internationally understood changes the entire perspective of the conversation and the outcome—as, for example, when money and information technology are connected within the global economic mainframe.

A good example is ISO/IEC 17799, a Code of Practice for Information Security Management issued by the International Standards Organization (ISO) and the International Electrotechnical Commission (IEC). This new international standard postulates how businesses should conduct the management of their information security requirements. The document is copyrighted by BSI and ISO/IEC. ISO 17799 primarily covers the platforms for IT security and Business Continuity Management; the U.S. position is strongly in favor of a major revision of the document that is currently underway. Business Continuity and Contingency Planning standards (BCCPs) play a major role in ISO 17799.

IT disruptions and BCCP processes will be applied to a business continuity management audit to cohesively incorporate, in a top-down manner, the continuity requirements of critical business processes and ensure that they and the resources that support them are available when a catastrophic event occurs.

A comparison of NYSE Rule 446; SOX, BASEL II, and ISO 17799 shows the different approaches taken by different organizations to encourage and ensure business continuity.

Rule 446 is all about corporate image; it demands that its members on the NYSE have viable and functional BCCPs. Its predecessor, Disaster Recovery Planning, was a primitive form of BC planning that derived from the Y2K period—which, in turn, focused primarily on the potential failure of technology. But the most viable Business Continuity standards are built on the full continuum of business processes, people, resources, communications, and other variables.

Sarbanes-Oxley (SOX), which applies to all public corporations in America, and Basel II, which pertains to financial institutions in more than 100 countries, will go into effect in 2006. Because all top 20 U.S. banks or financial institutions with locations in the European Union must accept SOX & BASEL II, their U.S. clients are affected as well by these rules. This creates a situation that ties back into Rule 446–which, along with Sox and Basel II—demands BCP/DRP/Operational Risk Management, in accordance with the ISO 17799 (BS 7799) standard, on a worldwide scale. This standard is available at http://www.iso.ch/iso/en/

A final point—about Homeland Security Presidential Directive # XX—National Business Continuity and Contingency Preparedness Planning—also might be relevant: Andy Rooney, a CBS commentator, once stated, "Don't rule out working with your hands. It does not preclude using your head." In a global economy, it may be time for the United States to change its position and accept what the rest of the world is no longer taking for granted. In the cornucopia of plausible disasters and the new age of transnational terrorism, horrible events are going to happen and they will likely have local, regional, and/or even international economic implications. Which means that the time may have come to establish a National Regulatory Standard for Business Continuity and Contingency Planning.

# Chemical & Biological Detection

## Featuring Flame Spectro-photometry Detection:

- All G Agents (GA, GB, GD, GF, GE, etc.)
- All V Agents (VX, VE, VG, VS, VN, etc.)
- HD Agents
- Homemade Agents (terrorist)
- Vapor, Aerosol, Liquid & Blister Forms
- High Sensitivity
- Fast Response Time at Best Sensitivity (2s for 1,5 ppb)
- Start-Up Under 20 seconds
- Fast Recovery Time
- Simultaneous Detection
- Rough Condition Performance
- No Shelf Cost

### AP2C Handheld Portable Alarm Detector

Unique All Surface Liquid Handheld Detector (example VX)
Detects: blister forms, precursors of chemical warfare
Detects on: skin, blood, urine, sweat (exclusive medical application)

### Applications Include:

Control of contaminated and decontaminated areas,
Chemical disarmament, water contamination control,
Medical sorting of casualities

### APACC Alarm Monitoring Agent Dose Meter Detector

Agent Dose Meter
Remote Control
Software
Sound and Visual Alarm
Network Capabilities
Remote Control & Display up to 1km

### Applications Include:

Advanced NBC teams
Security perimeter monitoring systems
CW weapons storage area, etc.

# PROENGIN

The Protection of Detection

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

Please see the SBCCOM Report at:
http:/hld.sbccom.army.mil/ip/reports.html#detectors.com