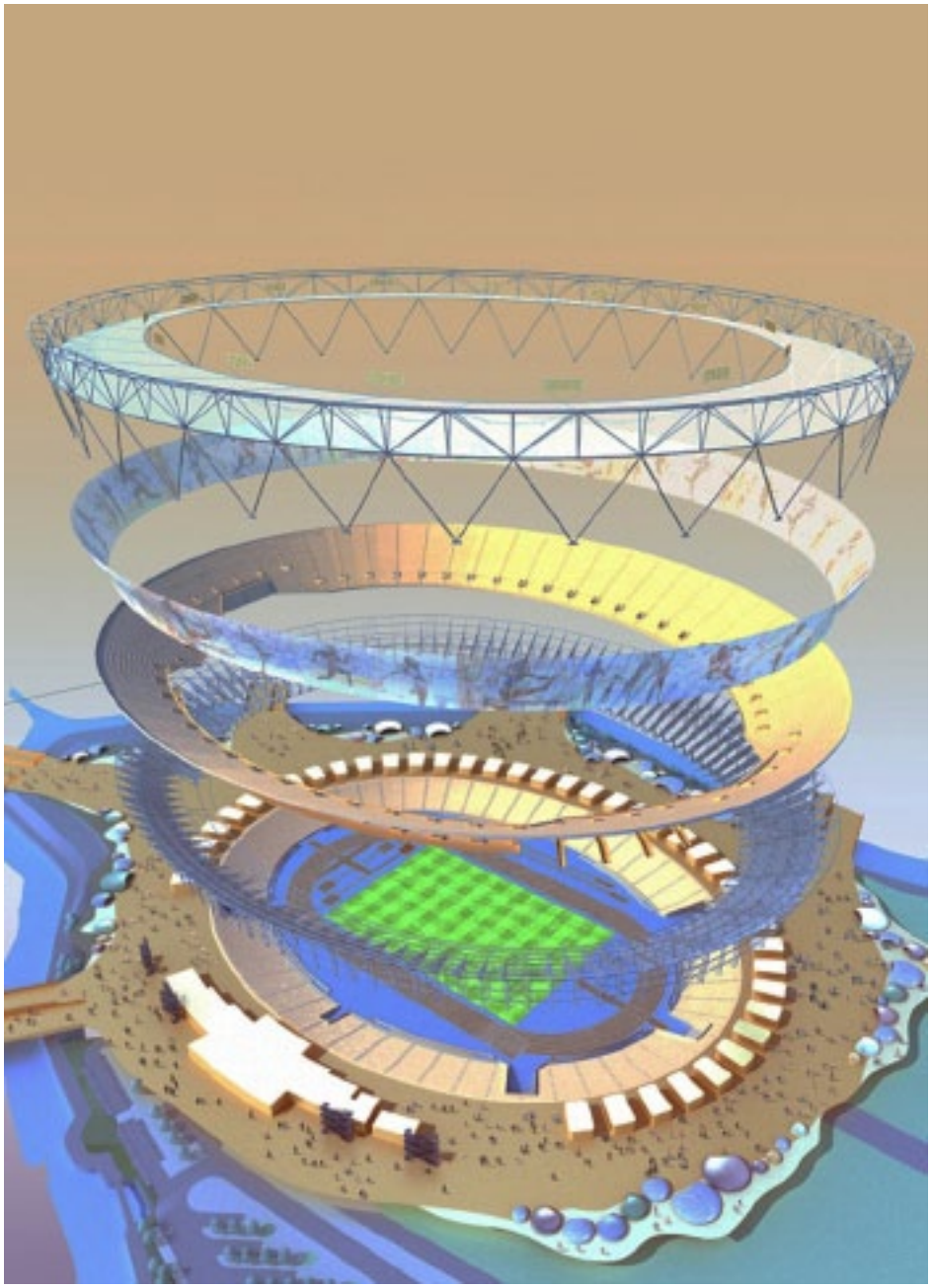
DomPrep Journal

US Annual $100 Volume 5 Issue 7, July 2009

Special Event Security

Defending Against CBRNE



Raider™

RAPID IDENTIFICATION AND VERIFICATION OF RADIOACTIVE MATERIALS

The covert movement of dangerous, radioactive materials is a serious security threat, The Raider™, a unique handheld radiation detection and identification device, advances the capabilities of personal radiation detection instrumentation.

Using innovative technology, the Raider records, displays and analyzes spectral information in real time, for fast and accurate identification of radioactive materials. After a detection, GPS coordinates, the spectra, identification results, picture and an audio description of the incident can be communicated back to a central command center via its reach-back capability.

Performance meets practicality.

www.icxt.com/detection

NEW THREATS.
NEW THINKING.®

icx™ technologies

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

Staff

Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Tammy Workman
National Sales Director
tworkman@domprep.com

Dan Brethauer
Account Executive
dbrethauer@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

Bruker Detection

GEOMET Technologies LLC

ICx Technologies

Idaho Technology Inc.

MSA

Penn State University

PROENGIN Inc.

Remploy Frontline

DomPrep Journal is electronically delivered by the IMR Group, Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; fax: 410-518-6020; also available at www.DomPrep.com

Articles are written by professional practitioners in homeland security, domestic preparedness, and related fields. Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher. Text is the opinion of the author; publisher holds no liability for its use or interpretation.

IMR GROUP

Editor's Notes

By James D. Hessman, Editor in Chief

All-Star games, the Super Bowl, presidential inaugurations, the Republican and Democratic national conventions, the Summer and Winter Olympics, Fourth of July celebrations, and a host of similar events have one thing in common: All of them are terrorist attacks waiting to happen.

That is the grim reality of life (and death) in the 21st century – which, no matter what politicians want to call it, will be remembered, for a very long time to come, by sports fans and other citizens as the Age of Terrorism. Terrorists want to kill Americans – Brits, Germans, Israelis, and other innocent people as well. They also want to strike fear into millions of others who do not share their own warped beliefs. They can achieve both of these goals by carrying out attacks on well attended political and entertainment events such as those mentioned above.

As the articles in this month's printable issue of *DPJ* point out, the primary duty of U.S. emergency managers, and their counterparts in other countries, is to prevent such attacks from happening. They also must be prepared, though, when (not if) prevention fails, to deal with the aftermath of a successful attack, or series of attacks. Exactly how they do that, and how well they do it, are the major unanswered questions that may determine the fate of perhaps tens of thousands of their fellow citizens.

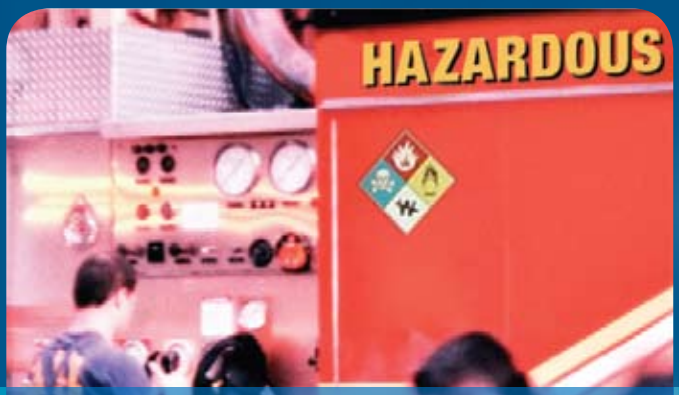
Andy Oppenheimer leads off this month's all-star cast of writers with an insider's report on the preparations being made by the City of London to deal with potential disruptions of the 2012 Summer Olympics. Dr. Neil Livingstone, an internationally known expert in the fields of terrorism and homeland security, follows up with an illuminating discussion of the post-9/11 steps taken by the U.S. government to thwart similar attacks in the future. Kay Goss then provides a much needed tutorial of the official publications, "how-to" guides, and other information readily available to help emergency planners and first responders develop and implement their own plans and preparations at the state and local levels of government.

Dennis Schrader continues the march by pointing out that federal funds are available for much of the training needed to hone the skills of responders and other working professionals. Joseph Trindal and Joseph Watson team up to examine how state and local governments can use federal planning templates to protect their own communities not only at lower cost but also much more effectively. Diana Hopkins uses two examples – the 2001 Super Bowl in Tampa, and the 2009 Super Bowl in that same city – to show how security planning for such National Special Security Events (NSSEs) has escalated from an administrative afterthought to the single most important factor in the overall NSSE planning process. (She also provides a thought-provoking article on the potential use of a global immediate-alert communications network to warn of tsunamis, typhoons, earthquakes, and other potentially devastating weather disasters.)

Rounding out the issue are articles by: (a) Joseph Cahill, who discusses several ways in which local emergency managers can use real-life events (such as the Boston Marathon) as training opportunities for healthcare and other professionals; (b) John Burke, who points out the importance, even in training operations, of protecting the patient-privacy rights of participants; and (c) Adam McLaughlin, who provides his usual interesting mix of preparedness milestones recently achieved in (this month) Kansas, Kentucky, Washington (D.C.), and Wisconsin.

About the Cover: Computer-generated image shows the different sections of the Olympic Stadium design that will be created for the London 2012 Olympic & Paralympic Games. See Andy Oppenheimer's article, beginning on page 5, for additional information about the 2012 Games and the security preparations now in the planning stages. Photo compliments of the official site of the London 2012 Olympic & Paralympic Games (http://www.london2012.com).

Bruker Detection Corporation



Early Detection is the First Step in Protection

E²M
GC/MS System

- Identifies and quantifies organic substance in soil, air, water and from surfaces
- Mobile, compact, fast and reliable
- Software includes all standard MS acquisition methods
- Use internally purified air as carrier gas – no helium, hydrogen, or nitrogen required

HAWK FR
Stand Off Detection

- Detects chemical vapors up to one mile line of sight
- Detects CWAs and many industrial chemicals
- Scan large areas in seconds
- Stand-alone or can be integrated into a network

M-IR
Mobile FT-IR

- Wear-free ROCKSOLID™ interferometer for industry leading performance and reliability in harsh environments
- Rugged, portable, self contained solids and liquids analyzer
- Bearing mechanism is space qualified and virtually free from wear
- Easy-to-use graphical user interface; assistant guided operation

(978) 663-3660 x1308 ▪ nbc-sales@bdal.com ▪ www.bruker.com/detection

think forward

CBRN Detection

London 2012: Protecting the Olympic Games

By Andy Oppenheimer, Special Events

With planning and construction for the London 2012 Olympic Games now well under way, measures to counter terrorist attacks are being factored into all preparations to protect the millions of visiting spectators, the Olympic Village inhabitants, Games officials, and the travelling public during the world's most high-profile sporting event.

Since the terrorist atrocities at the 1972 Munich Olympics, in which 11 Israeli athletes and one police officer were killed by Palestinian terrorists, all major sporting events attracting large numbers of people have been regarded as high-level terrorist targets requiring attendant increases in security measures and police presence. The most relevant terrorist outrage in the United Kingdom providing lessons for future events involving crowded situations was the 7 July 2005 bombings of the London transit system, in which 53 people died, and over 700 were injured, in four simultaneous attacks.

That this, the worst terrorist attack on British territory, took place the day after the capital celebrated winning the 2012 bid for the Olympics served, sadly, to emphasize the security challenges that lay ahead.

Other tragic *non*-terrorist events have provided lessons to be learned in how to steward spectator crowds, house them safely, and manage crowd incidents. Britain's worst sporting disaster – the crushing to death of 96 Liverpool Football Club supporters at the Hillsborough soccer stadium on 15 April 1989 – resulted in new multimillion-pound safety measures: all-seater stadia throughout Britain; and stricter controls on crowds entering the venues.

The latter measure was needed to prevent a repeat of the appalling event, which occurred when local police allowed too many Liverpool fans into the back of an already full stand. But even with all-seater stadia, should a terrorist incident – a chemical release, for example – occur, the stampede effect might still prove lethal.

The 2012 CBRNE Threat to London

The most likely threats security chiefs are preparing for at the London 2012 Olympic Games are improvised chemical devices (ICDs), the dispersal of chemical or biological agents, and radiological dispersal devices (RDDs) – as well as the more prevalent terrorist means of mayhem: suicide bombers carrying explosives, vehicle-borne IEDs (improvised explosive devices), and either airborne or mortar attacks (or both). Managers of military support units for first-responder services as well as emergency services and other security personnel are putting measures into place for London 2012, including detection, protection, and surveillance systems and exercises.

Several other terrorist scares have occurred in England in recent years – e.g., the feared targeting in 2004 of the Old Trafford soccer stadium in Manchester. The attempted car bomb attacks in London in June 2007 resulted in enhanced readiness against the possible targeting of events taking place simultaneously, such as the Wimbledon Tennis

championships. The authorities also have to factor in threats from environmental protest groups and organized crime.

Likely scenarios will be outlined to examine how an incident would unfold, working through realistic casualty rates and how to deal with casualties; how first-responders are briefed and trained up for such events; how to manage responses to a CBRNE (chemical, biological, radiological, nuclear, explosives) event, including evacuation measures, the decontamination of persons and locations, forensics and monitoring; the role of the media in covering an incident at such well publicized events; and how much the public should be told in advance of the event about the countermeasures in place – and how they would be informed during the unfolding of an attack.

The Protection of Spectators

To counter CBR threats, fast detection and identification of the toxic materials released is required. Decisions on medical attendance and decontamination procedures would have to be made speedily to ensure that casualties are treated and panic is avoided. Spectators should be unaware, in fact, that detection equipment has been deployed so as to avoid unnecessary anxiety. Therefore, a CBRN security plan should work in the background, so that visitors are able to enjoy the event without disturbance or alarm. The most difficult challenge, probably, is achieving a balance between security concerns and ensuring that spectators can enjoy a friendly and open atmosphere – in contrast to the rigid controls applied at the 2008 Beijing Olympics.

The London 2012 security operation is expected to be the largest ever in peacetime Britain. With security costs estimated at £838 million, it was reported as early as September 2008 that the overall Olympics budget is expected to exceed £10 billion – after the government had promised a maximum of £9.3 billion – because officials had "vastly underestimated" the cost of protecting the event from terrorism. However, the original £600 million figure was based on the costs of the 2000 Sydney Olympics, *before* the 9/11 2001 attacks against the United States and the 2005 London bombings.

Landline and mobile telephone communications were near impossible during the first two hours after the attacks; 45,000 calls came into the police Casualty Bureau phone line alone, and there was little information available from the incident scenes

The British Army will be drafted in as civil support to help protect the thousands of athletes and hundreds of thousands of spectators from an atrocity. Military helicopters as well as unmanned military air platforms – such as those used to monitor and sometimes attack the Taliban in Afghanistan – will patrol overhead, and jets will be on standby to intercept any suspect private plane heading for the main Olympic stadium in Stratford, east London. A database of aerial photographs, maps, and 3D views of all Olympic venues will incorporate new technology that enables 3D images to be spun through an arc of 360 degrees – pinpointing exits, meeting points, and fire hydrants, and allowing the simulation of major incident scenarios.

In addition to police from Scotland Yard and other forces, tens of thousands of volunteers will be drafted in to check the bags and tickets of incoming spectators. This will require the vetting on a large scale of some 200,000 people working at various venues. Blast mitigation to minimize the effect of bomb explosions is a vital aspect of the ongoing construction of the stadia and other prime buildings, which will incorporate blast-proof material and shatter-proof glass. Some events also will be staged in other areas of London – bike races, free-running, abseiling, kayaking, and mountain biking over a 50-km. course – and officials want the 2012 experience to be extended to street parties similar to those held in Sydney at the turn of the millennium.

Learning from London 7/7

The London transport network is expected to carry 240,000 passengers an hour during the Games. Extra officers will be needed to identify suspected bombers. Security preparations will be augmented by the lessons learned not only from the successful July 2005 attacks but also from the *attempted* attacks later that month. Here it should be noted that by no means did these lessons detract from the many acts of bravery by the emergency services, voluntary organizations, and members of the public during and after the attacks. Nevertheless, shortcomings of preparation, response, and the support provided to survivors were exposed.

The problems recognized in getting enough equipment and medical supplies to several sites have been addressed by the distribution of radio pagers to transit managers; in addition, the incident-control room has been reconfigured to allow for the possibility of multiple simultaneous attacks – the sheer scale of which created considerable confusion on 7/7, stretched supplies, and put unprecedented pressure on an outdated communications system. In fact, landline and mobile telephone communications were near impossible during the first two hours after the attacks; 45,000 calls came into the police Casualty Bureau phone line alone, and there was little information available from the incident scenes. Sir Ken Knight, the Commissioner for Fire and Emergency Planning, said it was a single hand-held radio at King's Cross subway station, not the entire system, that was faulty.

The most difficult challenge, probably, is achieving a balance between security concerns and ensuring that spectators can enjoy a friendly and open atmosphere – in contrast to the 2008 Beijing Olympics

Comms operators had to manage the high number of calls placed on both the fixed and mobile networks to prevent them grinding to a halt on 7/7 – a situation that, although not unprecedented, led to considerable distress when people caught up in the incidents could not contact one another. New dedicated digital radio systems are now in use, although cell phones continue to be used for multi-agency communication, particularly by senior officers. The cell phone networks' privileged access scheme is invoked only under very special circumstances on request by Police Gold commanders, and then only for a specific network, within a limited geographic area, and for the shortest possible period of time.

Another post-7/7 improvement is a new digital radio system that has been designed to connect all London Underground staff on a single radio network. In addition: (a) A purpose-built coordination center for local and regional responders now operates alongside the dedicated Gold command centers directing responder operations; and (b) The Metropolitan Police have pre-agreed arrangements in place to manage and coordinate a response to a pan-London incident.

Dealing With the Media

Of prime importance in 2012 will be the ability to supply timely and accurate information to the 24-hour news media to minimize panic and advise the public. The failure to establish reception centers for victims and worried families and friends to go to in the hours following the 7/7 attacks added to the overall response problems encountered at that time. In addition, detailed information was not collected from some of those caught up in the explosions so that they could be put in touch with sources of information, advice, support, and counselling. Many survivors were left with *no* access to information – almost as if the explosions had involved chemical agents – and no practical support to help them cope.

To address this issue, new procedures, systems, and training programs have been put in place, including mutual-aid telephone protocols between police units to enable the Police Casualty Bureau to handle more calls than was possible on 7/7, as well as recorded messages for the public, which will enable the bureau to focus on gathering information about missing persons.

Germany 2006: The Gold Standard for Chemical Readiness

Recent high-profile sporting events in other countries have generated equally high levels of protection. The successful staging by Germany of the 2006 FIFA Soccer World Cup Finals, and the measures taken by that country to enhance security, detection, and surveillance, are regarded as an excellent example of organization and anti-terrorist prevention.

Preemption was paramount – suspects were identified when crossing the border or even well before coming to Germany. NATO AWACS surveillance planes monitored German airspace to guard against airborne attacks. Strategies to promote effective communication were deemed successful, with liaison officers from federal and state agencies – including European police forces, the armed forces, and fire departments – designated to ease the exchange of information. The Bundeswehr was on standby for emergency situations with decontamination units.

The chemical-surveillance plan saw the introduction of a multi-layer concept (developed in close collaboration be-

tween Bruker Detection and the blue-light services). Among the equipment provided under the plan were infrared stand-off detectors for toxic clouds of gas; hand-held ion mobility spectrometers; and mobile gas chromatograph/mass spectrometers (GC/MS) designed (through the use of complementary sampling techniques) to identify any organic chemical from the soil, water, and air within 15 minutes.

These detectors provided detailed information content as well as on-site support and scientific management. Systems were integrated on vehicles or networks of chemical and biological detectors. Training and operations were reduced to the lowest possible level, and the detectors were installed in a stand-by mode invisible to the audience. Finally, the monitoring of the stadia where the Finals were played commenced four hours before the games began and was continued not only throughout the games but, in addition, for two more hours after they ended.

In addition, reconnaissance teams were in standby-position, out of sight of the crowd but in communication with the command center inside the stadium. Mobile detectors were installed on a fire engine. Had an emergency occurred, it is claimed, the reconnaissance teams would have been able to reach every position inside the stadium within minutes, with samples analyzed and clearly identified within 10 to 15 minutes – as long a period as could be tolerated if the correct decisions regarding decontamination procedures and medical treatment can be made.

Finally, firefighters stationed within the command center were able to check the located cloud positions via binoculars and, of prime importance, observe the behavior of the people inside or near a located cloud.

Andy Oppenheimer, a UK-based CBRNE consultant, is the former editor of Jane's Nuclear, Biological and Chemical Defence and the author of IRA: The Bombs and the Bullets (Irish Academic Press).

Premiere Performances

NSSEs, Non-NSSEs – And the Security Risks Involved

By Neil C. Livingstone, Special Events

Throughout the almost eight years since the 11 September 2001 attacks against prime terrorist targets in New York City and Washington, D.C., there has been heightened concern – not only within the United States but in many other countries as well – about the possibility of other attacks during major public events at ballparks, convention centers, race tracks, field houses, theaters, stadiums, concert halls, and other large-capacity facilities. That concern has led to increased security at such events – so much so that the higher levels of security now required are considered "routine," and are generally accepted as such by the event planners and participants, and by the general public.

These increased and improved security measures might still not be enough, though, to protect the public and/or the performers at so-called "major or super events," hereby defined as premiere events that capture national or international attention – e.g., sports championships and awards ceremonies such as the Super Bowl, the Olympics, major golf tournaments such as the U.S. Open and the Masters, the Kentucky Derby, the Wimbledon tennis matches, the Academy Awards and Golden Globe Awards, World Cup Soccer Matches – and, from the racing world, Formula One contests, the Daytona 500, and the Indianapolis 500. Concerts featuring top headliners, major political conventions, and G8 summits obviously can be added to this already long list.

Certain events in the United States that would be particularly attractive to terrorists or assassins – because of their political importance, their size, the number of U.S. and foreign dignitaries likely to be attending, and their overall significance and visibility – have been designated by the U.S. government as National Special Security Events (NSSEs). Prominent among the relatively recent events receiving the NSSE designation have been the funeral of former President Gerald Ford, the Presidential State of the Union addresses by Presidents George Bush and Barack Obama, the Democratic and Republican presidential nominating conventions, the post-9/11 presidential inaugurations, and certain major international meetings attended by U.S. presidents and their counterparts from other nations. Various major sports events, including the Winter Olympics in Salt Lake City, the Super Bowl, Major League Baseball's All-Star game, and the NBA's All-Star game also have been designated as NSSEs.

The Secret Service has been assigned to serve as the lead federal agency "responsible for coordinating, planning, exercising, and implementing security" for the NSSEs, and has formed a Major Events Division specifically dedicated to managing what is an obviously formidable task.

In 2006, Sen. Arlen Spector, then chairman of the Senate Judiciary Committee, sponsored a measure to amend the Patriot Act to permit the Secret Service to arrest people who knowingly enter restricted areas at NSSEs. The measure was opposed by the American Civil Liberties Union (ACLU) and other left-wing organizations, but ultimately became law as Sec. 602 ("Interference With National Special Security Events") of the Patriot Act.

Numerous reasons have been cited for designating an event an NSSE, but probably the *principal* reason why such events represent major terrorist targets is that they receive extraordinary media coverage. If terrorism is, first and foremost, a means of communication, then terrorists view a successful attack at or related to one of these events as a virtually guaranteed method of conveying their message of fear and vulnerability to the largest possible audience. At the time of the Munich Olympic Games in 1972, to consider but one conspicuous example, television cameras were bulky, heavy, and expensive – unlike today's minicams and other portable equipment. The Palestinian terrorists who attacked the Israeli athletes and coaches at the Munich Olympics had no doubt, therefore, that a very high percentage of all of the television cameras in the world would be at the Olympics and that, by carrying out a horrific hostage drama, they would be guaranteed a global audience of unprecedented size.

National Special Security Events: The Official Rules

The U.S. Department of Homeland Security (DHS), through its State Homeland Security Grant Program (SHSGP) and Urban Area Security Initiative (UASI), makes various grant monies available to state and local jurisdictions to help them cope with and manage the security aspects of NSSEs. Each such event must have an NSSE designation in order to qualify for a grant, but the DHS secretary has a certain degree of latitude to reprogram funds to deal with unforeseen and often unforeseeable events. According to at least one well placed

DHS source, any serious threat – such as specific intelligence regarding a potential terrorist strike in the United States – might be enough to persuade the secretary to allocate money or personnel resources to an event that had not initially been designated as an NSSE.

Because the Secret Service is the lead federal agency in dealing with NSSEs, and other agencies – ranging from the FBI and the Defense Department to the Environmental Protection Agency and FEMA (the Federal Emergency Management Agency) – also are likely to be involved, security forces from the venue itself and/or provided by local and state jurisdictions probably would be relegated to supporting roles. For that reason, the comments that follow will focus primarily on non-NSSEs – i.e., events of major significance and magnitude that do not quite qualify for an NSSE designation.

Non-NSSEs and Other Major Events

Managing security for a major event is likely to be the most difficult challenge that a security manager undertakes. If he or she does not have previous special-event experience, consideration should be given to bringing in someone with that background for the major event in question, and/or retaining the services of outside consultants for this purpose. The security requirements for a major event, even if it has not been designated an NSSE, will generally require the resources and cooperation of local, state, and federal police and fire protection agencies, as well as a host of organizations ranging from the public and private entities in charge of critical infrastructure (power, water, gas, telecommunications, etc.) to local hospitals and medical support, city and county agencies and organizations, transportation modes and facilities – railroad and bus depots, for example, as well as airports and public and private parking garages – and even those responsible for security in the air space over the venue.

Appropriate time must be allocated to planners to prepare for and organize each event. At high-capacity venues there may already have been a threat assessment, a security assessment, and an operations plan developed for addressing ordinary events. Even if this is the case, it is recommended that a new and more thorough threat assessment be carried out, particularly given the fact that conditions are now likely to be different, and more difficult, at a super event than they had been at a previous event. For example, more VIPs probably will be in attendance, the crowds may be larger, there almost certainly will be more members of the media covering the event, and other risk factors may be greatly enhanced. Organizers should refer to previous events of a similar nature, though, and use them as a template for their planning, paying special attention to the lessons learned and after-action reports.

After a new threat assessment has been prepared, planners can develop a master security plan and its operational counterpart for the specific event in question, often building on existing plans and previous operational experience. Today's major events may even require some physical modifications to the venue – increasing the "through capacity" of doors, for example, to accommodate the installation of outsized detection systems such as magnetometers, x-ray machines, and other sensors. Additional space also may be required both to facilitate the "wanding" of attendees by security personnel – and to search their bags, if bags are permitted on-site – and to carry out the more elaborate screening, in privacy, of potential high-risk attendees.

More space also may be needed for the hundreds or thousands of attendees queuing up to enter the venue, not only because the crowds are larger but also because it may take longer today to verify credentials and authenticate tickets.

An arena's (or theater's, or convention center's) air vents may have to be secured to prevent the introduction of chemical or biological agents. Consideration may also have to be given to expanding the outer security perimeter and screening all vehicles, no exceptions, entering the area. Underground parking beneath the venue may have to be tightly restricted – or banned altogether. If there are several venues involved, the creation of a secure and reasonably convenient transportation system between the different sites will become a major requirement,

About the photo: This photo was taken at the Glastonbury Festival 2005, and shows the Pyramid Stage Pit Team. Photo compliments of Specialized Security, one of the UK's leading Crowd Management Companies, with a wealth of experience, particularly in dealing with the unique problems of large-scale music festivals and mass gatherings.

and special arrangements will have to be established for buses and dignitary limos. Here it is worth pointing out that it was because of vehicle breakdowns and an underestimation of the number of buses required that the organizers of the 1996 Atlanta Olympics were forced to bring in more buses – after the Games had already started – and there was not enough time to repaint the buses. The result was a situation that not only caused considerable confusion but also created a number of potential security breaches.

Today, most large venues already have in place a centralized communications and coordination center (CCC) for command and control, but the existing CCC may have to be expanded (in size as well as in capabilities) to deal with the increased scale and complexity of a major-capacity special event. For world-class events the CCC may have to operate on a continuing 24/7 basis; in any case, it should be staffed by representatives of all of the participating agencies tasked with operational-security, crisis-management, and/or consequence-management responsibilities.

The CCC also will have to be equipped with up-to-date communications systems – including telephones, cell phones, computer lines, and wireless systems as well as interoperable radios that link the center to all key security nodes and locations as well as to every other type of internal and external communications resource available in the vicinity of the venue. Another vital component of the CCC should be an intelligence team, the members of which would constantly evaluate risk factors and receive, process, and share intelligence related to the event.

The planning for all special events will require the establishment of an information center or other designated media area to accommodate what is likely to be a major influx of print and broadcast reporters, photographers, and news organizations covering the event. Regular briefings should be scheduled so that the media's often insatiable need for news will be accommodated. If media reps do not receive enough information, they may attempt to generate it themselves, particularly if an incident or problem of some kind occurs, and this can lead to rumors and misinformation being reported as fact.

Today, badging and credentialing are more important than ever before because they: (a) permit organizers to control the number of people attending the event; (b) determine what areas the various groups of attendees should have access to; and (c) ensure that those being screened are who they purport to be. In recent years, a number of major sports events have had to deal with problems involving counterfeit tickets and/or credentials, not only experiencing a loss of revenue, but leading to problems such as too many people on "Pit Row" or backstage at a special event. Fortunately, new technologies and systems have become available in recent years to protect and verify tickets and credentials not only more quickly but also more effectively.

Some planning also should be devoted to the possibility of a catastrophic WMD (Weapon of Mass Destruction) attack on the venue. Preventing and/or coping with such an attack will require mass-casualty preparedness and environmental screening/public health surveillance, along with a scalable EMS response. It is and should be anticipated that medical staff will be on-site for such an event and that these professionals will have been both trained and exercised, beforehand, in addressing various WMD scenarios, including those involving chemical agents, radiological devices, biological agents, and/or hoaxes. Nonetheless, if an incident does occur, the organizers and medical staff must know in particular: (1) where to report to for backup assistance; (2) how to triage casualties; and (3) the precautions necessary to prevent themselves and other first responders from becoming infected or contaminated.

Finally, after the advance planning has been completed and all operational components are in place, the whole system must be exercised – not just once, but over and over again – until all of the "bugs and wrinkles" have been worked out. The cardinal rule of event security, like most security situations, is that any such event is only as safe as its weakest link. At the 1996 Atlanta Olympics the Achilles' heel was Centennial Park. It is vitally important that the planners of future such high-capacity events develop a seamless and well coordinated security program that is both inclusive enough and flexible enough that any deficiencies can be identified *before* the fact, and that appropriate fixes can be implemented before they can be exploited by terrorists or other evildoers.

Editor's Note: In earlier articles for DPJ, Dr. Livingstone discussed the routine security measures required, in the post-9/11 era, for major public events at theaters, field houses, concert halls, sports arenas, and other facilities where large crowds are expected. (See Facilities Management in the Age of Terrorism, in the 29 June 2005 issue of DPJ; and Stadium and Venue Security, in the 24 September2008 issue.)

Dr. Neil C. Livingstone, chairman and CEO of Executive Action LLC and an internationally respected expert in terrorism and counterterrorism, homeland defense, foreign policy, and national security, has written nine books and more than 200 articles in those fields. A gifted speaker as well as writer, he has made more than 1300 television appearances, delivered over 500 speeches both in the United States and overseas, and testified before Congress on numerous occasions. He holds three Masters Degrees as well as a Ph.D. from the Fletcher School of Law and Diplomacy. He was the founder and, prior to assuming his present post, CEO of GlobalOptions Inc., which went public in 2005 and currently has sales of more than $80 million.

Emergency Management and Special Events: Challenges, Support, Best Practices

By Kay C. Goss, Emergency Management

A special event is typically any planned activity considered likely to attract a group of 10,000 or more known or estimated participants and/or attendees in a defined area where access by emergency vehicles may be delayed (or, in some instances, limited by the host jurisdiction to a much smaller number).

The National Response Framework (NRF) sets the stage for the overall context of managing special events from an emergency manager's point of reference. The policy enunciated by the Federal Emergency Management Agency (FEMA) is that the federal government provides support and resources to state and local governments for significant special events. The Secretary of Homeland Security possesses the authority to designate an event as a National Special Security Event (NSSE). The NSSEs represent a unique category of public gatherings that – because of their political, economic, social, and/or religious significance – may make them particularly attractive targets of terrorism or other criminal activity.

If an event is designated as an NSSE, the U.S. Secret Service, which serves as the primary agency for coordinating federal support for such events, employs NIMS (National Incident Management System) principles and any applicable structures/organizational components within the Framework – e.g., a Joint Field Office, Emergency Support Functions, or Incident Annexes – to carry out its NSSE responsibilities. The most recent National Security Special Event was this year's Presidential Inauguration in January in Washington, D.C.

Collaborations, Cooperation, & Responsibilities

Typically, special events are local or state matters handled in various collaborative partnerships with state, tribal, and local governments, private-sector organizations, and non-profit agencies or organizations, including colleges and universities. Almost all emergency managers eventually are responsible for at least a few special events within their jurisdictions for which detailed security planning is required.

Almost all emergency managers eventually are responsible for at least a few special events within their jurisdictions for which detailed security planning is required

Many "best practices" in planning for special events are available for researchers and planners throughout the nation. *The Special Event Emergency Action Plan Guide*, prepared and published by the Bureau of Plans of the Pennsylvania Emergency Management Agency (PEMA), is a commendable example that provides a list of the procedures recommended for creating an Emergency Action Plan for special events. The establishment of adequate Emergency Medical Services is the first priority listed in the Guide. Other recommended/desirable components include on-site facilities to provide protection from weather (to ensure patient safety and comfort), an adequate number of beds and cots, and basic life support equipment – enough to provide for the evaluation and treatment of at least four patients simultaneously – and, finally, adequate light and ventilation.

The Guide also makes it clear that a licensed physician, a special-event emergency supervisory physician, various basic life and advanced life support systems, equipment, and people – specifically including emergency medical technicians (EMTs) and paramedics – a triage area, and a temporary morgue (because a worst-case scenario must be a part of any such plan), also would be needed.

The principal components of PEMA's Special Event Emergency Action Plan include, among other things, sections on: (a) a notification chart; (b) notification procedures; (c) group and individual responsibilities; (d) a list of emergency identification, evaluation, and classification policies and procedures; and (e) a helpful list of preventive-action recommendations. The Guide also includes several appendices, which may be used to cover: descriptions and locations of a special event; an analysis of the potential for disaster; the need for training, testing, and updating; the posting of a notification chart; an EMS response plan; a glossary; and recommended responses to specific disasters and other emergencies.

A Capital Guide for D.C.-Based Events

The National Capital Region (NCR) – i.e., the greater Washington, D.C., area, which of course is the site of many national, regional, multistate, state, and local special events – has developed more than its share of exemplary practices. Nearby Arlington County and the city of Alexandria in Virginia, as well as Montgomery County and Prince George's County in Maryland, provide many of the leading security professionals assigned to work with their NCR counterparts at the numerous D.C.-based special events taking place every year.

Loudoun County, somewhat farther out in Virginia, has developed an online resource tool for special events planning that the county makes available to all sectors and all jurisdictions in the area that are hosting a special event. In addition, a special-events coordinator is available to walk any organization through the county's process – which encompasses a host of necessary tasks ranging from securing a special-event permit from the county to: (1) the development and promulgation of an online event information form; (2) acting as liaison to agencies that the county suggests the organizer might want to contact and/or work with in the planning process; and, finally (3) providing a comprehensive list of the numerous (and frequently complicated) rules and regulations that might apply to a specific event.

In the District of Columbia itself, the Mayor's Special Events Task Group has designed, developed, and published an equally valuable publication – *Your Guide for Planning a Special Event in Washington, D.C.* The D.C. Guide differs in several ways from the other models mentioned, because it is designed strictly for event organizers, rather than emergency managers, and focuses on preventing or at least mitigating potential problems during the *planning* stages rather than during the special events per se.

West Virginia University (WVU) also has published a Special Events Planning Guide, which is designed for campus events that include 500 or more participants. The WVU special events are designated as such by the Director of University Police and are not covered by any other specific emergency-response plan, including but not limited to those governing the security of stadiums, gymnasiums, auditoriums, dining halls, and student centers. In addition to providing an overall concept of operations, WVU's Planning Guide includes sections on communications, facility evaluations, and training. Among its several appendices are an Emergency Action Planning Checklist, an Emergency Action Planning Template, a Special Campus Event Staff Briefing Roster, and a Post-Event Assessment, all of which are considered useful models that other special-events planners might want to consult.

Finally, the Security Standards Policy and Planning Committee of the American Public Transportation Association (APTA) has published its own *Recommended Practice for Security and Emergency Management Aspects of Special Events*. This voluminous guide, which is designed primarily for use by those responsible for public transportation systems and facilities affected by special events, serves as a particularly helpful model for emergency managers because the planning, training, exercises, technology, and partnership building related to any special event necessarily touch upon all modes of transportation in the area or jurisdiction hosting such an event.

Kay C. Goss, CEM, possesses more than 30 years of experience – as a federal and state administrator and in the private sector – in the fields of emergency management, homeland security, and both public finance and intergovernmental operations. A former associate FEMA director in charge of national preparedness training and exercises, she is a noted lecturer as well as the author of several books and numerous articles and reports in the fields of homeland defense and emergency management.

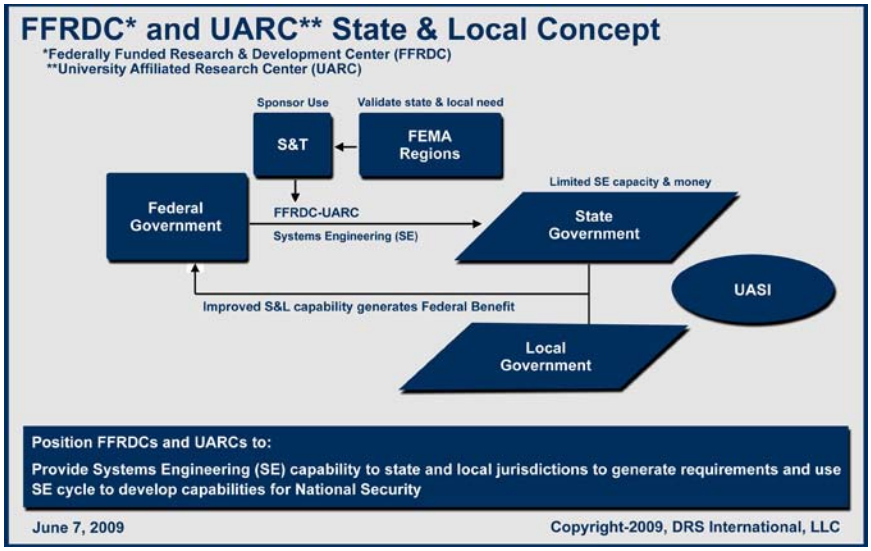
Providing Systems Engineering Support to State & Local Jurisdictions

By Dennis R. Schrader, Funding Strategies

It has been previously suggested that the federal government should provide direct assistance to state, local, and private-sector entities to develop the homeland-security capabilities of those entities and thus help meet *national* priorities. Over the past eight years, many state and local jurisdictions have struggled to engineer new capabilities, and/or to re-engineer existing capabilities, in accordance with the numerous homeland-security requirements coming out of Washington, D.C. – i.e., mandated by the executive and/or legislative branches of government. A continuing lack of systems-engineering and program-management resources and core competencies has intensified the challenge.

Two already existing resources – which have been largely untapped to date, however – are the Federally Funded Research and Development Centers (FFRDCs) and the University Affiliated Research Centers (UARCs), both of which are authorized under federal law to provide essential engineering, research, and development capabilities through non-competitive procedures. The accompanying diagram shows how the concept is supposed to work.

The FFRDCs were established during World War II to help federal agencies solve special R&D (research and development) problems that require intellectual capacity to augment existing internal resources. Acting as trusted advisors, the FFRDCs and UARCs enable agencies to carry out various RDT&E (research, development, test, and evaluation) tasks that are integral to the missions and operations of the sponsoring agencies.



Why Should Federal Resources Be Provided?

The Post-Katrina Emergency Management Recovery Act (PKEMRA) requires significant preparedness capabilities and assessments for states. The FEMA regions are assigned a significant role to play in this effort. The FFRDCs/UARCs can legally provide assistance to FEMA's regional staff to support improvements in capability development for state and local, particularly UASI (Urban Areas Security Initiative) jurisdictions.

The support that could be provided to the states through FEMA would improve and expand state and local capabilities that would enhance the nation's security and would be an innovative but affordable use of these RDT&E resources in support of FEMA's own national-preparedness missions and responsibilities. The process would also provide federal science and technology (S&T) organizations the validated requirements needed to invest federal resources either through S&T programs or through federal departmental and agency programs.

The FFRDCs and UARCs also could provide state and local jurisdictions the capability to effectively generate requirements and carry out systems-engineering programs. The systems-engineering cycle provides a ready path for documenting critical needs and then developing concepts and solutions that can be tested and evaluated. It also can document the scope of work involved in procurement and provide overall program-management support. Many if not all private-sector companies are reluctant to provide this service, it should be pointed out, because most state and local procurement rules would not allow them to participate in the downstream procurements.

It can be safely assumed that the nation's systems integrators are both willing and able to facilitate a transfer, to state and local governments, of the technologies and capabilities related to national-

Most Biohazard Detection Systems Come with a 20% Error Rate

Shouldn't You Be More than 80% Prepared for an Attack?

Instruments using antibody-based detection are less reliable because of their high false negative rate. Their results need to be verified at a separate lab using PCR. Idaho Technology's portable biohazard detection system, the RAZOR® EX utilizes the same PCR technology that health labs use without a need for in-depth knowledge of the science behind it. The RAZOR EX was made for HazMat and first responder teams that require more from a detection system.

The RAZOR EX is a complete product solution that is easy to setup, run, and read. Capable of testing ten bioterrorism agents in one run, the RAZOR EX provides more accurate results than other products in less then 30 minutes.

Visit our web site or call today and let us help you get the most trusted and accurate field portable detection system into the hands of your team.

Turn Your False Negatives Into Cash

Idaho Technology has many ways to help you get the best products for your team. For example, take advantage of our trade-in program by giving us your inferior antibody based detection system for cash towards the purchase of our more reliable PCR based detection system.

The RAZOR® EX with rugged carrying case

Idaho Technology Inc.

Innovative solutions for pathogen identification and DNA research

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

security environments. Private-sector companies obviously want to be able to provide products and services to state and local jurisdictions. However, they often are unable to determine, on their own, what the requirements are and are therefore perceived (erroneously, in most cases) as marketing solutions in search of problems.

After the requirements have been identified, there also could be Indefinite Delivery/Indefinite Quantity (IDIQ) contracts awarded through GSA (General Services Administration) schedules to provide follow-on systems-engineering and program-management services through private-sector companies.

The All Hazards Consortium (eight states, and the District of Columbia) of the mid-Atlantic region has been testing the use of FFRDCs and UARCs to develop prioritized regional requirements. The initial result has been the development and promulgation of five "White Papers" dealing with such important topics as fusion centers; communications and interoperability; the protection of critical infrastructure; catastrophic event preparedness; and geographic information systems.

The purpose of the White Papers is to identify consensus regional needs and to develop recommendations to meet those needs. Mitre, CNA, APL, and Argonne National Labs are prominent among the FFRDCs/UARCs that have participated so far.

The Oak Ridge National Laboratory in Tennessee is carrying out similar work in the Southeast area of the United States. In addition, the Naval Postgraduate School has prepared a report that analyzes the development of multi-jurisdictional networked alliances and emergency-preparedness organizations and entities. An inventory would undoubtedly discover other ad hoc innovations completed or now being carried out by FFRDCs and UARCs, as well as universities, throughout the nation. Systems engineering currently represents, in short, a significant gap that can be methodically, and cost-effectively, closed through the innovative use of the FFRDCs and UARCs.

Captain Dennis R. Schrader, USNR (Ret.), is president of DRS International, LLC, and former deputy administrator of the Federal Emergency Management Administration's National Preparedness Directorate. Prior to assuming his NPD post he served as the State of Maryland's first director of homeland security, and before that served for 16 years in various leadership posts at the University of Maryland Medical System Corporation. A licensed professional engineer in the State of Minnesota, he holds a bachelor of arts degree, with a focus in engineering, from Kettering University, and a master's degree from the State University of New York at Buffalo. While on active duty as a Navy Civil Engineer Corps officer he served overseas tours in Guam, Diego Garcia, and Sicily. He also has served on numerous homeland-security committees, including the Anti-Terrorism Advisory Council of Maryland and the Homeland Security Senior Policy Group.

Security Planning For Major Events

By Joseph Trindal & Joseph Watson, Law Enforcement

For Los Angeles, the recent memorial services for Michael Jackson were comparable to a state funeral in the nation's capital. Major events pose varying security and public-safety challenges requiring a systematic approach. However, there are very few criteria for determining what constitutes a major event from a public-safety and security perspective. Examination of the federal model for managing major national events is therefore a valuable template for state, local, and tribal communities to follow.

Presidential Decision Directive 62 (PDD-62), issued by President Bill Clinton in 1998, represented an early effort to address national major event standardization by assigning responsibility for coordinating "events of national significance" to the U.S. Secret Service (USSS). That executive action led to the Presidential Threat Reduction Act of 2000, which gives the USSS statutory authority as the lead federal agency for security planning of National Special Security Events (NSSEs). The president, or his designee – the secretary of the Department of Homeland Security (DHS) – determines which events merit the NSSE designation by considering, among other factors, the potential dignitary attendance, size, and significance of a specific event.

Surprisingly, perhaps, over the past 11 years there have been only about 30 NSSEs declared. Moreover, NSSE designation seems to be just as likely for an unfunded event as for an unfunded one. Congress did not provide funding to USSS for NSSEs, in fact, until 2006. Furthermore, obtaining federal funding for state, local, and tribal jurisdictions is even more difficult to achieve. However, non-federal agencies are usually able to use State Homeland Security Grant Program (SHSGP) and/or Urban Area Security Initiative (UASI) funds to support at least some NSSE security expenses. In addition, the cities hosting Democratic and/or Republican nominating conventions are usually provided some federal funding for security at those events.

The NSSE model provides a number of "gold standard" best-practice examples for lesser events. From a local perspective, it does not take federal designation for an event to be "Special and Significant" to the local community.

For example, in the spring of 2002 Major League Baseball (MLB) sought NSSE designation for that year's All Star Game. The MLB request was denied, but only a few months later the Super Bowl (XXXVI) was declared an NSSE (as has been every Super Bowl since then). For the law-enforcement community of Milwaukee (Wis.), the All Star Game was a Local Special Security Event. Like NSSEs at the national level, that particular local event posed security challenges that far exceeded the capabilities of any single local jurisdiction participating. The structure used for coordinating and managing NSSE security, however, proved to be a useful model.

Security Coordination At Major Events

There are few if any other metropolitan areas anywhere in the world that manage as many major events as the U.S. National Capital Region (NCR) – i.e., the greater Washington, D.C., area. During a preparation exercise for the 2005 Presidential Inauguration, then-DHS Secretary Tom Ridge asked Joseph Trindal, regional director of Federal Protective Service (NCR), and co-author of this article, if it was difficult coordinating security with so many law-enforcement agencies involved. "Not at all," Trindal responded, "we frequently work closely together because most events in Washington require interagency coordination." For the almost 40 jurisdictions within the NCR, almost every event is a local special security event.

Local special-security events provide excellent opportunities for state, local, and tribal jurisdictions to plan together with a common purpose. Planning and coordination are vital to safe and enjoyable local as well as national special events. The NSSE structure pre-establishes the basic principle that all major events are examined against security-relevant, risk-based criteria. Analysis of the NSSEs rests with a single department of the Executive Branch of government. On the federal side, therefore, there is no confusion or uncertainty about the DHS role. After an event has been declared an NSSE, a single agency is assigned the principal responsibility for security coordination and planning.

Leveraging the NSSE model at the local level should start, therefore, with ensuring that the responsibility for security coordination and planning is assigned to a pre-designated

law-enforcement agency. Other municipal, county, state, and private-sector stakeholders can and should, however, support the security function within their own core competencies and capabilities.

The Pre-Planning Phase of Major Events

In 2006, the Office of Community Oriented Policing Services (COPS) of the U.S. Department of Justice (DOJ) issued an excellent report of best practices for major event planning. That report – *Planning and Managing Security for Major Special Events: Guidelines for Law Enforcement Administrators* (i.e., the Guidelines) – provides practical guidance for major event planning at the local level. With input from the USSS and numerous other contributors, early event planning was highlighted in the Guidelines as an essential best practice.

The Guidelines stress the need to plan for worst-case scenarios, including but not limited to natural disasters as well as criminal, crowd-control, and terrorist contingencies; certain events also should include special sections for dealing with pre- and/or post-event protests

The planning for major events should balance public safety and public enjoyment with a realistic risk assessment. For example, a continuing risk related to the annual Independence Day celebrations on the National Mall in Washington, D.C., is the possibility that severe and/or fast-moving thunderstorms can produce dangerous lightning. After some rather tense events, a well coordinated plan was developed to provide early warning, rapid notification, and even temporary shelter for the hundreds of thousands of people who might be crowded together on or near the Mall when a thunderstorm approaches. That particular risk, and the contingency plan developed to deal with it, has turned out to be a repeated reality over the years.

The Guidelines also stress the need to plan for worst-case scenarios, including but not limited to natural disasters as well as criminal, crowd-control, and terrorist contingencies. Certain events also should include special sections for dealing with pre- and/or post-event protests.

Following the NSSE model, a local-event security-management structure should incorporate the Incident Command System (ICS). The Guidelines recommend the development of an event-specific organizational structure. Among the several important components of the ICS structure is the Administration and Finance Section – which also should reflect appropriate interagency collaboration and contributions.

Many local major events are recurring and/or otherwise well known in advance. The development of a 12-to-18 month planning timeline not only can greatly ensure the broad inclusion of all participating stakeholders but also provide sufficient time for thorough preparations in advance. In 2002, a local special-security event – but with national relevance – was thrust upon the City of Alexandria, Va. The DOJ had decided to hold a terrorist trial at the Albert V. Bryan U.S. Courthouse in this densely populated city just outside of the nation's capital. Fortunately, from the security planner's point of view, the U.S. judicial process is slow and deliberate – which meant, in this situation, that federal, state, and local agencies were able to coordinate, plan, and exercise extensively as the judicial proceeding for Zacharias Moussaoui moved steadily but very slowly toward his conviction and sentencing in 2006.

During the same period, not incidentally, other notable figures – including John Walker Lindh (the "American Taliban") and Robert Hanssen (ex-FBI agent/Russian spy) – also faced federal justice. The pre-event preparations in those cases developed and greatly strengthened interagency relations across disciplines of police, fire, hazmat, medical, transportation, and emergency-management services. In addition, the private sector and community were engaged partners to the overall security profile. The community in general was well informed and an active participant by the timely reporting of suspicious activities to the proper authorities. In this example, each day of planning was in essence a prior-planning drill for major events in the Moussaoui trial such as key judicial rulings, the verdict, and sentencing as well as other closely related high-threat judicial events.

The Management of Local Major Events

The creation of a special-event organizational structure is of prime importance. As mentioned earlier, the ICS structure is well suited as a model because it provides a clear delineation of responsibilities along cross-discipline functional competencies and is "scalable" enough to meet

both planned and unplanned dynamics related to the major event.

The establishment and equipping of an effective and reliable communications system is another vital component of event management. Communications challenges are ever-present at major gatherings. Communications protocols must therefore provide for relaying routine event coordination information as well as separate security-specific and dedicated communications for law-enforcement and security officials. The protocols needed for communicating important safety and security information to the crowd gathered at and around the event also must be established beforehand. The special-services communications required for the area's medical care and highway departments are usually handled through the protocols of those respective agencies. Nonetheless, special-services communications should be integrated, at the command level, with the event's overall ICS structure. Communications integration includes real-time, constant monitoring as well as the capability to pass information from ICS Incident Command and/or Section Chiefs to and across a number of disciplines and jurisdictions.

Event-management contingency plans should include the creation of pre-established criteria for deciding and implementing the actions needed not only to call off the event, if and when necessary, but also to rapidly communicate that decision to the media and participants, and to the general public. Many outdoor special events are subject to dangerous and rapidly changing weather conditions that may require fast decision-making and/or public-safety actions.

Resource management, a particularly important aspect of planning, is already built into the NSSE model through its incorporation of the ICS guidelines. During the event, resources of the right competencies and numbers should be positioned to best prevent, mitigate, and respond to contingencies. In terms of resource management, major events often require the involvement of the emergency services assets of several jurisdictions. Multiple-jurisdiction participation should be based upon Mutual Aid Agreements; however, contingency plans also should consider: (a) the potential need to draw additional resources from other jurisdictions; and (b) the potential need for participating jurisdictions to recall their pre-committed assets to deal with an unexpected event in their own jurisdictions.

Post-Event Considerations

All too often, after a major event has ended, there is a rapid retrograde of the public-safety principles established. However, even the conclusion of a major event poses substantial security challenges. When large crowds are moving away from the event venue, for example, there is a greater propensity not only for accidents but also for criminal activity. Public safety resources should be re-positioned, therefore, to facilitate the safe movement of pedestrians and traffic – and, not incidentally, to put those resources in a better position to respond to post-event contingencies. From the terrorist's perspective, the chaos inherent in post-event activities is an opportunity to carry out attacks that maximize casualties and exceed public-safety response capacities.

The Secret Service's NSSE protocols, and the Guidelines, stress the need to plan for a rapid retrograde of security operations and resources. The Guidelines also highlight the importance of After-Action Reporting and Improvement Action Planning to maximize the lessons learned and, of perhaps greater importance, to prepare for the next Local Special Security Event. Continued training and planning, after the conclusion of a major event, is an important best practice.

Fortunately for security planners, most if not all major events are predictable – to at least some degree. Almost every community, of any size, throughout the United States hosts a series of events during the calendar year that are that community's equivalent of a National Special Security Event. Developing a system for evaluating the security challenges for each such event, then planning and scaling resources accordingly, is vital for the community's safe participation in the event. Here, the inclusion of public and private stakeholders in the planning process is an important best practice. The federal protocols developed and promulgated for the coordination and planning of NSSEs, combined with the DOJ Guidelines, are excellent resources for local communities to follow in developing their own Local Special Security Event procedures.

Joseph W. Trindal (pictured) recently retired as chief of the Inspections & Enforcement Branch of DHS's Infrastructure Security Compliance Division. That branch is responsible for administering and enforcing the Chemical Facility Anti-Terrorism Standards. A career federal law-enforcement investigator and executive, Trindal served with the U.S. Marshals Service for 20 years before accepting the position of director for the National Capital Region, Federal Protective Service, DHS. Trindal is presently serving as Director of the Critical Infrastructure Protection Division of Covenant Security International.

Sergeant Joseph Watson is a former Marine Military Police Officer and 25 year veteran of the City of Alexandria Police Department. He is currently team leader for the Department's Special Operations Division, Community Support Section Homeland Security Unit. Watson is the founder and President of Special Operations Solutions, LLC. Consulting, Planning, Training, Exercises, and Operations. He is also a trainer in Basic and Advanced Special Operations, Firearms, Defensive Tactics, ODP Awareness, and Hazardous Materials. He was the recipient of the 2002 Washington Metropolitan Council of Governments, Chiefs Training Committee, Instructor of the Year award.

Protecting the Super Bowl – A Perfect Defense Is Mandatory

By Diana Hopkins, Standards

Incident management for major national events such as the Super Bowl requires the expenditure of millions of dollars, a great deal of preparation and planning time, and the utilization of advanced security technologies and incident-management skills. Moreover, these technologies and incident-management processes must meet DHS (Department of Homeland Security) standards for incident management as outlined in the department's National Incident Management System (NIMS).

When Tampa, Florida, hosted Super Bowl XXXV in January 2001, ticket holders could pass through security with a simple bag check and ticket scan. Today, continuing the tighter security standards in place since the terrorist attacks of 11 September 2001 against the United States, major stadiums and indoor sports arenas throughout the country are considered to be prime terrorist targets in terms of the mass casualties as well as the catastrophic economic impact that are likely to result from a terrorist attack. Along with the World Series and the Olympics, the Super Bowl is now classified by DHS as a National Special Security Event (NSSE).

Earlier this year – on 1 February 2009, to be more precise – Tampa was again the Super Bowl host, at Raymond James Stadium. This time around, though, it took two years of preparation and millions of dollars (contributed primarily by Tampa City and the National Football League) to cover the cost of security. Four days prior to the game, a final planning meeting was held that included over 100 law-enforcement officers and agents from more than a dozen organizations, including DHS, the Federal Bureau of Investigation, the Department of Energy, and the U.S. Coast Guard. Those officers and agents represented only a fraction of the more than a thousand agents and officers actually on duty before and during the game itself.

The preparations for Super Bowl XLIII also included extensive background checks (carried out by DHS's Immigration and Customs Enforcement agency) on the tens of thousands of applications submitted by people who typically work at the Super Bowls. A telephone number was provided to local citizens who noticed and wanted to report suspicious activity in the area. The City of Tampa also used an emergency-preparedness response system (comprised of SAP Business Intelligence Software Crystal Reports® and Xcelsius®, and NC4 E Team™ and Situational Readiness™ software) to permit web-enabled access by responders and to facilitate, among other things: enhanced information sharing; the development of risk assessments and disaster modeling; the creation and use of a centralized command system; the production of daily planning schedules; the monitoring of all agencies and branches involved with the Super Bowl; and the completion of various resource-management tasks. In addition, Kore Telematics and U.S. Fleet Tracking provided Tampa City with a system for tracking all security vehicles as well as those transporting VIPs to and from the Super Bowl.

Adherence to NIMS & HSPD-5 Also Required

But employing a host of new security bells and whistles was not enough in itself. The City of Tampa also had to meet the incident-management standards developed under NIMS. Here it is worth noting that it was on 28 February 2003 that President George W. Bush issued Homeland Security Presidential Directive 5 (HSPD-5 – entitled "Management of Domestic Incidents"). Under HSPD-5, the Secretary of Homeland Security is responsible for the coordination of federal preparations as well as the response to and recovery from terrorist attacks, major weather disasters, and other designated emergencies.

HSPD-5 also requires that the DHS Secretary put into place and administer the previously mentioned National Incident Management System – which, among other things, is responsible for the development and use of templates for government and private-sector emergency responders to follow in their collaborative efforts to prevent, protect against, respond to, recover from, and mitigate the adverse (and potentially catastrophic) effects of major incidents.

Under NIMS, the standards for coordinated planning and training, including training exercises, serve as the foundation for the interoperability and compatibility of resources before, during, and throughout an incident. Using the templates mentioned above, response personnel from different jurisdictions work in close cooperation to identify, combine, discover, and manage incident-specific resources.

For interested emergency-management personnel, the DHS/FEMA Emergency Management Institute (EMI) offers, free of charge, a variety of courses on the basic and advanced concepts of Emergency and Disaster Management. (Additional information on those courses is available at http://training.fema.gov/EMIWEB; additional information on NIMS and its standards is available at www.dhs.gov.)

PENN STATE | ONLINE

www.worldcampus.psu.edu

Become a leader in homeland security

Gain the expertise you need to respond to threats of terrorism and natural disaster.

Penn State offers four online graduate programs designed to create leaders in the homeland security profession:

- **Master of Homeland Security in Public Health Preparedness**
- **Certificate in Homeland Security and Defense**
- **Certificate in Bioterrorism Preparedness**
- **Certificate in Disaster Preparedness**

Put yourself in line for career advancement, earning your degree or certificate while working in your current position.

PENNSTATE World Campus

www.worldcampus.psu.edu/DomPrep

U.Ed.OUT 09-1334/09-WC-273edc/bjm

Special Events: Reality TV for Training & Exercises

By Joseph Cahill, EMS

New York City EMS (Emergency Medical Services) has long used the term "planned MCI" – i.e., a planned Mass-Casualty Incident – to refer to special events. That seemingly ambiguous description reflects both sides of the dilemma that describes such "special" events: on the one hand, that the responses to such incidents are or should be planned well in advance, and should therefore be carefully controlled; on the other hand that the outcome of such an event is as unpredictable as it would be of any other event requiring an emergency response. And, of course, such events generate real patients.

Smaller events such as a well attended concert can be viewed as a training ground for the intangible skills required to manage and carry out incident-command, logistics, and other basic ICS (Incident Command System) functions that can be initiated and completed in real time. The practice gained in receiving this type of experience in a controlled environment becomes invaluable if and when those in charge of the simulated incident are later called on to lead a response in a completely uncontrolled environment.

A major benefit of practicing the appropriate responses to various special events is that those involved learn from practical experience the meaning and use of such intangible but vitally important ICS concepts as chain of command, span of control, and resource management. The chain of command at the concert just mentioned might have only a few "patients" to deal with, but the communications requirements would be similar, and the incident commander would have to organize his or her subordinates in much the same way he or she would at and during a real-life MCI. And, of course, even a relatively small non-simulated event such as a "rock" or "rap" concert might in fact generate a large number of patients, yielding a different and probably even more valuable type of experience.

In some cases, one of the advantages provided by working at a real-life special event is that it provides MCI leaders with a ready pool of patients as well as a venue to test various plans, theories, and systems. Here, a prime example is the annual Boston Marathon, which for a number of years has been used to test patient-tracking software in real time – while simultaneously dealing with a varying number of real patients. Last year alone, more than 4,000 patients were seen either at hospitals or in any of several temporary healthcare field stations strategically positioned at various points along the marathon course.

Capitalizing on the Inherently Unpredictable

Perhaps the biggest advantage to using a special event such as a marathon as a full-scale exercise is that the patients and bystanders are equally unscripted, and as a result can be counted on to do the same unpredictable things that most humans do in their everyday lives.

The 2007 Boston Marathon was used, for example, as a full-scale exercise of the Massachusetts Department of Public Health's (MDPH) Hospital Capacity Website hospital resource tracking system, which allows hospitals to report – directly to the MDPH, and through a web-based system – the number of beds and other resources currently available in each healthcare facility in the area.

Because all hospitals in the area potentially could receive patients – but the reality of which hospitals *would* receive patients is unpredictable – the system could not be front-loaded with data; as a result the data stream coming in through the system in 2007 generated all of the same difficulties that would be encountered in the real-life reporting of such data.

A footnote of special importance to emergency managers: Many federally funded grant programs require that exercises be carried out as the final proof that the taxpayers' money has actually paid for a demonstrably improved response capability. Many of these same programs, however, allow grant recipients to use real-life response events in place of exercises. Which means, of course, that the grant-savvy manager may be able to save the cost of an exercise while at the same time providing the responders with a more substantial real-life experience.

Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as the citywide advanced life support (ALS) coordinator for the FDNY - Bureau of EMS, and prior to that was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. Much in demand as a speaker - he has addressed venues as diverse as the national EMS Today conferences and local volunteer EMS agencies - Cahill also served on the faculty of the Westchester County Community College's Paramedic Program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montfiore Hospital.

The PPO & Surge Capacity: A Different Type of "Insurance"

By John J. Burke, Fire/HazMat

To hospital and EMS (emergency medical services) healthcare providers the topic of surge capacity is one of the most widely researched and discussed aspects of public-health emergencies. The 22 June 2009 Metro subway crash in Washington, D.C., cast new light on the procedures involved in the handling of sensitive patient information both during and after high-profile mass-casualty incidents (MCIs), and raised new questions about the steps needed to prevent the possible theft of patient data during and after such events.

The Town of Sandwich, Massachusetts, conducted a major pandemic exercise on 14 November 2008. The one area where there appeared to be a glaring liability was in the handling and distribution of patient information during the simulation. The pandemic exercise was simulated during an annual flu clinic – during which patients were processed through a drive-thru vaccination area for their annual flu shot. The patients also provided medical information so that the Town could receive reimbursement through Medicare. However, there was no specific protocol set for the possession, destruction, and/or distribution of the sensitive patient health data material. That problem had to be addressed in the IAP (Incident Action Plan), with the responsibility assigned to an ICS (Incident Command System) specific position.

A Patient Privacy Strike Team was created originally as a working unit of the Intelligence Branch (under the director of operations) but could very easily have been shifted to the Intelligence Section Chief – a new position supported by the U.S. Department of Homeland Security. Included on the team would be five members trained in HIPPA (Health Insurance Privacy and Portability Act) requirements, who would handle the patient information "from cradle to grave" during the incident or exercise.

The creation and use of a Strike Team, which would be supervised by a Patient Privacy Strike Team Leader, was in line with the National Incident Management System (NIMS) principle requiring that similar resources be grouped together to ensure a more effective and efficient span of control.

The Strike Team is typically deployed in accordance with the comprehensive emergency plans developed for the Town of Sandwich and/or for Cape Cod Healthcare. In most if not all situations the Strike Team would coordinate its efforts with those of a Patient Data-Theft Task Force, which would be composed primarily of IT, law-enforcement, public health, and hospital personnel; an assistant district attorney also would be a member of the Task Force to provide legal guidance and oversight. One responsibility of the task force would be to immediately investigate any suspected breach of patient data and/or electronic health records, while also providing an intentionally visible awareness of – and, therefore, deterrence to – future illegal patient data miners.

Assignment of a working professional qualified in the position would ensure that the patient information gathered would not only be accurate, but also kept secure until the patient is transferred

In insurance circles, PPO usually stands for "Private Provider Option." In a mass-casualty incident the same acronym stands for patient privacy officer, whose duties and responsibilities would be little different from those of anyone else appointed to an MCI position. Establishment of the position, though, would reduce the Town's liability during and/or in the aftermath of major mass-casualty incidents.

Assignment of a working professional qualified in the position also would ensure that, during a large-scale surge event such as the Washington Metro crash last month, the patient information gathered would not only be accurate, but also kept secure until the patient is transferred to the custody of hospital and/or EMS transport personnel.

The initial arriving company officer had a lot of action items to think about upon his arrival at the scene. There was no indication that patient privacy was even a thought in his operational plan. The position could very easily be added as an MCI position and would provide both responders and receiving personnel some clarity as to whom they are actually receiving. The four basic positions for an EMS mass-casualty response are Triage, Treatment, Transport, and Loading Officers. The positions

of Loading and Transport are sometimes merged because of a manpower scarcity, so in reality the four positions would still be intact with a combining of two positions and the addition of one, the PPO.

The PPO would have a major task in managing all patient information, so the formation of the Strike Team mentioned previously makes sense for both continuity and security. The position has merit in large urban public-safety agencies, but may be more challenging for rural agencies to staff. The key fact is that patient privacy and HIPPA represent potential liabilities to municipalities – and to healthcare institutions, regardless of their size – so any changes or additions to existing plans directly addressing that possibility are a plus.

The irony is that there is significant potential for interaction with the Public Information Officer. The PIO and PPO would interact significantly in any case, because the PIO would be looking for certain information about almost any patient – his or her sex and age, for example. The release of that information is permissible under HIPPA, to keep the public informed about the scope and impact of the event. This relationship highlights the necessity of further training and collaboration between the PIO and the PPO.

A temporary shift in thinking is needed for the definition of a PPO as a personal insurance provider option. For public-safety and mass-casualty planners the PPO should define a different type of insurance that protects a municipality and/or healthcare institution from potential lawsuits, and from government fines, for HIPPA violations.

The tragedy of last month's Metro crash highlights the need for greater consideration of patient privacy issues. There are in many if not all transportation accidents at least a few follow-on improvements in mechanical safety recommended to prevent similar such accidents in the future. Similar improvements, in planning and response operations, to patient-privacy issues are just as important for public-safety agencies.

John J. Burke, a longtime employee of the Sandwich Fire-Rescue Department, received a bachelor's degree in Fire Science from Columbia Southern University. He is certified in all levels of the National Incident Management System and nationally certified as a firefighter I/II, a fire inspector I/II, and a hazardous materials operations and incident safety officer.

A Signal Opportunity

A Global Sensor Network for Disaster Warnings

By Diana Hopkins, Standards

A sensor is a device used to measure a physical quantity – temperature, pressure, and/or movement, for example – and to convert that measurement into an output signal for further human or computer processing. In the field of domestic preparedness, a sensor is a device that detects a natural disaster such as a tornado, a flood, a tsunami, or an earthquake and forwards that information into systems that evoke a response that will save lives and property. Although disasters are unpredictable, the sensor technology already exists that can signal, often within seconds, the time a disaster begins.

Although sensors have been developed that detect the very moment of a disaster's beginning, and some of these sensors are already in place, most nations throughout the world still rely primarily on their own human senses to detect disasters. Some countries such as the United States also use Doppler radar in certain situations, and alert the public, through the use of civil-defense sirens and broadcast warnings over local radio and television stations, that a major weather-related disaster might be imminent.

When one considers the suffering caused by the loss of lives, and the injuries incurred, when disaster strikes, and the worldwide annual economic cost of disasters (approximately $400 billion, according to a November 2007 Ceres Report, *From Risk to Opportunism*, by Evan Mills), it is reasonable to ask why earth-bound and remote satellite sensors are not used more extensively, on a *worldwide* basis, to provide the precious additional seconds or minutes of warning that could easily translate into reduced deaths, injuries, and property damage.

The High Cost of Inexplicable Delay

To understand the reasons behind the delay, it is important to recognize that sensors are only one component of larger and more complex geospatial information systems that distribute, gather, and process information about disasters. In other words, it is not as simple a matter as a two-step smoke-alarm process in which a stand-alone sensor device detects smoke and automatically triggers an alarm. However, the disaster information now gathered from sensors not only allows rapid response, but also permits the sensor data to be quickly gathered, stored, and processed for disaster recovery, mitigation, preparedness, and prediction.

But the question remains: With the advanced computer technology now available, why is there such apparent reluctance to use sensor technology more extensively? It would stand to reason that, with worldwide disasters costing an estimated $400 billion per year, most of the world – its land, seas, and skies – should by this time be automatically monitored by a global geo-sensor network to lower both the economic costs and the number of lives lost because of disasters.

The problems involving the use (or, in this case, *non-use*) of a global sensor network are caused, in large part, by difficulties in information sharing. Although not as plagued by the stigma of trust and security issues related to the sharing of national-defense and homeland-security information, the world's sharing of disaster information is still hampered by the lack of *interoperability* of current disaster-information systems. One at least partial solution to this problem might be the development of international consensus-based interoperability standards that facilitate and improve information sharing through the use of harmonized software, hardware, and processes that are openly accessible to all of the world's government and industry disaster-management stakeholders, emergency responders, scientists, and decision-makers. There seems to be no good reason, in fact, why such information should not also be available to the general public, which means that part of this solution would be to make such geo-information both rapidly accessible and free of charge through both the World Wide Web and the hand-held devices carried by individual citizens.

Encouraging Progress, But Formidable Obstacles Remain

Fortunately, there are several international geospatial consortia that have been working for some time on integrating data and systems to help in disaster-management situations. There also has been accelerating interest, enthusiasm, and rapid growth in this area of standards development, which is particularly important when one considers the numerous technological, political, and economic factors that must be taken into consideration before a global consensus and standardization in this area can be achieved.

Those factors include, but are not limited to, the following: the use of wireless sensors vs. non-wireless sensors; adding

intelligence to sensors; the positioning and spacing of sensors; data communications and data development; the mining and processing of information; spatial and temporal granularity; the incorporation of data received from multiple sources; the validation, accuracy, and precision of the data received.

When one adds to that list various social and institutional hurdles, human user issues, the middleware for pervasive computing, the automatic acquisition of data, the accessibility of data, various ethics issues, data updating and harmonization requirements, energy constraints, and the management of massive volumes of sensor data it quickly becomes apparent why the development of a global disaster-information network is such a formidable challenge.

A Growing Consensus For Increased International Cooperation

For those working in the disaster-management field who wish to know more about progress made in the area of sensors and/or want to be included in the process of developing standards for sensors – and/or for the interoperability of associated geospatial information systems – the Open Geospatial Consortium (OGC [http://www.opengeospatial.org]) is a very active U.S.-based organization that focuses on the development of open standards for sensor networking; the OGC already has close to 400 members, many of them key representatives of the international geospatial community.

At this time, OGC has five proposed and adopted SWE (Sensor Web Enablement) specifications, and harmonizes its work with other geospatial standards and standards developers, including the standards developer IEEE (Institute of Electrical and Electronics Engineers), which has produced voluntary consensus standards for developers of intelligent transducers (sensors) and their information-sharing interfaces. (See a family of IEEE 1451 standards at http://standards.ieee.org/sds/index.html.)

OGC's SWE standards enable sensor developers to fit their devices to agreed-upon criteria so that sensor information is accessible, in standard code, and able to be manipulated using standard protocols and standard application interfaces. OGC's SWE standards and specifications provide a way for potential users to find the location of sensors, and to access published data on sensors of interest. The OGC SWE Standards Framework includes the following:

OpenGIS (Geographic Information Systems) Observations and Measurements (O&M) Best Practices Document (www.opengeospatial.org/standards/dp), which serves as a model for representing and exchanging observation results, and is accompanied by an OGC Best Practices Paper on "Units of Measure Use and Definition" that covers XML (extensible markup language) details;

OpenGIS Sensor Model Language (SensorML) Implementation Specification v0.0 (05-086r2) (http://portal.opengeospatial.org/files/index.php?artifact_id=12606) – which provides an information model for the discovery and manipulation of web-based sensors and their data;

OpenGIS(R) Transducer Markup Language (TML) Implementation Specification v0.0 (http://portal.opengeospatial.org/files/index.php?artifact_id=14282) – which is basically a standardized transducer (sensor) message format that facilitates accessing, exchanging, and storing sensor data;

OpenGIS(R) Sensor Observation Service (SOS) Implementation Specification v0.0 (www.opengeospatial.org/standards/requests/32), which defines an application program interface that provides a standard way to access information from all sensor systems; and

Sensor Planning Service (SPS) Implementation Specification v0.0 (www.opengeospatial.org/standards/requests/34), which helps large enterprises in sensor planning vis-a-vis large information flows of both live and stored sensor and imaging data.

A Final Footnote: Considering the urgent need for sensors to detect and disseminate disaster information on an international scale, it is heartening to review – at (http://www.opengeospatial.org/ogc/member) – the list of OGC members which include technical, strategic, and principal members representing well funded and well staffed sensor and geospatial initiatives in progress all over the world. Despite the interoperability difficulties inherent with information sharing, therefore, it seems clear that, with this level of effort, geo-sensor networks are now in the making that will facilitate disaster management, reducing loss of lives and property on a worldwide scale.

Diana Hopkins is the creator of the consulting firm "Solutions for Standards" (www. solutionsforstandards.com). She is a 12-year veteran of AOAC INTERNATIONAL and former senior director of AOAC Standards Development. Most of her work since the 2001 terrorist attacks has focused on standards development in the fields of homeland security and national defense. In addition to being an advocate of ethics and quality in standards development, Hopkins is also a certified first responder and a recognized expert in technical administration, governance, and process development.

OUR MISSION
YOUR SAFETY

MSA
The Safety Company

Selected for CEDAP 2008
Biological Agent Detection

5 MINUTE TIME-TO-ANSWER

Rapid analysis of white powder and liquid biohazards with

MSA's BIOSENSOR® 2200R
Biological Agent Detector

- Unique bioassay technology
- Low false positives
- Results are GO / NO GO
- Bio threat-specific kits

Agents Detected

- Anthrax
- Botulism
- Ricin
- Plague
- SEB
- Small pox

VISIT US ONLINE
MSANET.COM

MULTI-THREAT DETECTION

CWA & TICs
HANDHELD PORTABLE

FIXED-POINT CWA
MULTI-THREAT DETECTION

1.866.MSA.1001 | www.MSAPOLICELINE.com/domprep.html

Kentucky, Kansas, Washington, D.C., and Wisconsin

By Adam McLaughlin, State Homeland News

Kentucky
OnStar Technology: "Getting Help Quicker"

A well known technological innovation, installed originally in automobiles to help determine their location – and, in some situations, cause a stolen car to slow down – is now being used by 911 dispatchers to speed up response times for users in distress for any of several reasons.

Technological devices such as General Motors' OnStar system are becoming increasingly popular in today's automobiles, and manufacturers are finding new ways to make them even more effective. When OnStar first came into use, a call for help – if a driver was involved in an accident in the middle of the night, for example – would be transmitted to an OnStar call center, where an operator on duty would relay the emergency call, and the user's location, to the nearest 911 center.

"The weather, bugs, and snakes" that were unplanned elements of the exercise were a "good substitute" for the stress that would be created by a real-life incident

In Kentucky's Daviess County last month, the OnStar system began to automatically send a user's location to the county's 911 system, not only connecting users to the help they needed but also showing dispatchers, immediately, exactly where that help was needed. "Technology is changing every single day, and in the world of 911, it is more and more … [important] to have technology conducive to getting help quicker," said Daviess County 911 Director Paul Nave.

The technology itself also has come a long way, Nave said, and not only for in-vehicle systems. Eleven years ago, cell phones could tell dispatchers only what transmission tower the signal was being sent from, and the caller's phone number. Now, it can give them that same information, and narrow the caller's location to within 150 meters (allowing for a small margin of error). Moreover, the technology is pre-set to automatically give dispatchers that information the moment the caller dials in.

"It makes a world of difference knowing where the caller is," and if he or she needs help, Nave said. "We can save minutes and save a life." The same technology is also valuable for solving crimes – particularly automobile theft. Today, a stolen vehicle equipped with OnStar or a similar system can be remotely activated and traced, helping law-enforcement agencies recover the vehicle – and, possibly, make an on-the-spot arrest of the car thief. "I believe it [the OnStar capabilities] would make a criminal think twice about stealing a vehicle that can be disabled and located," Nave said.

OnStar also is useful in finding someone who has been reported missing. Law-enforcement personnel can now not only track cell phones but also determine the location from which a person accesses a certain Web site – e.g., Facebook or a bank account number. This creative use of a still-evolving technology "makes our life easier, and … is also beneficial to the victims," said Lt. William Thompson, head of the Criminal Investigations Division of the Daviess County Sheriff's Department.

Because the OnStar technology is rapidly changing, and becoming even more capable, it is today increasingly important, Nave said, that emergency-response capabilities also keep improving. "More than 70 percent of our 911 calls are wireless [i.e., from cell phones]," Nave said. Because of OnStar and other technological advances, he said, "people feel safer, I think. They have a wireless device that can get them help anywhere." The current technology will continue to improve for the foreseeable future, he added, making the job of law enforcement not necessarily easier, but faster and significantly more effective.

Kansas
Hosts Multistate Exercise at "Crisis City"

Everything that could go wrong will go wrong at Crisis City. It could be a domestic terrorist triggering an explosion on a railroad line, causing a derailment, or a propane tank catching fire and exploding into a nearby building, causing it to collapse.

All of this "it" was part of an exercise in late June at Crisis City, the name given to an emergency-responder training site near the town of Salina in central Kansas. The mock city is a component of the Great Plains Joint Regional Training Center, which includes the Smoky Hill Range Complex, the Kansas

Regional Training Institute, and the Kansas Army National Guard Training Center. The goal of last month's exercise was to identify current gaps in preparedness and response capabilities, and pass on the lessons learned to emergency planners, first responders and other operational personnel, and senior decision-making officials.

The Kansas exercise involved state and local officials from Iowa, Kansas, Missouri, and Nebraska, along with National Guard units and representatives from several federal agencies. It was part of a larger exercise, dubbed Vigilant Guard, that started several days earlier in Iowa.

Despite temperatures that reached about 100 degrees, officials said the Crisis City exercise met their needs admirably. Maj. Gen. Tod Bunting, Kansas adjutant general and the state's emergency-management director, commented that "the weather, bugs, and snakes" that were unplanned elements of the exercise were a "good substitute" for the stress that would be created by a real-life incident. "Events happen on a Friday night when it is dark," he said. "It [the Vigilant Guard exercise] is the kind of training you do not want to do in the middle of town."

Maj. Greg Platt of the Kansas National Guard managed the Salina-based exercise, which he called "a 600-piece puzzle involving mostly city and county emergency responders working side by side." Many of those directly involved were "doing it for the first time … [as part of] a group effort," Platt said.

The Crisis City training site, which covers 40 acres, was built by the Kansas Emergency Management Agency – using $9 million in state funds and $30 million in federal funds – near the Smoky Hill Air National Guard Weapons Range. The exercise was the mock city's first, and was carried out while construction crews were still pouring asphalt for an observation center. In the not-too-distant future there will be venues at Crisis City for responding to agricultural accidents and/or incidents or events involving a vertical tower, an urban village, and a tanker truck – any or all of which could be terrorist targets and/or the scene of a major natural disaster.

Platt said that the training venue should help state agencies improve collaboration and cooperation for the next big Kansas tornado, such as the one in 2007 that almost wiped out the town of Greensburg in the southern part of the state.

State Senator Jay Emler (Republican) said that the unique training opportunities provided at Crisis City could be one way for Kansas to generate revenue – by becoming a regional training site for emergency responders from other states in the region. "There is no doubt we are better [equipped]" to provide such training, Emler said.

Washington, D.C. Hosts "Flu Summit" Chaired by Obama Administration Officials

The nation's school-age children will be a key target population for a pandemic flu vaccine in the fall, and most if not all of them may be vaccinated at school in a mass precautionary campaign not seen since the polio epidemics of the 1950s.

The federal government expects to have an estimated 100 million doses of vaccine available by mid-October, if the current production – by five companies – goes as planned. But the larger supply of vaccine needed for inoculating the 120 million people considered especially vulnerable to the newly emerged strain of the H1N1 "Swine Flu" influenza virus will not be available until later in the year.

Those were among the more important messages administration officials delivered to about 500 state, territorial, city, and tribal health officials on Thursday, 9 July, during a "flu summit" at the NIH (National Institutes of Health) campus in Bethesda, Maryland, just outside of Washington, D.C.

President Obama, speaking by audio link from the Group of Eight summit in L'Aquila, Italy, urged "complete ownership" of preparations for what he said could be a "significant outbreak" of H1N1 flu in the next several months.

"We want to make sure that we are not promoting panic, but we are promoting vigilance and preparation," he said. "The most important thing for us to do," he added, "is to make sure that state and local officials prepare now to implement a vaccination program in the fall."

Children, pregnant women, adults suffering from chronic illnesses, and healthcare workers probably would be first in line for the vaccine, Health and Human Services (HHS) Secretary Kathleen Sebelius told the gathering. Secretary of Education Arne Duncan, who also addressed the group, said that his department "would absolutely welcome" the possibility that the nation's schools serve as a principal venue for delivering the vaccine. The schools are "natural sites" for such a program, he said, and "to open our doors and be part of the solution really makes sense."

In recent years, some public school systems have offered seasonal flu vaccine to students. But there have been no school-based mass campaigns since the late 1950s, when a generation of children lined up to be inoculated with the Salk polio vaccine. How a similar but larger and possibly more complicated 21st-century effort might be accomplished was among the most urgent priorities discussed at this summer's pandemic planning meeting.

Vaccination campaigns, wherever they are held, would be run primarily by local governments. To help the nation's states and cities make their own specific plans, Sebelius said, the federal government will provide an additional $350 million – most if not quite all of it to be disbursed by the end of this month. An estimated $260 million would be allocated to states and territories; the remaining $90 million would be provided to the nation's hospitals to help them prepare for a likely surge of flu patients in their emergency rooms and intensive-care units.

The federal government has spent approximately $1 billion to date on pandemic-flu vaccines, and has about $7 billion available for further purchases and other pandemic countermeasures.

Wisconsin

University Study Suggests H1N1 Virus More Dangerous Than Suspected

In a fast-tracked report published last week in the journal *Nature*, an international team of researchers led by University of Wisconsin-Madison virologist Yoshihiro Kawaoka has provided a detailed, and alarming, portrait of the new pandemic H1N1 flu virus and its pathogenic qualities.

In contrast with run-of-the-mill seasonal flu viruses, the H1N1 virus (better known as the "Swine Flu") exhibits an ability to infect cells deep in the lungs, where it can cause pneumonia and, in severe cases, death. Seasonal viruses typically infect cells only in the upper respiratory system.

"There is a misunderstanding about this virus," says Kawaoka, a professor of pathobiological sciences at the UW-Madison School of Veterinary Medicine, and a leading authority on influenza. "People think this pathogen may be similar to seasonal influenza. This study shows that is not the case. There is clear evidence the virus is different … [from] seasonal influenza."

The H1N1's ability to infect the lungs, notes Kawaoka, is a quality frighteningly similar to those of other pandemic viruses – most notably the 1918 "Spanish Flu" virus, which killed tens of millions of people throughout the world at the end of World War I and in the following two years. There probably are other similarities to the 1918 virus, says Kawaoka, pointing out that the *Nature* study also showed that people born before 1918 still harbor antibodies that protect against the new H1N1 virus. It also is possible, he adds, that the new virus could become even more pathogenic as the current pandemic runs its course – during which time the virus could evolve and mutate to acquire new features. Summer in the northern hemisphere of the world is flu season in the southern hemisphere, and the virus is expected to return in force to the northern hemisphere later this year – more specifically, sometime during the 2009-10 fall and winter flu season.

To assess the pathogenic nature of the H1N1 virus, Kawaoka and his colleagues infected different groups of mice, ferrets, and non-human primates – all of which are widely accepted models for influenza studies – with both the pandemic virus and a seasonal flu virus. They found that the H1N1 virus replicated much more efficiently in the respiratory system than the seasonal flu virus did, and caused severe lesions in the lungs similar to those caused by other more virulent types of pandemic flu.

Last week's *Nature* report also assessed the immune responses of different groups to the new virus. The most intriguing finding, according to Kawaoka, is that those people who had been exposed to the 1918 virus – all of whom are now in advanced old age – have antibodies in their system that neutralize the H1N1 virus.

Kawaoka said that, although the research team found that the H1N1 virus is apparently a more serious pathogen than previously believed – which in itself is a legitimate cause for concern – the new study also indicated that existing and experimental antiviral drugs can form an effective first line of defense against the virus and slow its spread.

There are currently three approved antiviral compounds, according to Kawaoka, whose team tested the efficacy of two of those compounds as well as the efficacy of the two experimental antiviral drugs in mice. "The existing and experimental drugs work well in animal models," Kawaoka said – and that finding suggests, he added, that they also "will work in humans."

Adam McLaughlin is with the Port Authority of NY & NJ, and is the Preparedness Manager of Training and Exercises, Operations & Emergency Management, where he develops and implements agency-wide emergency response and recovery plans, business continuity plans, and training and exercise programs. He designs and facilitates emergency response drills/exercises for agency responders, state and federal partners, and senior Port Authority executives.

