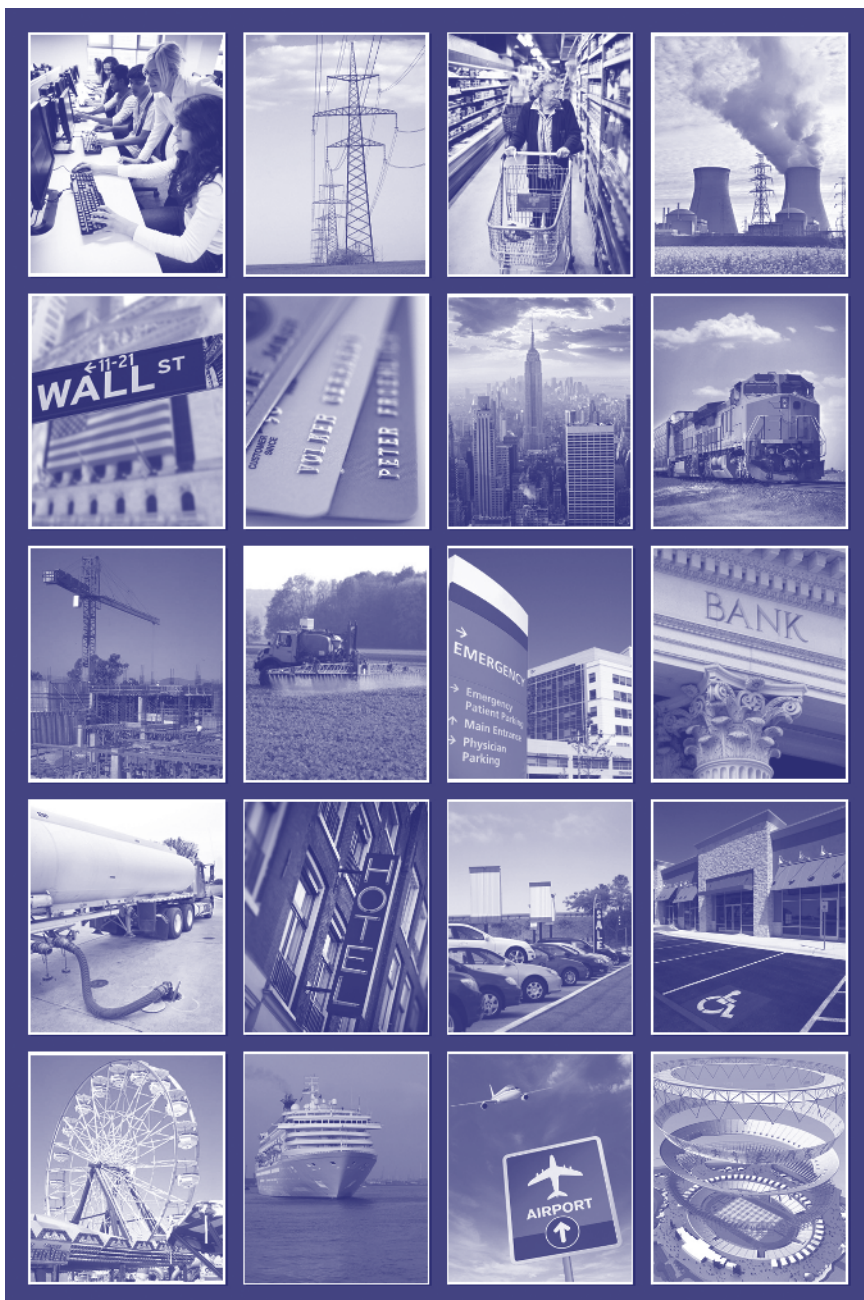


PS-PREP

And Why YOU Should Care!



The Insurance Industry's Role in PS-Prep
By Donald Byrne, CIP-R

Update on Private Sector
Preparedness (PS-Prep) Standards
By Diana Hopkins, Standards

"IT Security for Knuckleheads":
Ten Basic Rules
By Allan Carey, Cyber & IT Security

Monitoring the Monitor:
Additional Breakthroughs Predicted
By Joseph Cahill, EMS

Security Standards to Help
Keep Federal Facilities Safe
By W. Craig Conklin, CIP-R

Public Safety Agencies Fight to
Protect Privacy via Cyber Security
By Rodrigo (Roddy) Moscoso, Cyber & IT Security

Decision-Making in
Chemical Warfare Agent (CWA) Response
By Christopher Wrenn, Senior Director, Sales &
Marketing, Envirionics USA, Case Study

Lessons Learned from
EOCs & Their IT Support
By Sophia Paros, Emergency Management

Florida, Washington D.C.,
Wisconsin, and Michigan
By Adam McLaughlin, State Homeland News

WE REDUCED THE SIZE. NOT THE PROTECTION.

NIOSH
National Institute for
Occupational Safety and Health
CBRN



NH15
ESCAPE HOOD



AVON
PROTECTION

1 888 AVON 440
www.avon-protection.com

Editor's Notes

By James D. Hessman, Editor in Chief



The individual first responder is part of a small group, a government agency or organization, a private-sector business – or even a huge international corporation. The group – volunteers, in many cases – is part of a community in a village, a small town, or a major city, which is a key unit and/or political jurisdiction in a county, a state, and – at the top – a nation.

In today's world, all of these individuals, communities, and political jurisdictions must work closely together – continuously and effectively – to develop, maintain, and expand the local community's, and nation's, emergency preparedness capabilities. Each individual and group will be assigned duties and responsibilities largely separate from another, but also united to form both a massive shield and a strong, unbreakable chain.

Which is largely what this month's printable issue of *DPJ* is all about. Included in the issue are articles by nine working professionals representing a broad spectrum of specialized disciplines that make up the nation's collective and considerably multifaceted domestic preparedness community. Their assigned topics range from broad federally mandated rules to upgrade private-sector preparedness to recent technological upgrades in medical emergency equipment to current (and rapidly expanding) cyber-security vulnerabilities to some practical and much-needed "working tips" for senior managers as well as endpoint users in that same field. Plus several closely related one-pagers by five knowledgeable working professionals.

Donald Byrne and Diana Hopkins start the issue with complementary reports on private-sector preparedness – or, far too often – lack of preparedness, both in the United States itself and internationally. Byrne focuses primarily on the congressional hearings, and subsequent legislation, to improve and vastly expand U.S. private-sector preparedness – and reports that only minimum progress in this area has been achieved in the now almost nine years since the terrorist attacks on 11 September 2001. Hopkins also deplors the minimal gains, but suggests that, after valid and effective national and international standards in this field are finally agreed on, additional progress can and probably will be made. And in a relatively short time frame. Both authors are somewhat but not overly optimistic.

Allan Carey and Roddy Moscoso join forces in: (a) warning about the already immense and still rapidly growing ability of the nation's enemies to breach U.S. public- as well as private-sector cyber security systems; and (b) discussing what can, should, and must be done to remedy current national weaknesses in this area. Carey's article ("IT Security for Knuckleheads") also kicks off what will be a continuing series of "helpful hints" articles for the thousands of point-of-the-spear first responders in *DPJ*'s many-splendored audience.

In the other one-pagers (particularly appropriate for the hot and humid month of August): Joseph Cahill discusses recent upgrades in EKGs, defibrillators, and other medical systems now considered standard equipment – and looks forward to similar breakthrough advances in the foreseeable future. Craig Conklin provides an illuminating report on the massive workload involved in maintaining the physical security of federal facilities – more than 300,000 of them at last count. Christopher Wrenn initiates a four-part series of articles with a skillful synopsis of the major decision-making guidelines involved in developing and promulgating an effective response to chemical-warfare incidents. And Sophia Paros discusses the valuable lessons learned about the effective use of emergency operations centers in events ranging from last year's presidential inauguration to major floods in Iowa and similar disasters in other states. Adam McLaughlin tops off the issue with short but incisive reports on: airport security in Orlando, Florida; the national See Something/Say Something campaign recently launched in Washington, D.C.; and highly successful training exercises carried out earlier this month in both Michigan (anthrax drills for postal workers) and Wisconsin (potential radiation exposure at nuclear power plants).

About the Cover: Multi-Image mosaic, by DPJ Creative Director Susan Collins, showing a carefully selected few of the literally hundreds of thousands of private-sector facilities of all types – all of them potential terrorist targets – that must be protected in the Brave New (but exceptionally dangerous) World of the 21st century. (iStockPhotos)

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

Susan Collins
Creative Director
scollins@domprep.com

Catherine Feinman
Customer Service Representative
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

ASPO-USA Peak Oil Conference

AVON Protection

Bruker Detection

Envionics

ICx Technologies

Idaho Technology Inc.

PROENGIN Inc.

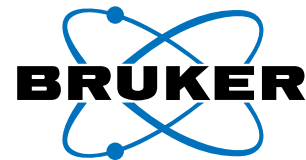
Upp Technology Inc.

© Copyright 2010, by IMR Group, Inc.; reproduction of any part of this publication without express written permission is strictly prohibited.

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.





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

Contributors

First Responders

Kay Goss
Emergency Management

Joseph Cahill
EMS

Glen Rudner
Fire/HazMat

Steven Grainer
Fire/HazMat

Rob Schnepf
Fire/HazMat

Joseph Trindal
Law Enforcement

Rodrigo (Roddy) Moscoso
Law Enforcement

Joseph Watson
Law Enforcement

Medical Response

Michael Allswede
Public Health

Raphael Barishansky
Public Health

Bruce Clements
Public Health

Theodore (Ted) Tully
Health Systems

Adam Montella
Health Systems

Government

Corey Ranslem
Coast Guard

Dennis Schrader
DRS International LLC

Adam McLaughlin
State Homeland News

Infrastructure

Neil Livingstone
ExecutiveAction

Industry

Diana Hopkins
Standards

The Insurance Industry's Role in PS-Prep

By Donald Byrne, CIP-R



This month marks the third anniversary of Public Law 110-53, which was signed into law on 3 August 2007. In response to the 9/11 Commission's recommendations, one provision of the law – Title IX – calls on all private-sector businesses to develop preparedness plans and voluntarily submit them a certification process. However, awareness of that provision has been spotty, even among the insurance industry – a sector singled out to play an active role in the law's promotion.

After disbanding the original 9/11 Commission on 21 April 2004, ten members of the commission announced the formation of the so-called 9/11 Public Discourse Project. The new group's goal was to complete the 9/11 Commission's original mandate – i.e., finding ways to guard the United States against future terrorist attacks. On 5 December 2005, the new group issued its Final Report, which included a "score card" on the initial actions taken by the government (many "Ds" and "Fs" were among the assigned grades) and contained numerous additional recommendations. Among the latter, specific attention was given to the promotion of private-sector preparedness. The final report also called on insurance and credit rating companies to look "closely" at a company's compliance with the ANSI (American National Standards Institute) standard "in assessing ... [the company's] insurability and creditworthiness."

Over the past three years, some progress has been made, but full implementation of the program, now known as "PS-Prep" (Private Sector Preparedness), has not yet been achieved. The Department of Homeland Security (DHS) has much of the required infrastructure in place, however, and has held a series of public meetings to solicit feedback. Nonetheless, public support among the business community remains tepid. In fact, a recent Gartner Group forecast on PS-Prep predicts that, by 2012, "less than 10 percent of end-user enterprises will have obtained external certification for their BCM [business continuity management] and IT [information technology] disaster recovery programs."

ANSI, ANAB, and IBHS: Incremental Progress

The ANSI National Accreditation Board (ANAB), which was awarded the DHS contract to oversee the certification process, has announced, though, that it will begin accepting applications for the PS-Prep program by 1 September 2010. Scott Richter, the ANAB'S director of Planning and Development, said that he has spoken "to six to eight certification bodies interested in the PS-Prep program" and expects that twelve to fifteen organizations eventually will apply "to certify companies to the PS-Prep standards." After this phase of the program is in place, marketing by certification firms can begin and public awareness may well increase.

One group that responded to the DHS call for comments is the *Institute for Business & Home Safety* (IBHS), a nonprofit organization headquartered in Tampa, Florida, and funded by hundreds of insurance and reinsurer companies. Debra Ballen, IBHS general counsel and senior vice president of public policy, has met with DHS on more than one occasion to discuss PS-Prep.

IBHS has expressed support for the program, and Ballen has urged DHS itself to “do more to advance an understanding that preparedness is not just about terrorism. Businesses need to pay attention to the areas that are responsible for most losses during times of natural hazards such as building construction and equipment. While concern over terrorism is well founded, companies need to develop a culture of preparedness that takes an all-hazard view if they are to achieve resiliency.”

When asked about the current visibility of the PS-Prep program, Ballen answered that there is “a much greater awareness of the program among large companies” – but more work “needs to be done,” she continued, “to educate people in the small and mid-size markets.”

A similar opinion was expressed by Charles Sidoti, vice president of risk control at OneBeacon Insurance of Canton, Massachusetts. “The cost of insurance reflects the everyday risks companies face,” he said. “Insurance companies welcome any initiative that encourages better preparedness, but the program has to reflect the realities of business and should include guidance on how to prioritize and cope with risks ranging from pandemics to accidental fires.”

Congressional Encouragement, But New Obstacles Still Loom

One provision of the charter given to DHS by Congress calls for development of a business case that encourages participation in the PS-Prep certification process. Initially, some outside the insurance industry called for premium discounts for organizations that earned a certification. That argument was quickly dispelled once they understood that insurance premiums are usually based on analysis of historical claims.

“We don’t have enough information to make a decision on whether or not having a preparedness plan leads to fewer claims,” Sidoti pointed out. “Besides, there is no set price

for insurance. Every business and every building is unique in some way, and decisions are made on a case-by-case basis. If your business has a plan, make that known to the underwriter and factor it into your price negotiations, but there can’t be a set discount because there is no set price.”

Two markets highlighted in the PS-Prep legislation but not yet addressed by a DHS plan are: (a) smaller businesses;

and (b) the industry sectors designated as Critical Infrastructure and Key Resources (CIKR). The 18 CIKR business sectors, which range from financial institutions and nuclear power plants to national monuments and electrical grids, pose a special challenge to the PS-Prep program. DHS has announced, though, that it is working on a way to blend the preparedness requirements mandated by the existing regulatory environment with the standards being used by PS-Prep.

Small businesses pose a challenge of another sort. Given the extreme price sensitivity of most small business, few of these companies are expected to voluntarily spend resources on certification without a tangible return. “Making the case to small business is a real challenge,” said Ballen. IBHS offers a free tool – i.e., Open-for-Business® – that allows small and medium companies to quickly put together a preparedness plan,

but only a relatively small fraction of American firms are using it.

“Our industry is supportive of any initiative that educates the public and gets them better prepared. But we also realize that PS-Prep is really the beginning of the process of preparedness, not an end,” said Ballen.

Donald Byrne is the Managing Director of North River Solutions and has been involved with the PS-Prep program from its inception. A certified Lead Auditor, CBCP, and data center expert, he teaches graduate courses at Boston University and writes for the news website www.continuitycompliance.org. He can be found at Linked In and followed on Twitter @Don_Byrne.

On 5 December 2005, the new group issued its Final Report, which included a “score card” on the initial actions taken by the government (many “Ds” and “Fs” were among the assigned grades) and contained numerous additional recommendations; among the latter, specific attention was given to the promotion of private-sector preparedness

Update on Private Sector Preparedness (PS-Prep) Standards

By Diana Hopkins, Standards



Although activity on the DHS (Department of Homeland Security) Private Sector Preparedness (PS-Prep) initiative appeared to have lagged a bit following the last stakeholder meeting in November 2009, efforts were stepped up following the April 2010 Gulf oil spill. British Petroleum's apparent lack of disaster preparedness prompted the chairmen of both the Senate Homeland Security & Governmental Affairs Committee and the House Committee on Homeland Security to jointly nudge DHS and the Federal Emergency Management Agency (FEMA) to move faster on the development of more effective controls and improved standards of operation for private-sector businesses – more specifically, on development and implementation of the PS-Prep standards.

Prior to 15 July 2010, there were no DHS-adopted standards by which U.S. businesses and other private sector entities could develop and properly assess their preparedness for all hazards – preparedness that could, among other things: (a) reduce the impact of all hazards; (b) protect employees; and (c) help ensure business recovery following a crisis. The private sector includes companies, facilities, hospitals, stadiums, businesses, universities, and non-profit organizations – which collectively own and are responsible for an estimated 85 percent of the nation's critical infrastructure and other material resources. Those resources are vital to disaster preparedness and response capabilities and to enhancing the nation's readiness and resiliency capabilities. It is therefore critical to homeland security that the private sector be well versed on how to prevent, endure, and mitigate crisis situations.

In 2004, the 9/11 Commission recognized the need for private sector preparedness standards, and endorsed the use of NFPA (National Fire Protection Association) 1600 as the National Preparedness Standard. Three years later, though, in 2007, Congress recognized that not all of the 9/11 Commission recommendations were being met, and for that reason mandated that DHS develop and implement a voluntary program of accreditation and certification of private entities – using preparedness standards adopted by DHS.

Relevant Standards, Consensus Approval, Timely Certification

The purpose of the new program would be to enhance nationwide disaster response and recovery capabilities

by encouraging and facilitating private sector preparedness. Public Law 110-553 was passed, entitled Implementing Recommendations of the 9/11 Commission Act. Title IX of that Act established The Voluntary Private Sector Preparedness Accreditation and Certification Program (PS-Prep) – which, among other things, creates a partnership between DHS and the private sector that can be used to reach consensus on preparedness standards relevant to all stakeholders.

The PS-Prep program involves several parts, including: (1) the solicitation, development, and consensus approval of private sector standards by government and private sector stakeholders; (2) the development and DHS approval of a system for certifying private sector conformity to approved standards; and (3) implementation of the standards by the private sector, and of the certification program by accredited certifiers.

In July 2008, DHS selected the ANSI-ASQ National Accreditation Board (ANAB) as a sole-source accreditation body to support, develop, and oversee implementation of the voluntary Private Sector Preparedness Certification Program, which is based on ANAB's unique experience as the U.S. accrediting body for the voluntary certification programs for quality and environmental management systems which in turn are based, respectively, on the ISO (International Standards Organization) 9001 and 14001.

An Extended But Deliberately Reiterative Process

Six months later, in December 2008, the DHS's target criteria for private sector preparedness standards were published in the Federal Register as Notice 73 FR 79140. In that notice, DHS introduced the PS-Prep program and, as required by law, solicited preparedness standards from stakeholders, and also requested their comments on implementation of the program.

DHS then engaged with its private sector partners through a series of additional Federal Register notices, public meetings, and other initiatives, gathering stakeholder comments and incorporating them into all aspects of the PS-Prep initiative. Since the December 2008 Federal Register notice, DHS also has engaged the public on programmatic issues through yet another series of Federal Register Notices, public meetings

and other interactions with private sector firms, associations, and other entities. In all, 25 preparedness standards were submitted, 21 of them by the private sector, for consideration as the final standards recommended for DHS adoption. Finally, in October 2009, DHS announced – also via the Federal Register – its intent to adopt three of the PS-Prep standards that had been submitted, each comprehensively dealing with preparedness in a fashion that was both relative and realistic to most private sector entities. That announcement was followed by another series of regional public meetings, and public comments from stakeholders on the three standards were incorporated into the final documents.

Eight months later – more specifically, on 15 June 2010, with the Gulf oil spill debacle pressuring completion of the initiative – FEMA announced that the three PS-Prep standards had been approved for use by the private sector for disaster preparedness and recovery. The three standards are:

- ASIS International SPC.1-2009 *Organizational Resilience: Security Preparedness, and Continuity Management System – Requirements with Guidance for use (2009 Edition)*. This standard is available at no cost.
- British Standards Institution (BSI) 25999 (2007 Edition) – *Business Continuity Management (BS 25999:2006-1 Code of practice for business continuity management, and BS 25999: 2007-2 Specification for business continuity management)*. Both parts of this BSI standard are available for \$19.99 each.
- National Fire Protection Association 1600 – *Standard on Disaster/Emergency Management and Business Continuity Programs, 2007 and 2010 editions*. This standard also is available at no cost.

With the PS-Prep standards now approved, ANAB plans, over the next several months, to manage the accreditation of third party certification organizations to carry out PS-Prep certifications in accordance with accepted procedures of the

program, and is already prepared to accept confirmation from certification bodies to participate in the program.

Meanwhile, ANAB has worked closely with DHS and FEMA over the last two years to develop accreditation procedures, recommended by a Committee of Experts formed by ANAB, for the PS-Prep program, and expects to complete that task sometime next month. Certification will serve

as confirmation that an accredited third party certification organization has validated a private sector entity's conformity to one or more of the three approved preparedness standards listed above. Private sector entities that choose to use these standards may apply for certification – and, once certified, will undergo periodic reassessment and auditing to ensure their continued conformity. DHS will publish a list of all PS-Prep certified private sector entities that ask to be listed. FEMA Administrator Craig Fugate is the Designated Officer of the PS-Prep program and serves as Chair of the Private Sector Preparedness Coordinating Council. He and the council members are responsible for monitoring the effectiveness of the accreditation and certification program on an ongoing basis.

In 2007, Congress recognized that not all of the 9/11 Commission recommendations were being met, and for that reason mandated that DHS develop and implement a voluntary program of accreditation and certification of private entities – using preparedness standards adopted by DHS

Note: Although three PS-Prep standards have been selected and are DHS-approved, FEMA continues to solicit comments on the new PS-Prep initiative. Comments may be submitted to <http://www.regulations.gov> or FEMA-POLICY@dhs.gov in Docket ID FEMA-2008-0017. For additional information, stakeholders are encouraged to visit <http://www.fema.gov/privatesectorpreparedness/>.

Diana Hopkins' consulting firm "Solutions for Standards" (www.solutionsforstandards.com) focuses on helping businesses navigate the complex standards development process. 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 emergency management. 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 and governance as well as process development and improvement.

They Expect You To Be More Than 80%* Prepared for a Biological Threat



Now You Can Be with the New **RAZOR™ EX**



RAZOR EX

Field Portable BioHazard Detection System

Less than 1% error rate

Screen ten targets in a single run with The 10™ Target Kit

Used by Military, Hazmat, and First Responders

The 10™ Target Screen Kit:

Anthrax	<i>E. coli</i> O157	<i>Salmonella</i>
<i>Brucella</i> spp.	Tularemia	Smallpox
Botulism	Ricin	Plague
<i>Coxiella</i>		



Call **1.800.735.8544** or visit www.idahotech.com to discover how to reliably protect those you serve.

*Most other field biohazard detectors have a 20% error rate.

“IT Security for Knuckleheads”: Ten Basic Rules

By Allan Carey, Cyber & IT Security



Cyber security has reached a heightened level of attention both in the media and in the minds of U.S. citizens. When household names openly admit that they have been compromised by sophisticated adversaries, it gives the American public an uneasy sense of vulnerability. If it can happen to those large organizations, the thinking goes, it can easily happen to the average person surfing the Internet as well. Beyond awareness, the media attention has also caused a significant amount of confusion not only about what constitutes a cyber threat, but also what non-government as well as government organizations and agencies should be doing to improve and protect their cyber security systems and overall readiness.

What many citizens do not fully comprehend – this generalization also applies to many senior leaders of both public and private organizations – is the level of sophistication and complexity that already has been achieved by the nation’s cyber adversaries. In fact, an attacker “supply chain” has developed that is analogous in many respects to how the illegal drug industry works: One group focuses on developing malware, another is responsible for and effective in quality assurance, yet another acts as the “trusted broker” between supplier and buyer, and the buyer specializes in developing and implementing exfiltration strategies. When large quantities of data – e.g., credit card numbers, healthcare records, and other personal-identity information – are stolen, the data is broken down into smaller units and sold to groups that use the information for illegal, larcenous, and sometimes dangerous actions against private citizens and public officials alike.

Greater in-depth understanding of the global “underground” cyber economy and its participants can be found in *Fatal System Error* by Joseph Menn. The bottom line is that, if an organization – whether it is a government entity providing critical citizen services or a commercial enterprise – possesses

valuable information, someone, or some group, will go after that information.

Advance Planning, Total Awareness & Meticulous Attention to Detail

Despite existing in an increasingly hostile and dangerous environment, many public as well as private organizations and agencies still lack the basic fundamentals of a sound information security program. Following are 10 common-sense mandates [“IT Rules for Knuckleheads,” as one observer put it] that can and should be promptly developed, and fully implemented, in almost any type of organization to help prevent and detect threats to that organization’s most critical operations.

The bottom line is that, if an organization – whether it is a government entity providing critical citizen services or a commercial enterprise – possesses valuable information, someone, or some group, will go after that information

1. Accept the fact that an organization *will* be compromised at some time or another. This is not fear, uncertainty, and doubt, but a statement of fact – backed by industry research and public datasets. There is virtually no doubt that a security breach will happen at some point in time – which means that the appropriate detection and response systems and processes must be in place – beforehand.

2. Know both the business risks and the areas where the data is stored. Before developing a security strategy, there must be a baseline of the risk posture needed, as well as conversations with management to determine what risks

may be acceptable and which ones require mitigation steps. In addition, the types and amount of data on the network must be understood. Many organizations do not segment and/or compartmentalize their most sensitive information from other information that might be considered either public or at least less critical. Extra effort in this area will pay lasting dividends so that additional resources can be properly applied both to the systems themselves and to the data that matter most to the organization.

3. Using a baseline risk assessment, develop both an information security policy and the operational procedures needed to implement that policy – which should be designed to cost effectively: (a) reduce risk to the organization; and (b) ensure compliance with any applicable requirements.
4. Develop a complete inventory of every asset on the network, including the applications running on those systems. Unfortunately, relatively few U.S. organizations, public or private, now have effective asset inventory and management systems in place – despite the fact that it simply is not possible to prepare an effective defensive stance or response effort if the systems that could be potential openings to compromise are not recognized.
5. Patch vigilantly, and implement effective configuration and change-management processes. Operations and systems depend on software functioning properly and being patched in a timely manner. A healthy patch-management program is one of several possible layers of defense that can help guard against known vulnerabilities.
6. Employ effective access controls – both to restrict access to computer programs and data, and to prevent and detect unauthorized access. A workable procedure for assigning user access rights and permissions should be in place, with periodic reviews of access rights and permissions scheduled, and carried out, to ensure that individual access, which should be granted on the basis of job responsibilities, remains appropriate.
7. Use “endpoint” protection technology as another layer of defense. Endpoints – e.g., desktops, laptops, and mobile devices – are typically the main entry point for attackers and malware into a network. Much if not quite all current anti-virus technology has been commoditized and is frequently ineffective. However, most organizations have moved toward policy-enforced endpoint security suites that integrate several technologies into a single system for simplicity.
8. Develop a more effective network monitoring capability to give the network a memory. Many and perhaps most intrusion-detection and other signature-based approaches do not detect the most serious network attacks. To cope with today’s threat environment, the data will have to be not only recorded, but also analyzed for post-incident forensics and real-time situational awareness – as well as, not incidentally, for predicting potential future intrusion scenarios and the development of preventive countermeasures (similar to those used in business-continuity planning and disaster-recovery exercises).
9. Also have in place a solid incident-response plan and capability, either in-house or through an external provider, to swiftly and efficiently: (a) remediate any cyber incident; and (b) collect forensic evidence. (This step probably does not have to be mentioned to preparedness professionals, but it *does* have to be reinforced.)
10. Educate end-users on the risks posed by cyber threats. Also, enable them to make informed decisions when performing their jobs, and to act responsibly when using the Internet. Human error – e.g., clicking on email attachments from unknown sources, and visiting infected websites – and social engineering are quite possibly the biggest threats to an effective information security program. In ways somewhat analogous to those used in other domestic preparedness and response scenarios, users must know how to act, quickly and effectively, and react in the cyber realm.

By implementing a sound information security program, backed by an easily understood and enforceable policy, preparedness professionals and their organizations will be in a much better position to defend against cyber attacks. Armed with both factual knowledge and operational intelligence, a level of situational awareness and confidence can be achieved to answer the truly difficult security questions such as “Did we have a breach?” and “Was there any data lost?”

Allan Carey, a Director with NetWitness, has 10 years of information-security industry experience from serving as senior vice president (research and product development) of IANS and program manager of security services of IDC. He also has been a professional advisor to a number of Fortune 1000 organizations, providers of security technologies and services, and various financial-community companies through in-depth market analyses, industry intelligence, and consulting.

HAZMAT IDENTIFICATION. IN THE PALM OF YOUR HAND.



Ground-breaking Raman technology in an affordable, palm-size instrument for rapid identification of unknown materials.

Fido® Verdict™ provides real-time, accurate identification of unknown liquids, powders and solids for HazMat professionals. With Verdict, the capabilities of Raman technology are available in an easy to use, miniaturized system at an affordable cost. Hazardous materials identification is now within reach for the entire first responder community.

Contact ICx Technologies at 1-877-692-2120 for more information on Verdict and the Verdict HazMat-CB Responder Kit which includes enzyme-based chemical agent tests and bio-assay strips for a comprehensive chem bio solution.

www.icxt.com

NEW THREATS.
NEW THINKING.®

icx[®]
technologies

Monitoring the Monitor: Additional Breakthroughs Predicted

By Joseph Cahill, EMS



The cardiac monitor is a device that displays a patient's electrocardiogram (EKG) or heart rhythm as a thin line of light with a peak showing at each heart beat. The defibrillator is a device that sends a charge of electricity through the heart to re-set its rhythm.

Ten years ago, the future of these devices was, in a word, “modularity.” Each and every device was fitted with the basics – and, if an additional capability was needed, a technician simply opened the device, plugged in a circuit board, and uploaded software. Meanwhile, the users picked up and plugged in a new cable, and they were back in service with improved capability. This made the devices of a decade ago considerably robust and in most if not all cases allowed them to avoid obsolescence. Today, though, there is a new future: “connectivity.”

There are different needs within the various types of medical and responder systems involved. First responders such as firefighters, police officers, and basic life support (BLS) ambulances, for example, are equipped with semi-automatic defibrillators, and many public buildings have automated defibrillators in place as well. These devices record and analyze a patient's/victim's heart rhythm and deliver a shock of electricity as and when needed. Paramedics and emergency room staff use more advanced devices.

Clot Busters + Long-Distance Connections = Improved QA

During a heart attack, a clot restricts the flow of blood to the heart muscle. “Clot-buster” medications, which dissolve the clot and restore the flow of blood, usually provide an effective treatment. However, because heart muscle is damaged so quickly, time is often the determining factor not only in a patient's survival but also for his or her continued quality of life.

When clot busters were first introduced, hospital personnel worked long and hard to increase the speed in which the drug was administered. By connecting the paramedic in the field to the hospital, this time was significantly reduced.

Many EMS systems have been using electronic ambulance reports for more than a decade. These reports often can be downloaded and/or printed out at the hospital. Ideally, the system should be able to take the ambulance report and connect the patient's biotelemetry data from the monitor directly to it, making a complete package.

Having this record in hand – combined with all of the data recorded for the patient and stored in a central location – allows more effective system management, in a number of ways. Improved quality assurance (QA) is achieved at both the system level and the individual paramedic level. This allows not only more effective corrective action with the individual patient but also improved planning for later system-wide training and/or adjustment.

Some systems also have the ability to record and transmit data on the specific device being used; that capability allows technical services staff to keep the equipment at top performance.

Today, Tomorrow, and Just Over the Horizon

All of the preceding is available right now. The future holds even greater promise, though, and the next great leap forward probably will mirror the current explosion in, and derived from, smart cellular technology, with each component connecting through the air to the rest. The first firefighter on the scene, for example, uses a device to upload his/her data, which is then joined with the data provided by the paramedics and the hospital.

This capability provides more effective use of not only current EKG monitors and electronic reports, but additional devices as well. Responders at each link in the chain of medical care are able to review the information collected in all previous steps – and then add to it. Instead of individual reports, there is a stream of data that can be viewed as a medical timeline, in much the way patient information already is recorded in most hospitals and other medical facilities.

The technology already exists to have these devices communicate: (a) on scene, using low-energy wireless such as bluetooth; and (b) long range – to the hospital and/or central server by cellular connection (in the same way that a smart phone connects to the Internet). Fortunately, the manufacturers of current monitoring systems have made their software “open source,” which means that they provide the computer code so that other programs can use it. This allows the manufacturers of other products – e.g., electronic ambulance reports – to design their products to interface with the monitor-technology products.

The last generation of medical monitors became “more than mere EKG machines.” The next generation is very likely to be “more than just a single machine.”

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.

Security Standards to Help Keep Federal Facilities Safe

By W. Craig Conklin, CIP-R



Not quite four months ago, the Interagency Security Committee (ISC) – which is chaired by the Department of Homeland Security, National Protection and Programs Directorate’s (NPPD), Office of Infrastructure Protection – released

two publications related to the interim federal facility security standards designed to keep the nation’s more than 300,000 non-military federal facilities safe and secure.

Those publications – the *Physical Security Criteria for Federal Facilities*; and the *Design-Basis Threat Report* – are the most comprehensive federal facility security standards created to date, and establish baseline physical security measures that: (a) are innovative; (b) bolster protection against terrorist attacks and other threats; and (c) reflect the extensive subject matter expertise of the ISC itself and its individual members.

The ISC, which is composed of chief security officers and other senior executives from 45 federal agencies and departments, works to enhance the quality and effectiveness of physical security, and to protect buildings and civilian federal facilities throughout the United States.

Physical Security Criteria – A Single-Standard Approach

The *Physical Security Criteria for Federal Facilities* (PSC) is a compendium of standards designed to provide consistency throughout and across the large number of preexisting standards related to facility security. In addition to consolidating existing standards, the new document establishes a baseline set of physical security measures both to be applied to all nonmilitary federal facilities and to serve as a framework to tailor the measures to the unique risks and requirements of each facility.

“The release of the *Physical Security Criteria* represents an important milestone for the federal government,” said Austin Smith, ISC executive director. “The PSC is the culmination of 15 years of work and the coming together of 45 departments and agencies to mitigate security threats to our federal workforce in this modern age of terror.”

The standards apply to all buildings and facilities within the United States that are occupied by federal employees for

nonmilitary activities. Included in the PSC compendium are: existing buildings, new construction, and buildings undergoing major modernizations; facilities already owned – or expected to be purchased or leased; stand-alone facilities, federal campuses, and, where appropriate, individual facilities on federal campuses; and special-use facilities.

The DBT Report, Validation & Final Publication

The ISC’s interim *Design-Basis Threat (DBT) Report* is a stand-alone threat assessment designed to be used in conjunction with the *Physical Security Criteria* compendium. The DBT establishes a profile of the type, composition, and capabilities of various adversaries; the profile can then be used to inform the design of countermeasures called for in the PSC compendium.

The DBT, which provides an estimate of the threats to federal facilities across a range of undesirable events, is based on intelligence information, reports, assessments, and crime statistics available to the working group at the time of publication. It will be updated, as needed, to ensure that facilities are considering and responding to evolutions in the threat environment.

The next steps forward for the new standards will be a 24-month validation period – which will include field testing and implementation by nonmilitary federal facilities – after which the ISC will publish final versions of both documents

For additional information:

On the ISC and federal facility standards, visit www.dhs.gov/isc
About critical infrastructure protection, www.dhs.gov/criticalinfrastructure

W. Craig Conklin, director of the Sector-Specific Agency Executive Management Office with the Department of Homeland Security’s Office of Infrastructure Protection, is responsible for implementing the private/public sector partnership model defined in the National Infrastructure Protection Plan for six critical-infrastructure key resource sectors: chemical, commercial facilities, critical manufacturing, emergency services, dams, and nuclear. He also is responsible for the Interagency Security Committee (ISC), which was established in response to the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City. The ISC is charged with developing security standards for all non-DOD (Department of Defense) buildings housing federal employees. Mr. Conklin has approximately 30 years of experience in emergency preparedness and response, Navy nuclear propulsion programs, the commercial nuclear power industry, and the federal government.



A single solution for all your needs



From emergency management, mass casualty evacuation and patient tracking to day-to-day asset, resource and inventory management, irms|360™ Enterprise is the only proven integrated management solution for statewide public health and public safety.

The irms|360 Enterprise application framework is designed to be scalable, interoperable and highly available, providing federal, state and local agencies a comprehensive solution suite for tracking critical supplies, people and processes.

Asset
Management

Clinic
Management

Emergency
Management

Patient
Management

Vaccine
Management

Warehouse
Management

Public Safety Agencies Fight to Protect Privacy via Cyber Security

By Rodrigo (Roddy) Moscoso, Cyber & IT Security



U.S. public-safety agencies have long been entrusted with protecting sensitive information collected from, and/or about, the general public. From traffic citations to the details of juvenile crime, law enforcement organizations are required to ensure that criminal records, as well as data collected as part of their own day-to-day operations, are well protected.

Today, because so much of the data collected is now in an electronic format, the mechanisms of protection have, in many cases, moved from lock and key to “user name and password” and other Cyber Security measures. The rapid migration and accumulation of such data necessitates new strategies, policies, and infrastructure designed specifically to protect sensitive public safety records. These efforts must also address new and changing privacy rules, as well as entirely new forms of data that require protection – and which may require new access and use restrictions.

Last month – more specifically, on 14 July – the Cyber Security Coordinator and Special Assistant to the President, Howard Schmidt, hosted a White House meeting to discuss the status of Cyber Security efforts across various levels of government and in the private sector. The meeting addressed several of the key issues involved, with special focus on the draft National Strategy for Trusted Identities in Cyberspace (NSTIC), which calls for, among other things, the creation of “an online environment where individuals can voluntarily choose to obtain a secure, interoperable, and privacy-enhancing credential from a variety of service providers – both public and private – to authenticate themselves online for different types of transactions.” That type of solution, Schmidt pointed out, is critical to ensuring that the “right people access the right data.”

GFIPM, Global Justice, GPS, and LPRs

One example of enhanced credentialing is the Justice Department’s Global Federated Identity and Privilege Management (GFIPM) initiative, which establishes a standardized credentialing framework for the justice community that is designed to improve access security while at the same time allowing more information to be shared. GFIPM is also designed to reduce the administrative burden on numerous government agencies and other data “owners” by: (a) automating the authentication process; and (b) implementing “single sign-on” solutions (where possible). GFIPM is based on Global Justice XML and NIEM (National Information Exchange Model) usages and provides a standard mechanism to share and exchange both user identities and authentication privileges.

Although enhanced authentication will provide secure and more efficient access to public safety datasets, the technology used must keep pace not only with new privacy laws but also with the evolving interpretations of what types of data require special protection, including judicial approval for access. Earlier this month, however – on 6 August – the U.S. Court of Appeals for the District of Columbia ruled that the use of global positioning system (GPS) location data that had been collected by law enforcement officers – who had surreptitiously (and without warrant) planted a tracking device on a vehicle used by two drug suspects – had violated the suspects’ expected right to privacy under the Fourth Amendment. Data collected from the device was a key factor in the conviction of one of the suspects – but the Court overturned that conviction.

The Court of Appeals ruling may have implications for public safety’s use of tracking and location data, which in many jurisdictions is now automatically – and continuously – being captured by an ever-growing number of license plate readers (LPRs). Many states have installed and are using these systems for law enforcement and other purposes, and one result is a growing volume of data being amassed on the movement of vehicles. Although such information is, or could be, a major boon to law-enforcement investigations and crime analysts, access to that data must obviously be very tightly controlled. In large part for that reason, the International Association of Chiefs of Police last year issued a Privacy Impact Assessment about the use of LPR that provides valuable insights and recommendations for public safety agencies on issues related to the collection and use of LPR data.

As the types and quantity of data collected by public safety agencies continue to grow, the security and protection of the data must be correspondingly enhanced. The new datasets being accumulated are too valuable not to be used in support of law-enforcement investigations. That said, however, it also should be emphasized that privacy concerns are equally important – particularly for the purpose of maintaining public trust. Abuses in providing access to such data, and/or a lack of adequate cyber security protection, could erode and perhaps even eliminate that accumulated trust and result in the imposition of politically driven limits on the use of such important information.

Rodrigo (Roddy) Moscoso currently serves as Communications Manager for the Capital Wireless Information Net (CapWIN) Program at the University of Maryland. Formerly with IBM Business Consulting Services, he has over 15 years of experience supporting large-scale IT implementation projects, and extensive experience in several related fields such as change management, business process reengineering, human resources, and communications.

Decision-Making in Chemical Warfare Agent (CWA) Response

By Christopher Wrenn, Senior Director, Sales & Marketing, Environics USA, Case Study



This is the first of a four-part series on Chemical Detection and Decontamination for Multiple Applications.

When it comes to detection and decontamination, many factors play a role in the decision-making process. This four-part series has been created to not only provide important information on the equipment itself, but also to discuss the basics of various chemicals and their effects. In response to releases of CWA, there may not be one technology or one “answer” that is correct.

The responder must take into account all of the clues to determine the presence or absence of CWAs in order to take appropriate action. The first part of this series is titled “Decision-Making in Chemical Warfare Agent (CWA) Response” (AP-102). This article describes the clues to look for in CWA response and how to layer them with the various CWA detection technologies available. The physical clues related to CWAs include where they come from, how they behave, and how they are disseminated. It is also important to note biological indicators, including animals and human victims.

This article also discusses location, classification, and identification technologies, as well as the pluses and minuses of each one – e.g., simulants for these technologies and the cost of ownership for each one. Finally, this article presents strategies for layering the physical and biological clues with the location, classification, and identification clues to come to the right conclusions when responding to a CWA incident.

While the Environics ChemPro100 was designed as a Chemical Warfare Agent (CWA) “classifier” for military applications (“Decision-Making in Chemical Warfare Agent Response,” Environics Application Note AP-102), it has the added versatility to be used for a wide variety of HazMat applications like “sniffing” and decontamination (“The ChemPro as a Decontamination Tool,” AP-104), Clan Lab interdictions (“Orthogonal Detection for More

Complete Protection from Clandestine Methamphetamine Lab Chemicals,” AP-101), and even firefighting overhaul activities (“Orthogonal Detection for More Complete Protection from Toxic Gases and Vapors in Overhaul Operations,” AP-103).

Christopher Wrenn is the Sr. Director of Sales and Marketing for Environics USA, a provider of sophisticated gas & vapor detection solutions for the military, 1st responder and safety markets. Previously Mr. Wrenn was a key member of the RAE Systems team. Chris has been a featured speaker at more than 20 international conferences and has written numerous articles, papers and book chapters on gas detection in HazMat and industrial safety applications.

Environics Application Note: 102
Decision-Making in Chemical Warfare Agent (CWA) Response

In response to releases of Chemical Warfare Agent (CWA), there may not be one technology or one “answer” that is correct. The responder must take into account all of the clues present and take appropriate action. Understanding what the clues are and how to layer them when a decision is critical to successful CWA response.

Why is Gas Detection Important?
Responders cannot rely on their senses for how to use detection techniques. Responders are unable to properly identify threats and actual hazard. Detection technologies supplement responders senses when making decisions in potentially hazardous environments. Relying on the senses alone can be dangerous in chemical response; detectors become the eyes and ears when those senses fail. Proper use of detection technologies coupled with the clues present at the scene allow for better decision making.

Over-Responding Can Be Dangerous to the Community
Over-responding can be dangerous to the community because panic is as effective a killer as bullets, bombs, or chemical attacks. The community will echo how the first responders act accordingly. If the first responders over-react and immediately jump into full encapsulation protection, it could panic the public and cause unnecessary worry and even injury.

Overprotection Can Be Dangerous to the Responder
Heat stress is the number one injury in HazMat response and immediately jumping into full Level A encapsulation is a good way of overheating oneself. Level A encapsulation also makes one much more susceptible to slip, trip, and fall injuries. Finally, overprotection makes it harder to get things done. When properly used, detection allows responders to respond at lower levels of personal protective

Why Worry About CWAs?
CWAs are chemicals designed to either kill or debilitate an opposing military. They are often derived from civilian Toxic Industrial Chemicals (TICs) such as insecticides, chlorine, and hydrogen cyanide. In 1994, the Japanese cult Aum Shinrikyo released a Sarin spray from a refrigerated box truck in a quiet neighborhood of Matsumoto Japan with the intent to kill three judges who were due to rule against the cult. Seven people were

CWA Response is a 3-Step Process

- 1. Location:** One needs to quickly figure out where the problem is coming from using clues, common sense, and survey tools. Victims running from a central liquid all provide location clues. Survey technologies like Photoionization and Flame Ionization Detectors (PIDs and FIDs) also can help in location.
- 2. Classification:** One needs to quickly get a general idea of the kind of threat by using clues, common sense, or colorimetric techniques, Ion Mobility Spectroscopy (IMS), Surface Acoustical Wave (SAW), or Flame Spectrophotometry. In the case of CWAs, at this stage, it is not necessary to differentiate between Soman (GA) or Sarin (GB) because the initial response protocol is the same.
- 3. Identification:** Using clues, common sense, or an instrument, the specific identity of a chemical or a mixture of chemicals can be determined. This can be helpful in further prosecution and will include Fourier Transform InfraRed Spectroscopy (FTIR) and Gas Chromatography/Mass Spectroscopy (GC/MS).

Copyright © 2010 Chris Wrenn
Environics USA, Inc.
1308 Continental Drive, Suite 2, Ashington, MD 21009
Tel: (410) 612-1250, Fax: (410) 612-1251
sales@environicsusa.com www.environicsusa.com
Page 1 of 10

Click to Download Full Report

Lessons Learned from EOCs & Their IT Support

By Sophia Paros, Emergency Management

Whether dealing with a natural disaster, severe weather incident, or the election of the nation's first African American president, all potential "incidents" require information technology (IT) support and a real-time information portal for first responders.

In 2008, then-Senator Barack Obama was elected as the nation's 56th president, and on 20 January 2009 he became the first African American to serve in that post. Emergency managers and first-responder agencies in the greater Washington, D.C., area anticipated record crowds – an estimated 2-5 million people – for the three-day program of inaugural events, and recognized that maintaining security from start to finish would be a major challenge. The District's Homeland Security and Emergency Management Agency (DC HSEMA) served as the lead District agency to plan and coordinate the city's resources from multiple agencies and jurisdictions.

One of the many challenges that faced emergency managers was how to collaborate and coordinate their response and management efforts both timely and effectively. WebEOC, a Web-enabled crisis information management software tool, was employed by DC HSEMA to distribute information to National Capital Region (NCR) partners through the portals' message boards. Emergency responders, police officers, and other personnel were able to upload field reports, share important data, and detail real-time information on the Inaugural operations, events, and priorities, all via WebEOC.

Access to the WebEOC portal not only gave NCR partners the tools they needed to stay attuned to all operational activities, but also enabled them to adjust staffing and planning efforts to meet changing situations spelled out in live reports posted on the message boards. By and large, NCR partners found the WebEOC tool both useful and necessary to their efforts. The *2009 Presidential Inauguration Regional After-Action Report* – available on *Lessons Learned Information Sharing (LLIS.gov)* – recommends that standard operating procedures (SOPs) also be developed as an additional improvement for coordinating and communicating important information during future inaugurations and other regional special events.

Weather Disasters & Other Emergencies

In addition to national special events, IT support and information sharing would be critical not only in the event of a

natural disaster but also, in most cases, during severe weather across neighboring regions. The year 2008 also marked a summer of destruction in Iowa, for example, during which extreme weather produced a series of severe storms – which in turn produced several tornadoes and a large amount of rainfall. By the end of the summer these storms had resulted in 17 fatalities, required the evacuation of 38,000 people, and damaged or destroyed over 21,000 housing units.

One example: After an EF-5 tornado struck Parkersburg, Iowa, on 25 May 2008, the Iowa Homeland Security and Emergency Management Division (HSEMD) activated the state emergency operations center (SEOC). The SEOC, in turn, granted WebEOC access to county and local officials both to facilitate information management and to maintain continued situational awareness through the WebEOC message boards. County EOCs and the SEOC were able to upload information related to property and road damage, county EOC activations, shelter operations, and resource requests.

The grand scale of these storms required greater use and reliance on IT systems and technical support. At times, the technology needs overwhelmed the center's IT staff, and support personnel had difficulties balancing their official support assignments with their other support tasks. The *2008 Iowa Summer Storms After-Action Report* (also available on *LLIS.gov*), recommends that the SEOC "explore additional opportunities to enhance its IT capabilities for future operations through additional collaboration with the Department of Administrative Services Information Technology Enterprise staff." Applying this lesson learned from the after-action report will undoubtedly help ensure proper IT staffing for use in future large-scale and/or extended-duration incidents.

For additional information on the after-action reports mentioned, and more documentation on information technology and information sharing in general, log into *LLIS.gov* at www.llis.dhs.gov.

Sophia Paros is an outreach analyst for Lessons Learned Information Sharing (LLIS.gov), the Department of Homeland Security/Federal Emergency Management Agency's national online network of lessons learned, best-practices, and innovative ideas for the U.S. homeland-security and emergency-response communities. She received a dual bachelor's degree in Computer Information Systems and Business from the College of Notre Dame of Maryland.

NEW

CHEMPRO

Handheld Chemical Detector **100i**

ChemPro100i is a handheld vapor detector for classification of Chemical Warfare Agents (CWAs) and Toxic Industrial Chemicals (TICs). The ChemPro100i adds 6 more sensors to increase the number of chemicals that it can detect and to decrease the potential for false alarms.



No maintenance costs for 5 years!

- Industry leading sensitivity
- Stores well - no regular exercise needed
- Non-threatening design
- Easy-to-use

* Contact Us for details on our standard 5-years Guaranteed Cost of Ownership (GCO) program



Environics Oy
Graanintie 5
P.O. Box 349
FI-50101 Mikkeli, Finland
tel. +358 201 430 430
fax. +358 201 430 440
www.environics.fi
sales@environics.fi

Environics USA Inc.
1308 Continental Drive, Suite J
Abingdon, MD 21009
USA
tel. +1 (410) 612-1250
fax. +1 (410) 612-1251
www.EnvironicsUSA.com
sales@EnvironicsUSA.com

Florida, Washington D.C., Wisconsin, and Michigan

By Adam McLaughlin, State Homeland News



Florida

Orlando to Receive \$23 Million in ARRA Funds for Airport Security

Department of Homeland Security (DHS) Secretary Janet Napolitano has announced that approximately \$23 million in American Recovery and Reinvestment Act (ARRA) funding will be available for an inline baggage screening system at Orlando International Airport (MCO) – enhancing the ongoing efforts of the Transportation Security Administration (TSA) to bolster airport security while boosting the local economy.

“This state-of-the-art technology will strengthen security for travelers by enhancing our capability to detect and disrupt threats of terrorism,” said Secretary Napolitano. “Infusing vital Recovery Act funds into critical airport security technology projects at Orlando International Airport will create local jobs, streamline the passenger check-in process, and bolster security at airports across the nation.”

“Employing enhanced baggage screening technology at Orlando is a key part of TSA’s efforts,” TSA Administrator John S. Pistole added, “to detect explosives, stay ahead of threats to aviation security, and ensure the safety of the traveling public.”

The Recovery Act funds provide the capital needed for construction and installation of an inline baggage screening system at Orlando International Airport. Inline screening systems use state-of-the-art technology to screen checked baggage for explosives more quickly than previously possible, while at the same time streamlining the ticketing process. They also provide on-screen resolution capabilities for security officers screening baggage – reducing the number of re-scans and physical bag searches required.

In July, Napolitano announced that \$7.5 million in ARRA funds would be allocated to MCO to expand its closed circuit television (CCTV) system by, among other things, installing several hundred cameras to provide enhanced surveillance capabilities throughout the airport.

Under ARRA, which was signed into law by President Obama on 17 February 2009, more than \$3 billion is provided for

homeland security projects under the jurisdiction of DHS and/or the General Services Administration. Of the \$1 billion allocated to TSA for aviation security projects, \$734 million is earmarked for the screening of checked baggage, and \$266 million is provided for airport checkpoint screening and CCTV technologies.

Washington D.C.

Initiates National “If You See Something, Say Something” Campaign

Department of Homeland Security (DHS) Secretary Janet Napolitano has announced a series of new initiatives designed to: (a) support state and local law enforcement and community groups across the country in identifying and mitigating threats to their communities; and (b) expand the DHS “If You See Something, Say Something” campaign to the Washington, D.C., area in conjunction with “National Night Out”; the latter is an annual anticrime campaign involving private citizens, police agencies, and neighborhood groups.

“Homeland security begins with hometown security, and our efforts to confront threats in our communities are most effective when they are led by local law enforcement and involve strong collaboration with the communities and citizens they serve,” Napolitano said in her 3 August statement. She was joined at the announcement ceremony by Eleanor Holmes Norton, the D.C. Delegate to Congress, District of Columbia Police Chief Cathy Lanier, WMATA (Washington Metropolitan Area Transit Authority) Police Chief Michael Taborn, and Homeland Security Advisory Council (HSAC) Chairman Judge William Webster.

The new measures announced by Napolitano are based on recommendations made by HSAC’s “Countering Violent Extremism” Working Group – composed of chiefs of police, sheriffs, community leaders, and homeland security experts – on various ways that DHS can better support community-based efforts to combat violent extremism in the United States.

The See Something/Say Something campaign, originally implemented by New York City’s Metropolitan Transit Authority – and funded, in part, by \$13 million from the DHS Transit Security Grant Program – is a simple and effective program designed to: (a) raise public awareness of

the visible indicators of terrorism, crime, and other threats; and (b) emphasize the importance of promptly reporting suspicious activity to the proper transportation and law enforcement authorities.

The Washington, D.C., area's local See Something/Say Something campaign will leverage the Metropolitan D.C. Police Department's long-standing participation in the nationwide Suspicious Activity Reporting (SAR) initiative, which leverages best practices from the law enforcement community while at the same time engaging the public in identifying and reporting suspicious activity.

The 3 August announcement represents the third major expansion this summer of the See Something/Say Something initiative, and follows earlier expansions, in July, to Amtrak and general aviation. DHS plans to continue to expand the campaign nationally in the coming months by, among other things, the distribution of public education materials and the use of advertisements and other outreach tools to encourage travelers, businesses, community organizations, and both public- and private-sector employees to remain vigilant and play an active role in keeping the nation safe.

Wisconsin **Power Plants Strive To Enhance Preparedness**

For a few seconds in mid-August, the simulator of the Kewaunee Power Station's control room went dark – except for several banks of warning lights and a near-constant series of alarms – while the five-man operating crew methodically worked through a difficult problem that testers had tossed in their laps. This was not a normal situation the crew probably would face, but something that they – and/or many others in the industry – may never see. But like many drills, it was something that the station's officials say they practice “just in case” the situation does arise.

Nuclear Regulatory Commission testing, inspections, and certification – along with simulations that test the capabilities of operating crews – are part of a wider effort to ensure the safety

of the communities around nuclear power plants such as those in both Kewaunee and Point Beach.

The Kewaunee Power Station, which is located on the shore of Lake Michigan in Northeastern Wisconsin – and owned by Virginia-based Dominion – houses a single reactor. The Point Beach Nuclear Plant, which is five miles to the south, and is owned by Florida-based Next-Era Energy Resources, has two reactors.

Emergency preparedness is one of the cornerstone capabilities required for either of the two plants to qualify for an operating license. “We live, and drill, every day like ... [an emergency] is actually happening,” said Ashleigh Burish, an emergency preparedness specialist at Kewaunee. “That is what we live, eat, sleep, and breathe. You could not have a business without protecting the health and safety of the public.

“We work very closely with the state and both Manitowoc and Kewaunee counties,” she continued. “We meet quarterly ... we do training together and incorporate each other in our drills and exercises and have a good working relationship.”

Fostering that close relationship with the state and the two counties is essential to continued operational success, Burish emphasized. “Not only are they in close proximity to you, within our emergency

planning zone, they are also our neighbors ... and it is where our employees live,” she said. “You are invested in the community.”

Emergency managers in both counties confirm the need for strong working relationships with both plants, as do both sheriff departments, which would be key players in responding to an incident at either plant. “We have confidence in each other,” said Inspector Gregg Schetter of the Manitowoc County Sheriff's Department. “We have confidence in what they are doing on their end as a private entity, and they have confidence in us as public safety.”

Both Kewaunee and Point Beach are equipped with control-room simulators where operating crews can train on different scenarios. Both plants also work diligently to keep local residents informed on what to do in the event of a dangerous situation at either plant.

Emergency preparedness is one of the cornerstone capabilities required for either of the two plants to qualify for an operating license: “We live, and drill, every day like ... [an emergency] is actually happening”

Michigan Postal Workers Practice Bioterrorism Response Procedures

Last Wednesday (18 August), postal workers wearing protective white coverall suits, yellow boots, and green gloves walked out of Lansing's mail processing center and into an inflatable decontamination station. None of the employees were in any danger; they were simply completing

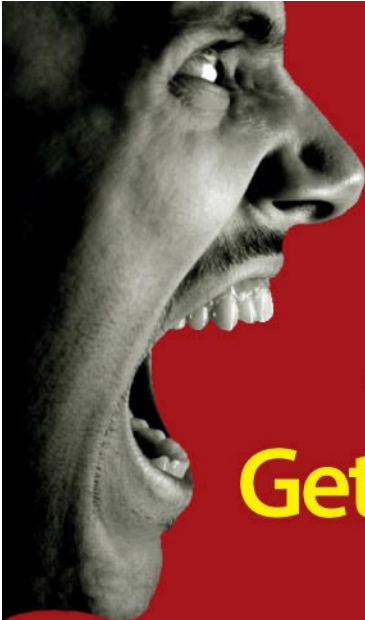
a "bioterrorism attack drill" to practice the response needed in case they ever come into contact with a potentially lethal dosage of anthrax – a disease caused by the spore-forming bacteria *Bacillus anthracis*.

In October 2001, five people, including two Washington, D.C., postal workers, died after being exposed to anthrax that had been sent through the mail in what seems to have been an intentional act of bioterrorism. Since then, the U.S. Postal Service has taken more measures, such as last week's drills, to protect its workers.

The last similar exercise at the Lansing post office and processing center was in 2007, according to Postal Service spokeswoman Sabrina Todd. "It [last week's exercise] just gives us all an opportunity to get together, look at our processes ... and make sure everything works in an orderly fashion," she said.

The Lansing police and fire departments and the Ingham County Health Department also took part in the drill at Lansing's main post office (at 4800 Collins Road). "Drills such as these help officials find and fix problems in their response plans and practice working with other agencies," said Marcus Cheatham, assistant deputy health officer at the Health Department. "Before 9/11, and before we started doing these drills," he pointed out, "we never partnered with the post office or the fire department, or the sheriff, on things like this, and now we are doing stuff jointly all the time."

Adam McLaughlin currently serves as the Manager of Emergency Readiness, Office of Emergency Management, for the Port Authority of New York and New Jersey. His responsibilities include both the development and coordination of Port Authority interagency all-hazards plans and the design and development of emergency preparedness exercises. A Certified Emergency Manager (CEM), he is a former U.S. Army officer – and a veteran of the war in Afghanistan – and a member of the Faculty of Senior Fellows for the Long Island University's Homeland Security Management Institute.



If This Is Your Crisis Plan For Chemical & Bio Hazards?

Get A Better Plan!

The **AP4C** Handheld Chemical Detector

- ▶ Fast Start-Up
- ▶ No Shelf Cost
- ▶ Easy to Use



Contact Us Now, Before It's Too Late...

PROENGINE

The Conference that Connects the Dots!

The Problems:

Deepwater Disasters, Fear of Fracking,
Coal Mine Catastrophes, Economic & Geopolitical Unrest.

MEET PEAK OIL!

The Solutions:

Prudent E&P, Effective Mitigation, Conservation,
Efficiency, Alternatives.

ASPO-USA's 6th ANNUAL PEAK OIL CONFERENCE

October 7-9, 2010, Capitol Hill Hyatt, Washington, D.C.

No More "Drill Baby Drill"

Oil, gas and coal are the nation's top three energy sources. Prudent energy companies have never taken a cavalier attitude toward hydrocarbon extraction, in spite of political hyperbole to the contrary. Due to Peak Oil, industry is forced to operate in more challenging environments than ever before: drilling miles below the sea, hydro-fracking shale formations, and conducting dangerous mining operations and mountain-top removal. Challenging environments call for more prudent drilling and operating practices than ever before. The low-hanging fruit has been picked; we must scrape the bottom of the barrel with great care.

But Drill We Must!

The most ardent advocates of alternative and renewable energy know we need hydrocarbon fuels to make the transition. We need oil to build the solar panels, wind turbines and electric cars and trucks that renewable advocates rightly envision. Meanwhile, offshore oil accounts for over 30% of our domestic production, and it can't be replaced with renewables. We must educate the public and the media about the real problems and real solutions to our growing energy crisis. We must start now to put prudent E&P, effective mitigation, conservation, efficiency and scalable alternatives at the top of our national energy agenda.

The Conference That Connects the Dots

ASPO-USA's 6th Annual Peak Oil Conference will maintain its traditional focus with a full agenda of world-class speakers who know how to connect the dots between the peak oil energy crisis and the complex socioeconomic and geopolitical factors that surround it. Confirmed speakers include **Dr. James Schlesinger** (Former U.S. Secretary of State), **Jeff Rubin** (Former Chief Economist CIBC), **Dr. Charles Schlumberger** (World Bank), **Rear Admiral Lawrence Rice** (on the military's Peak Oil Report), **Congressman Roscoe Bartlett** (R-Maryland), **Charlie Maxwell**, **Art Berman**, **Dr. Robert Hirsch**, **Dr. Roger Bezdek**, **Dr. Tad Patzek**, **Chris Skrebowski**, **Jeffrey Brown**, and other prominent energy analysts.

With hundreds of Peak Oil watchers at the Capitol Hill Hyatt, just a short walk from the U.S. Capitol itself, we will launch an outreach effort to take the conference to the elected and appointed officials down the street. We are working to organize Senate and House Briefings, a News Conference at the National Press Club, and other activities designed to make our presence, and our message, impossible to ignore. The conference itself will feature plenary and breakout sessions on Peak Oil and national security, natural gas and coal, renewables, net energy, the laws of energy, technology and scale, sustainability, food and climate change. Please see our conference website at the address below for a more complete agenda and list of speakers.



SAVE ON EARLY REGISTRATION

Sign up today to take advantage of early registration fees, and join ASPO-USA for additional discounts and benefits. Phone: 877-363-ASPO (2776) EXT 2

www.aspousa.org