DomPrep Journal

US Annual $100 Volume 9 Issue 4, April 2013

Transportation

Since 1998, Integrating Professional Communities of Homeland Security, Preparedness, Response & Recovery

Kestrel

High Comfort & High Protection CBRN Oversuit

Kestrel

High Comfort & High Protection CBRN Oversuit

The Kestrel is a highly comfortable and highly protective two piece CBRN oversuit harnessing much of the technology used in the Phoenix Lightweight Protection suit. At around 30% lighter than conventional systems, it provides qualified CBRN vapour protection with the added benefit of water/oil repellence and fire retardant coatings, thus making the Kestrel an extremely versatile CBRN protection system for use in multiple CBRN threat environments

For further information:
W: http://frontline.remploy.co.uk
E: frontline@remploy.co.uk
T: +44 (0) 151 630 3811

Remploy
Putting ability first

Frontline

The Ketrel is constructed using a lightweight activated carbon liner, combined with a breathable, rugged and anti-rip outer.

- Lightweight and breathable, the Kestrel has been tested using the Avon FM12 respirator, and can be configured to suit many other types of respiratory protection

Highlights

- Conforms to NATO standards
- High protection
- High air permeability
- Greater comfort and low physiological burden
- 20 times launderable
- 10 year shelf life
- Compatible with a range of accessories
- Fire retardant and water/oil repellent
- Stand alone garment or overgarment
- Rugged and durable
- Available in various colours and camo patterns

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

Staff

Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

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

Catherine Feinman
Editor
cfeinman@domprep.com

Susan Collins
Director, Production & Strategic Execution
scollins@domprep.com

Derek Sharp
Manager of Business Development
dsharp@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

John Morton
Strategic Advisor
jmorton@domprep.com

DomPrep Journal is electronically delivered by the IMR Group Inc., 517 Benfield Road, Suite 303, Severna Park, MD 21146, USA; phone: 410-518-6900; email: subscriber@domprep.com; 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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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.

Editor's Notes

By James D. Hessman

The killing of several innocent bystanders and the maiming of more than 200 others during this year's Boston Marathon raise questions about safety that do not have reassuring answers. "Perfect" safety is not possible – today, tomorrow, or probably ever. Although new and better surveillance systems, detection devices, and hard work make communities "safer," it is still not good enough.

The nine professionals gracing this month's issue of *DPJ* discuss a broad spectrum of political and economic issues, operational challenges, and even human frailties related to transportation concerns. They also offer some cogent advice, focus special attention on the need for a truly united federal/state/local attitude and operational approach in both long-range planning and current doctrine, and spell out several practical ways to better protect people and cargo throughout the world.

Corey Ranslem and Richard Schoeberl look at the U.S. port system, and find, not surprisingly, that the United States is now spending much more on port security than ever before. But "much more" is still much less than what is really needed. Almost all of the nation's hundreds of seaports are at serious risk from deliberate attacks, involving weapons of mass destruction hidden in cargo containers, that could kill thousands of people at one stroke, and cost hundreds of billions of dollars. The current approach – an alleged "carefully calculated" but still random inspection of a mere fraction of the hundreds of thousands of cargo containers arriving in U.S. ports annually – is not good enough.

Craig DeAtley gives a somewhat higher grade to the improved security at the nation's healthcare facilities thanks to the increased professionalism and much improved training of the security guards and other employees, as well as the healthcare providers themselves. Thomas P. Russo adds a complementary piece on the very special but sometimes unavailable transportation requirements of the nation's special needs populations – which includes a number of patients who, even in extremely dangerous weather conditions, prefer to remain in place rather than accept transportation to a safer location. William Rooney looks to the future in a strong and fact-filled article focused on the need now, not later, to include "the security factor" in the planning and policy issues involved in developing and building an affordable, and safe, high-speed-rail system for the United States.

Also featured in this month's printable issue are four "how to" articles by: (a) Joseph Cahill, who comments on the blessings as well as certain dangers involved in using the new and already ubiquitous social media; (b) Dennis R. Schrader, whose subject is catastrophic planning (and, sometimes, the lack thereof); and Michael Vesely, whose common-sense topic is the overly optimist use (and frequent misuse) of the predictive models relied on by at least some long-range planners. Stephan A. Parker rounds out the issue with a recommended-reading list of official publications, guidelines, and other helpful informational and legal resources available to working professionals, senior managers, and political decision makers alike.

About the Cover: A photomontage, by Susan Collins, of several modes of transportation – a long-range passenger aircraft, a high-capacity container ship, and cargo truck – and a silent-sentinel array of surveillance and traffic-control cameras that help keep them and as well as their passengers and cargo safe. (iStockPhotos)

AP4C

Handheld
CWA, TICs/TIMs
chemical detection
in confidence

Easy to use,
reliable, sensitive
and always ready

PROENGIN

Chemical and biological detection system

PROENGIN, inc.
140 S. University Dr, Suite F
Plantation, FL 33324 USA
Ph: 954.760.9990
contactusa@proengin.com
www.proenginusa.com

Key Hazards & Security Guides

By Stephan A. Parker, Transportation

Since 9/11, government agencies and the American public have turned to the scientific and engineering communities to develop faster, more efficient ways to detect, thwart, and respond to terrorist attacks on the U.S. transportation system. As part of the National Academies – which include the National Academy of Sciences, National Academy of Engineering, Institute of Medicine, and National Research Council – Transportation Research Board (TRB) committees and research programs have responded to this challenge and developed a "bookshelf" of security resources and guides for transportation professionals, decision makers, and members of the general public. In addition, TRB maintains a wide-ranging website on transportation system security and emergencies, and disseminates monthly updates on TRB and National Academies security activities.

Agencies, Programs & Committees

Surface transportation agencies – because of their broad policy responsibilities, public accountability, large and distributed workforces, heavy equipment, and robust communications infrastructure – are uniquely positioned among civilian government agencies to swiftly take direct action to protect lives and property. The institutional weight of such agencies also provides a stable base for campaigns to mitigate or systematically reduce risk exposure over time through all-hazards capital investments.

The TRB's Cooperative Research Programs are designed to assist transportation agencies in adopting the National Incident Management System (NIMS). In an 8 September 2004 letter to state governors, DHS Secretary Thomas Ridge wrote that, "NIMS provides a consistent nationwide approach for federal, state, territorial, tribal, and local governments to work effectively and efficiently together to prepare for, prevent, respond to, and recover from domestic incidents, regardless of cause, size, or complexity."

The Special Committee on Transportation Security and Emergency Management (SCOTSEM) of the American Association of State Highway and Transportation Officials (AASHTO) and the American Public Transportation Association Executive Committee Security Affairs Steering Committee provide direction to the coordinated Cooperative Research Programs Security Research under the National Cooperative Highway Research Program (NCHRP) and Transit Cooperative Research Program, respectively. All hazards, all modes oversight and project selection guidance is provided by NCHRP Project Panel 20-59, Surface Transportation Security Research. SCOTSEM and NCHRP Project Panel 20-59 host the Transportation Hazards & Security Summit and Peer Exchange in Irvine, California, each August (see the 2012 program).

Useful Documents & Reports

Two documents developed under the NCHRP – and adopted in August 2012 by the AASHTO Special Committee on Transportation Security and Emergency Management – are:

- *Security 101: A Physical Security Primer for Transportation Agencies*, which focuses on measures and concepts designed to: (a) safeguard personnel; (b) prevent unauthorized access to equipment, installations, materiel, and documents; and (c) safeguard equipment, installations, materiel, and documents against espionage, sabotage, damage, and theft.

- *A Guide to Emergency Response Planning at State Transportation Agencies*, which provides operationally oriented and practical guidance for state transportation agencies to plan, organize, staff, train, exercise, manage, implement, and fund the preparations needed to carry out their emergency responsibilities.

Among other key reports published by the Transportation Research Board are the following:

- *A Guide to Planning Resources on Transportation and Hazards*, which: (a) provides a framework for thinking about the stages of a disaster from a transportation perspective; (b) describes the most current and innovative hazards-related research to a transportation audience; and (c) introduces research from fields – including social science, mitigation and land use planning, and policy analysis – not always associated with transportation engineering.

- *Guide for Emergency Transportation Operations*, which supports development of a formal program for the improved management of traffic incidents, natural disasters, security events, and other emergencies on the nation's highway system.

- *Costing Asset Protection: An All Hazards Guide for Transportation Agencies (CAPTA)* – a convenient and robust planning tool for top-down estimation of both the capital and the operating budget implications of measures intended to reduce risks to locally acceptable levels.

- *Communication With Vulnerable Populations: A Transportation and Emergency Management Toolkit*, which provides a guiding framework and the tools needed for developing a scalable, adaptable communication process built on a network of agencies from public, private, and nonprofit sectors.

TRB's Security and Emergencies website provides links to various TRB security-related publications and other resources as well as the highlights of selected transportation security research-related activities taking place in the United States and other nations.

Stephan A. Parker is a senior program officer for the Transportation Research Board (TRB) of The National Academies. Prior to joining TRB in 2000, he developed courses on intelligent transportation systems and supervised the NTI Fellows program for the Advanced Technologies and Innovative Practices section at the National Transit Institute at Rutgers, The State University of New Jersey. He served as scholar associate for a review of the Department of Homeland Security's Approach to Risk Analysis (National Academy of Sciences, 2010). As administrator for the Joint Powers Transportation Board of the Town of Jackson and Teton County, he served as general manager for the START Bus transit system in Jackson Hole, Wyoming, and was founding vice-president of WYTRANS, the Wyoming Public Transit Association. He holds a Bachelor of Sciences degree in speech from Northwestern University and a Master of Sciences degree – in interdisciplinary studies: civil engineering and management of technology – from Vanderbilt University.

Transportation Requirements for Special Needs Populations

By Thomas P. Russo, Emergency Management

How to reach special needs populations pre-disaster and prepare them for response actions and post-disaster recovery operations is one of the many aspects of advance planning that local authorities must address as they seek to build community resilience. A particularly complex phase of pre-disaster preparedness is planning for the transportation needs of those who are designated as "access and functional needs populations" (AFNP) within coastal communities. A model that triages special needs populations pre-disaster depending upon transportation requirements could be instructive when planning with the diversity represented in AFNP.

U.S. coastal communities have unique and difficult transportation needs during major disaster situations. Compounding the problem are many differences in the transportation resources required for access and functional needs populations.

Along the coastal communities in states where the threat of hurricanes is high, emergency managers wrestle with how best to integrate planning for those who have an access or functional need. Coalition development has been a key tool for organizations that may have competing interests or even have missions with unlikely commonality. It also is a tool that coastal communities can use to form a task force, which would include stakeholders and individuals with access and functional needs, to address their unique transportation issues during a disaster. The purpose of an AFNP coalition task force is threefold: (a) explore the assumptions, limitations, and other interrelated transportation issues involved; (b) determine the resources and options available; and (c) define and better understand AFNP groups. To understand the behavior of AFNP evacuees, such as occurred during Hurricane Sandy in 2012, this model describes three general scenarios governing preparedness operations needed to meet the local transportation needs for AFNPs.

Each person, of course, may have his or her own transportation preferences, depending on specific functional needs. The worst case scenario for coastal regions would be a threatening hurricane as was witnessed in 2012 along the New Jersey coast with significant surge and strength to trigger a major coastal evacuation. This model of evacuation scenarios, with certain assumptions, would also work for other disaster situations and for other operational plans – the stockpiling and distribution of various Strategic National Stockpile medications and other resources, for example.

The following model and its three scenarios could be adopted to guide, or triage behavior patterns of AFNPs into smaller and better defined groups, and to prioritize the planning efforts developed by both scenario and functional need: (a) If transportation is available, the AFNP would act on the recommendation to evacuate; (b) If transportation is *not* available, adoption of the order to evacuate would depend on the availability of other public and/or private resources; and (c) If transportation is available, there still would be isolated and/or unidentified populations, as well as recalcitrant – i.e., unwilling to evacuate – citizens.

Background Complexities & What-If Scenarios

Among coastal communities, emergency management authorities (EMA) have long recognized the critical need to: (a) reach all population groups in the area; and (b) determine the most effective strategy to include access and functional needs populations in its emergency plans.

EMAs have adopted and currently operate under the federal government's National Incident Management System (NIMS) since NIMS inception. Many emergency operation centers (EOCs) are structured around incident command, with organized support services provided in its planning, logistics, operations, and administration sections. EMAs have also made great efforts to build

many partnerships along the coast, in addition to those with public transportation resources. During hurricane evacuation operations, regional transportation authorities have been incorporated into the EOC under Emergency Support Function 1 (ESF 1 Transportation) to assist with transportation issues during an emergency. Scenario 2 of the model directly involves ESF 1 during pre-disaster orientation, training, and exercise, as well as post-disaster response. In contrast, the emphasis of the model with Scenario 1 is directed toward pre-disaster education. Following are some of the particulars for each scenario of the model.

Scenario 1: If Transportation Is Available: Many AFNP residents with transportation resources know that to maintain the level of functionality for such residents requires a stable infrastructure and, primarily for that reason, evacuation would be the most prudent choice. These sensitive populations often are dependent on utility infrastructures and systems such as electric power, which may be limited following a disaster. In the aftermath of Hurricane Sandy in 2012, when power was out for an extended period of time, many examples of similar dependencies were documented. Citizens reliant upon or needing dialysis drove a vehicle (or were driven) to hospital emergency rooms for resupply or treatment because the circumstances of the storm overwhelmed their pre-disaster preparations. This segment of AFNP could be reached, in most cases, pre-disaster through a targeted and determined educational campaign.

The pre-disaster role of a coalition task force is to work with stakeholder organizations and AFNPs to develop an educational campaign and accompany it with an individual evacuation plan when a transportation source is available. An evacuation plan should be developed that could be used by any organization that works with an AFNP. For example, in South Carolina, special medical needs providers use such a plan for healthcare facilities that partner and pre-plan with those who may have to evacuate. This tool could be adapted and become an additional topic for a pre-disaster education campaign.

Other topics in the campaign could include emergency management EOC operations and orientation sessions, with specific focus on transportation as one of the major components of the pre-disaster education effort. Educational topics of discussion also include: (a) the use of emergency management methods for first-alert communications when a threat is impending; and (b) activation of the methods for achieving the outreach of information or its community outreach information network (COIN) to mobilize for evacuation.

Scenario 2: When Transportation Is Not Available: Vehicle accessibility, for both supply and accommodation, poses the greatest current challenge to emergency planners and becomes much more complex during emergency operations. In addition to a limited supply of vehicles, the need to use vehicles without special accommodations further complicates planning efforts.

A first step is to conduct a gap analysis and determine the specific factor(s) contributing to the limited availability of (or inaccessibility to) the transportation resources in the area. The questions to be asked are threefold: (a) Is the transportation problem caused by vehicle availability? (b) Is it because of limited or no access to public transportation? (c) Is it a result of inaccessibility to vehicles with special accommodations such as chair lifts?

A typical concern is that, although the use of public transportation may seem to be a possible option of last resort, many if not all AFNPs might have, at best, limited access from their residences to the pickup points during evacuation operations. It is only after these and other transportation limitations are fully understood that known and available transportation resources can be matched to determine the gaps that may still exist in the AFNP emergency transportation infrastructure.

Scenario 3: Isolated, Unidentified, or Recalcitrant Populations: Those who work with AFNP, including EMA, acknowledge that there are certain people such as the homeless, those suffering from mental illness, or others with functional disabilities who will elect to remain isolated, unidentified, or simply refuse to evacuate under any circumstance. In South Carolina, estimates suggest that approximately 20 percent of the state's AFNPs would fall into this group.

Also worth noting, several reasonable assumptions will surface as a coalition task force engages in the logistics of addressing the unique transportation needs of AFNPs for disaster response and recovery. For example, if the desired outcome is evacuation, the assumptions that underlie this action could represent several behaviors that must be reconciled before a decision is made to evacuate. It is essential, therefore, that stakeholder organizations and AFNPs have been sufficiently educated that, once alerted, the evacuees act as expected (Scenario 1 described above) and accept decisions that would result in either taking refuge in a safe shelter or evacuating.

Another assumption is that the unique methods of communication identified for each functional group should be developed and implemented prior to an incident. A key factor in this calculation is that adequate time must be available to mobilize the communications network and activate the necessary transportation resources to meet incident requirements. Given the current alerting technology, hazards that start with little or no warning such as tornadoes and earthquakes may not allow sufficient time for notification, but others such as hurricanes would provide advance notice.

Limitations & Restrictions

In terms of the supply of transportation resources – both public and private sector – likely to be available, a number of limitations could compromise the recruitment of either private sector or nonprofit organizations to provide supplemental transportation resources. These limitations include the following:

- A memorandum of agreement would be necessary prior to an incident when supplemental transportation resources are required;

- Private sector resources would almost always require a cost reimbursement agreement of some type, and even nonprofit organizations may require some level of reimbursement as well; and

- Either type of organization, public or private, may have competing commitments of its own.

Public transportation organizations are typically the most accommodating during an emergency that requires short-notice transportation resources. Private sector transportation resources are usually committed to a contract and, therefore, may not be available when requested for public use. Resources that would offer some potential relief are public and/or private organizations possessing vehicles that are not only multipurpose and equipped with special accommodations but also meet the special requirements posed by AFNP rescue operations. As a result, this composite of resources, their capabilities, and availability should be identified and inventoried, and the conditions of availability determined for both pre-disaster and post-disaster situations.

Thomas (Tom) P. Russo, CEM, is an independent public health and emergency management professional with nearly 30 years of experience in strategic planning, project management, and professional development, including 18 years in public health. Trained in emergency management, public health, homeland security, and association management, Russo holds a Master's degree in Homeland Security Studies from the Naval Postgraduate School's Center for Homeland Defense and Security and has authored a number of articles on topics ranging from medical surge, mass fatality and pandemic policy and preparedness to the continuity of operations planning readiness for medical facilities.

Shipping Containers & Hidden Dangers

By Richard Schoeberl, Transportation

American seaports are not only the maritime doorway to the nation but also a crucial link in the U.S. two-way trade with other nations. Today, billions of dollars' worth of unchecked goods move in and out of U.S. international seaports every month, making ports vulnerable to disruption from both terrorist attacks and natural disasters. In the United States, the Customs and Border Patrol (CBP), the U.S. Coast Guard, the Department of Agriculture, port authorities' own police forces, and many other local, state, and federal government agencies diligently work together to protect the nation's seaports from myriad threats. Nuclear proliferation is a viable threat and the possibility of a terrorist attack on a U.S. seaport is certainly plausible – both with the potential to cause immediate devastation to the local community and to cripple the already delicate global economy.

Busy Ports

The United States currently is served by more than 360 commercial ports – which, according to the U.S. Coast Guard, provide nearly 3,200 handling facilities for both cargo and passengers. Additionally, U.S. seaports process more than 2 billion tons of import/export freight per annum. In 2009 alone, according to the U.S. Department of Transportation, nearly 10 million ocean-borne cargo containers entered the United States through its seaports.

Los Angeles and Long Beach, California, are unequivocally the busiest North American container ports, trailed by the Port of New York and New Jersey. In 2011, the Port of Long Beach handled more than 6 million containers and the Port of New York and New Jersey handled 5.5 million – both container totals are measured in TEUs (20-foot equivalent units).

Cargo containers are an important component of the global supply chain – the flow of goods from manufacturers to retailers. Unfortunately, the mass influx of containers provides innumerable opportunities for would-be terrorists to smuggle and detonate a weapon of mass destruction (WMD) on U.S. soil. Although terrorism remains a critical security focus at seaports, it is actually rated by U.S. Customs as a lower risk than other threats – e.g., drug smuggling, human trafficking, weapons trafficking, and trade and import safety violations – that have the potential to compromise the nation's supply chain.

Consequences of an Attack

Apart from the potential human costs that may result from a lack of port security, the economic costs of a maritime attack can be overwhelming. During a time when workforces face layoffs, impending unemployment extensions, and foreclosures, any political or economic factor that impedes the flow of trade would not only affect the seaports themselves but also interrupt the supply of goods. The widespread effect would be felt throughout the country, and in many other nations as well.

Rear Admiral Paul Zukunft, the Coast Guard's Assistant Commandant for Maritime Security, told the House Subcommittee on Border and Maritime Security last year that, "Considering that high concentrations of our population live in and around port areas, and 95 percent of our international trade is done via the sea, the consequences of any attack or disruption on our maritime transportation system are potentially severe."

Section 1701 of the 9/11 Commission Act of 2007 requires that all maritime cargo containers bound for the United States must, as of 12 July 2012, be scanned by non-intrusive imaging equipment and radiation detection technology before being loaded on ships. Reinforcing efforts to counter the looming terrorist threat at U.S. ports is the fact that then-candidate Barack Obama promised during his 2008 presidential campaign to "Develop technology that can detect radiation and work with the maritime transportation industry to deploy this technology to maximize security without causing economic disruption."

The Benefits & Pitfalls Of 100-Percent Screening

Unfortunately, the practicality of fully implementing the "100-percent screening" mandate is questionable – so much so that today, nearly six years since the 9/11 Commission Law was enacted, the U.S. Department of Homeland Security (DHS) has failed to implement the mandate ordered by Congress.

Given the complexity and magnitude of the global supply chain, as well as the massive number of containers transported to and from the United States each year, U.S. seaports remain susceptible to a broad spectrum of threats that domestic as well as international terrorists may be able to exploit. Although the U.S. intelligence community has long suggested the possibility of terrorists smuggling a WMD into the United States inside a shipping container is relatively low, the vulnerability to such an attack is theoretically very high.

According to the CBP, in fact, agency officials scanned only 473,380 – about 4.1 percent of the approximately 11.5 million containers shipped into U.S. ports in 2012 – with X-ray or gamma-ray machines, and some shipments getting only a cursory paperwork review. The low percentage of scanned cargo is officially rationalized as a "layered risk-based approach" to cargo scanning and focuses primarily on specific cargo considered to be "high risk" – how that term is defined and bestowed is not always clear.

Detecting radioactive materials or any other harmful matter at U.S. ports clearly remains a challenge for federal officials. However, U.S. Representative Candice Miller, a Michigan Republican who chairs the House Subcommittee on Border and Maritime Security, accepts the current approach. In a statement before the subcommittee on 7 February 2012, she acknowledged that, "We all recognize it [the current process] may be optimal but perhaps not realistic from a cost perspective." She also reiterated a statement from DHS Secretary Janet Napolitano that, "The 9/11 Act's mandate to scan 100% of maritime cargo containers is not achievable, does not necessarily make sense, and is not in line with the current risk-based approach."

At the same hearing, though, former Rep. Laura Richardson (D-Calif.) said that a successful terrorist attack "on one of our ports, such as the Port of Los Angeles or the Port of Long Beach, would have a devastating economic impact and severely impact the global supply chain. The cost of one terrorist attack in

our ports," she continued, "would far surpass the costs of instituting the 100 percent container scanning that is required by law and was recommended by the 9/11 Commission. We have been extremely fortunate that an attack has not yet occurred in our ports."

A Recipe for Disaster – Funding Cuts & Dense Populations

The Megaports Initiative – a collaborative effort between DHS, the U.S. Department of State, and their counterparts in U.S. international partners – is also facing severe spending cuts. The U.S. government has spent roughly $850 million on 42 different maritime security projects in 31 other nations to carry out such tasks as: (a) providing the seaports of other nations with radiation recognition equipment; (b) training foreign inspectors; and (c) providing other assistance to the employees of foreign governments who operate the ports.

U.S. seaports – the "doorway" to the nation – are not just poorly guarded but also, in the view of at least some security experts, highly susceptible to both terrorist attacks and natural disasters.

Whether that funding stream will continue at the same level seems doubtful. According to a GAO statement in November 2012, "The administration's fiscal year 2013 budget proposal would reduce the Initiative's budget by about 85 percent, and NNSA [National Nuclar Secrity Administration] plans to shift the Initiative's focus from establishing new Megaports to sustaining existing ones."

It is important to note that a number of America's seaports can be found in or near highly populated areas and, therefore, are attractive targets for a terrorist organization. The New York region, for example, is home to approximately 19 million people. The consequences of a WMD or nuclear attack at the Port of New York and New Jersey could be cataclysmic.

According to 2006 estimates by the RAND Corporation and a 2005 report from the Congressional Research Service, an attack on a U.S. seaport could cause thousands of deaths and severely impair international trade, with damages ranging from a "low" of $45 billion to more than $1 trillion. In order for the 100-percent screening mandate to be fully realized, regardless of costs associated with the mandate, DHS must safeguard the movement of cargo at each and every link of the supply chain, beginning at the port of origin, continuing during the entire time the cargo is in passage, and not ending until such time as the cargo reaches its port of destination in the United States. In short, simply inspecting the cargo manifest – the rather porous "inspection process" often used – is no longer sufficient.

In summary, the costs associated with scanning all maritime cargo containers before they arrive in this country are great, but the consequences of not doing so could be much greater. Securing the nation will become increasingly more difficult as budgets continue to decrease, screening and security measures are delayed until after containers reach their U.S. destination, and only a small percentage of the scanning required is actually carried out – on random containers.

In a worst-case situation, a nuclear weapon concealed inside a cargo container can be triggered from a distance. If a WMD does in fact happen to be detected at random by radiation portal monitors – in New York or Long Beach, perhaps – it may still be too late to stop or even mitigate the damage and to save the lives of tens of thousands of people living within the port area targeted.

Richard Schoeberl has more than 17 years of counterintelligence, counterterrorism, and security management experience, most of it developed during his career with the Federal Bureau of Investigation, where his duties ranged from service as a field agent to leadership responsibilities in executive positions both at FBI Headquarters and at the U.S. National Counterterrorism Center. During most of his FBI career he served in the Bureau's Counterterrorism Division, providing oversight to the agency's international counterterrorism effort. He also was assigned numerous collateral duties during his FBI tour – serving, for example, as a Certified Instructor and as a member of the agency's SWAT program. He also has extensive lecture experience worldwide and is currently a terrorism and law-enforcement media contributor to Fox News, Sky News, al-Jazeera Television, and al-Arabiya.

Today's "New" Maritime World – Threats & Risks

By Corey Ranslem, Viewpoint

Around the world, ship crews face a number of security concerns whether in port, underway, or at anchor. The International Maritime Bureau reported in January 2013 that piracy in the hot spots in and around the Gulf of Aden/Indian Ocean operational region is down significantly from 2011 to 2012, and that piracy worldwide declined from 439 reported attacks in 2011 to 297 in 2012. However, maritime experts also reported that piracy against vessels outside the Indian Ocean region is continuing to rise.

During personal interviews conducted in April 2013, the following three maritime experts shared their views and concerns about the piracy threat and how to effectively assess and mitigate the related risks: (a) Luke Ritter, principal at Ridge Global (a consulting firm started by former Homeland Security Secretary Thomas J. Ridge) and author of *Securing Global Transportation Networks*; (b) Brian Peterman, chief executive officer of Command at Sea International (a maritime security company) and a retired Coast Guard vice admiral; and (c) Philip Murray, chairman of the Maritime Security Council (a private nonprofit organization headquartered in North Carolina that represents ocean carriers, cruise lines, port facilities and terminals, logistics providers, importers, exporters, and related maritime industries throughout the world).

"Piracy continues to be a problem around the world; however, the problem can be effectively addressed, but more resources are needed," commented Ritter. "Shipping companies, private yachts, and cruise lines do not have a lot of options when it comes to real-time threat reports and port risk assessments. The maritime industry is worldwide and very disjointed when it comes to collaborating on threats and information sharing."

Peterman said that there is no actual coordinated effort to collect and share information, "There is a reasonable amount of information as to what is happening in the commercial arena, but not much information in the private yacht world."

Data Collection & Sharing

There are a number of government and quasi-government agencies around the world collecting information, but very few share information with the maritime industry. "The maritime industry is extremely complex and touches so many different industries and transportation modes," said Ritter. "Unfortunately, there is not a lot of information sharing, and the onus for collecting threat information falls back on the shipping companies, cruise lines, and large yachts."

Following the 9/11 terrorist attacks, the U.S. Department of Homeland Security spent considerable time and significant resources working with various industries to develop better methods for sharing threat information. The National Council of Information-Sharing Analysis Centers (I-SACs was formed in 2003 by a volunteer group of ISAC representatives to manage the 15 different I-SACs) stretching across various industries including real estate, transportation, supply chain, health, and maritime.

Murray said that the Maritime I-SAC has been funded 100 percent by the Maritime Security Council and geographically spans the world. "The Maritime I-SAC covers a large amount of information and territory worldwide," said Murray. "We are looking to continue to grow the Maritime I-SAC, but would benefit from additional funding to expand to the same level as the other I-SACs."

"People don't always understand what maritime covers. Maritime is thought of differently by different

constituents," said Ritter. "There is no one U.S. government agency with overarching authority in the maritime sector, federal, state, and local law enforcement, and regulatory agencies cover various aspects of the industry."

Peterman agrees that the maritime realm touches a number of federal, state, and local agencies and there is no overarching agency that coordinates the collection of threat information. "The information sharing and coordination is much better at the local level than on the national level. There is great information sharing at that level because it is necessary to get the job done."

Reporting Threats & Assessing Risks

There are a number of private companies and industry consultants that provide shipping companies, cruise lines, and large yachts with threat reports and risk assessments, but this information comes at a cost to the user. "We tried to conduct assessments of a number of private intelligence collection companies and have only found a couple that understand the maritime environment, but they provide limited information concentrating on certain parts of the world," said Peterman.

The Maritime Security Council acts as the coordination center of information coming from sources around the world. "We work hard to protect proprietary information from our members and the users of the Maritime I-SAC," said Murray. "The Maritime Security Council is best positioned as a private nonprofit to coordinate, protect, and disseminate timely threat reports and information to the I-SAC users."

"There is a great opportunity for the maritime industry to collaborate on threat reporting and risk assessments, because the industry shares a common adversary," said Ritter.

Positive Advances – Despite Budget Cuts & Limited Resources

Port and maritime security in the United States is primarily handled by local and state law enforcement agencies with overlap by federal agencies. The physical security in most ports is typically handled by local law enforcement agencies or port authority police. Through the ongoing financial crisis, these agencies continue to experience program and budget cuts that leave agencies scrambling for resources.

"There have been a lot of positive advances in local maritime security because of the Port Security Grant Program," said Peterman. "However, we are probably going to see a major reduction in grants and funding at the state and local level with budget cuts." Peterman also stated that he thinks one of the programs that might get cut is the Coast Guard's foreign port assessment program. Through this program, the Coast Guard conducts threat assessments of foreign ports to determine security risks.

"Piracy, cargo theft, and general maritime security threats continue to be a problem as criminals are becoming more sophisticated, while law enforcement agencies are facing major program and budget cuts," stated Ritter.

Ritter, Peterman, and Murray all agree that there is a lot of work that still needs to be done in the maritime industry in order to collaborate on threat reports and risk assessments. As the focus in the United States shifts from maritime threats to immigration and border security, funding will likely be diverted from maritime security to land border security.

Corey D. Ranslem, chief executive officer of Secure Waters Security Group Inc. – a maritime-security and consulting firm heavily involved in maritime training, maritime security, and a broad spectrum of other security programs in the maritime field – is the former regional manager of Federal Government Operations for Smiths Detection. He has received numerous awards and citations from the U.S. Coast Guard and other agencies and organizations active in the field of maritime security. He holds a Bachelor's Degree in Communication and Political Science from the University of Northern Iowa and an MBA in International Business from Georgetown University; he has almost 18 years of experience in maritime law enforcement and security.

The Security of Healthcare Facilities – A Growing Challenge

By Craig DeAtley, Health Systems

Whether the situation involves person-on-person violence, forensic patient management, or the handling of patient property, healthcare facilities (HCFs) across the United States are finding themselves with a growing number of security-related issues that require well-trained and highly skilled security officers. Today's healthcare facility security officer is no longer a "guard" per se, but in many cases also a special police officer who is, among other things: (a) armed with arrest powers; (b) trained on how, and when, to defuse tense emotional situations; and (c) armed with various other weapons and personal skills that can be used if, when, and as needed.

Today's HCF security officers may, in fact, be either a facility employee or a member of a security firm contracted by the facility. Some HCFs may also employ local off-duty police officers to bolster their staff – often at night and/or on weekends. Regardless of his or her employer, the security officer must in almost all cases pass a background check, meet the physical standards prescribed for his/her duties, and complete both local and state educational requirements directly related to the security profession. The initial training hours for security officers vary widely – depending on the jurisdiction and facility performance expectations. Successful completion of the coursework prescribed usually requires passing certain written and practical exams.

Training, Certification & Hands-On Force

After certification has been completed, annual refresher training that blends classroom assignments along with hands-on physical training also is required. The successful officer should be able to expertly defuse tense situations through reasonable but firmly stated discussion – as well as the use of a baton, pepper spray, other crowd-control agents, and/or hands-on personal force when physical control is required. Some facilities authorize their security personnel to use electronic control devices (e.g., a taser), or a handgun – both of which obviously require additional and highly specialized training.

In some states, the basic and continuing-education training provided to special police officers mirrors at least some of the training provided to that community's regular police officers. Fortunately, the International Association of Healthcare Security and Safety (IAHSS) not only has a variety of training courses available that have been adopted by most of the nation's HCFs, but also the certification examinations – both for officers and for command staff personnel that also are or should be required.

Among the numerous other variables involved in determining the number of officers who should be on duty at any given facility are the size of the facility, the specific times of day involved, and the probable work requirements for each shift. A well-defined chain of command also is needed – not only to provide administrative and operational direction for the department but also to share and encourage career promotion opportunities.

New & More Violent Security Challenges Emerging

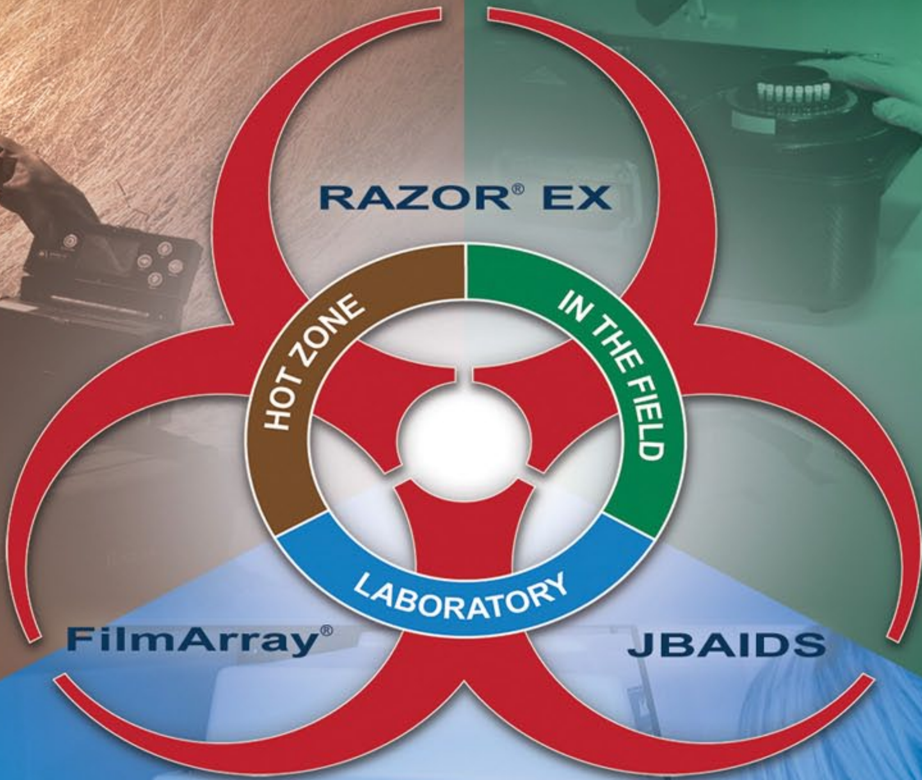
Among the more important challenges HCF security departments face today is the growing incidence of violence – whether patient-on-employee, employee-on-employee, or some other combination – in the workplace. The increase in workplace violence that has been reported in recent years is significant, and represents a difficult challenge to the often-limited number of on-duty personnel available. It is now increasingly common, in fact, for security departments to try to reduce the threat through staff education provided both at new employee orientations and at regularly scheduled department meetings.

Managing forensic patients – i.e., patients in police custody requiring medical care because of injury or illness, and/or patients threatening or having the potential for violent actions because of drugs or behavioral disorders – is another challenge to hospital security officers. Depending on the state, regulations are or should be in place that require accompanying police officers to be briefed on the HCF's own forensic patient policies at the time of patients' admission into the facility.

BioSurveillance

Flexible, Accurate, Proven Ready

BioFire Diagnostics delivers a fully integrated suite of Biological Agent Identification Systems. Since 1998 we have fielded BioSurveillance products that span the range of operations from the lab to the field, clinical diagnostics to environmental surveillance.



Idaho Technology is now

BIO FIRE™
DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

To offset the increased threat of violence, while also ensuring that the facility can protect its patients and staff – especially those having to cope with an increase in crime – a growing number of HCFs are considering whether or not to issue sidearms to their security officers. The perception of the public, the added expense of acquiring and maintaining the weapons, and the officer training necessarily associated with such action are just a few of the important considerations that must be addressed before making such a difficult decision.

There are, of course, both positives and negatives involved in deciding whether or not to arm an HCF officer. However, anecdotal evidence suggests that the facilities that do use armed officers often see an increase in the respect afforded to those officers by the public and staff and a decrease in violent crime. Those facilities opposed to issuing their officers a gun cite start-up and annual costs, as well as the possibility of the weapon being wrestled from the officer and used to cause harm, as reasons not to arm their officers.

The Increased Use & Higher Cost of Modern Technology

The use of modern technology is another important aspect of police security in an HCF. Many facilities already depend heavily on the use of closed-circuit TVs (CCTVs) for the real-time monitoring of several vital locations – particularly when there are no officers physically present in those locations. The CCTV monitoring is often recorded and stored for future playback, if and when needed. The ability to electronically close and lock doors is another desired capability that many HCFs now possess.

In an attempt to limit the risk of violence, many HCFs are now using a front-desk check-in procedure that requires the temporary identification, in one form or another, of each visitor, contractor, and vendor. Some HCFs complement this practice by also requiring each visitor to either pass through a magnetometer and/or to be electronically "wanded" before entry. This process may be employed in emergency departments and in other areas of heightened security. Unfortunately, the cost and recognized benefit of these check-in practices have limited to some extent the number of HCFs actually using either or both as part of their routine security practices.

Working With Others: Always a Better Idea

In some communities – the District of Columbia, for example – HCF security directors regularly meet to discuss issues of common concern. In the District of Columbia, the directors have worked closely with the Metropolitan Police Department (MPD) to create "Code Pink" (abducted infant or child) and "active-shooter" planning templates, which each facility has used in turn to craft its own plan.

A new and effective plan has been written for how the MPD itself can access the schematic drawings for each facility, and an intranet-based web page has been developed to provide a secure means for sharing operational and emergency information if and when needed. The directors' group also sponsors an annual training conference with local and national speakers addressing various security topics of general interest.

To briefly summarize, healthcare facilities throughout the United States face a growing series of new challenges related to keeping their staffs, as well as patients, safe and secure. Vital to this effort is recruiting and training a professionally staffed, highly motivated, and properly trained security department capable of using advanced technology – including various types of weapons – to meet the diverse challenges faced by each facility involved. The desired result is a well-earned increase in the trust and respect shown by patients, visitors, professional staff, and the community as a whole.

Craig DeAtley, PA-C, is director of the Institute for Public Health Emergency Readiness at the Washington Hospital Center, the National Capital Region's largest hospital; he also is the emergency manager for the National Rehabilitation Hospital, administrator for the District of Columbia Emergency Health Care Coalition, and co-executive director of the Center for HICS (Hospital Incident Command System) Education and Training. He previously served, for 28 years, as an associate professor of emergency medicine at The George Washington University, and now also works as an emergency department physician assistant for Best Practices, a large physician group that staffs emergency departments in Northern Virginia. In addition, he has been both a volunteer paramedic with the Fairfax County (Va.) Fire and Rescue Department and a member of the department's Urban Search and Rescue Team. He also has served, since 1991, as the assistant medical director for the Fairfax County Police Department.

Providing Security for High-Speed Rail

By William Rooney, Transportation

Although undoubtedly confusing to those persons trying to learn English as a second language, one often hears the expression that, "There is an elephant in the room that no one is talking about" – i.e., a topic or issue so obvious that it cries out to be addressed but is often ignored for one reason or another. The "elephant in the room" in most if not all current discussions about high-speed rail (HSR) projects in the United States is "security."

Until now, in fact, most discussions about HSR projects have centered on such political and/or financial/economic questions as the following: What is or should be the role of the U.S. government in facilitating the building of the first HSR system in the United States? What is or should be the role of the private sector? What will be the "hand-off costs" to U.S. taxpayers to maintain the HSR system? What will be the real economic benefit to travelers?

Similar discussion points about affordability, spending priorities, and the long-range impact on modernizing the national transportation system infrastructure also have been raised. Regrettably, most of these discussions seem to be increasingly politicized as debates continue to focus primarily on the growing U.S. deficit, the spending priorities at all levels of government, calls for additional tax revenues and/or spending cuts, and – last but not least – the need to modernize the overall U.S. transportation system.

The Question Not Asked: What About Security?

It is of critical importance that security be included in the earliest stages of HSR planning and design. Ignoring security as an essential ingredient in mission planning could lead to fatal flaws in future HSR prospects throughout the United States. Nonetheless, current ongoing HSR discussions – in California, Texas, and Illinois – seem to focus primarily, and predictably, on such questions as the following: Who benefits? Who pays? Is this a budget necessity? Do taxes go up? Who builds the system? Is it a spending boondoggle? Is it affordable? And where does it fit in the overall list of spending priorities? Considering the fact that there are significant disagreements in all three of those states on what are or should be the answers to these and other questions, it is not surprising that security discussions have been put on the back burner.

As was true in the 9/11 terrorist attacks on the Twin Towers and on the Pentagon – well-known iconic symbols – a new HSR system established anywhere in the country would, if only for propaganda reasons, certainly become another prime target for terrorists. For one thing, a successful attack on such an important transportation icon would send a worldwide message about the possible vulnerability of the nation as a whole.

Ignoring security concerns in the early stages of planning for so-called "bullet" trains could have disastrous effects. Unfortunately, "high speed" can translate quickly into high target risk as well.

U.S. decision makers, planners, engineers, and project architects should never overlook the fact that a unique new U.S. transportation system of the type contemplated would almost certainly be high on the targeting screen of would-be terrorists. And it would be different in many respects from many other potential targets, including the fact that the primary purpose in building it would be to provide much faster transportation.

With time being of the essence, delays of any kind would not only be counterproductive and self-defeating, but also would have to be avoided whenever possible; after all, most HSR passengers would be in a hurry and scheduling would be tight. For both of those reasons, there probably would be minimal time-delaying security procedures and/or passenger screenings aimed at spotting persons who might be in the early stages of "casing" a target by looking for various vulnerabilities and design weaknesses.

Even so, with boarding protocols at a minimum, the HSR train itself could be the terrorists' highest value target; one that, if attacked while moving at high speed, would assure a great number of deaths, graphic publicity, and a psychological shockwave throughout the nation and around the world. Such a disaster could have a tsunami-scale ripple effect – opening a floodgate of liability claims, as well as congressional inquiries on security lapses, and planning failures. In short, just one deadly setback might conceivably bring the entire system to a screeching halt.

Discussion Points & System Vulnerabilities

Clearly, planning and maintaining security for any HSR project involves significant risks with no guarantee of success. Nonetheless, the U.S. security business, considered as a whole, is preparing and planning to reduce those risks, protect the public, detect and deter criminal activity, and avoid corporate catastrophe.

To actually do all that, however, the security business must be in on the ground floor of discussions about mission design, engineering, and corporate planning. Among the more obvious security issues that could be discussed in these first stages of planning and design are the following:

- The installation and use of camera systems both in train stations and on the trains themselves;

- The protection of "designated" right of ways;

- The installation and use of intrusion-detection alarm systems, specifically including systems monitoring the detection of various chemicals;

- The plans and procedures needed to train and use bomb-sniffing dogs;

- The emergency planning required to ensure a quick and effective response from first responders;

- The law enforcement protocols required: (a) to detect and deter terrorist activities; and (b) to legally authorize requests for personal identification and/or the inspection of backpacks, attaché cases, and other carry-on packages; and

- The assignment of management responsibility for such high-level tasks as the development and use of emergency-alert procedures, evacuation planning, crisis management, and public affairs strategy.

Learning From Others To Create a Global Showcase

Wherever and whenever the first U.S. HSR system is established, it will be a "showcase" project that would be viewed by at least some terrorist groups as another opportunity to send a message to U.S. citizens, government, and allies throughout the world. Fortunately, there is much more that still can be done during the preliminary discussions and decision-making processes to fit security into the design and development stages of HSR planning.

A number of U.S. allies – Japan, Taiwan, Spain, Germany, Italy, South Korea, China, and the United Kingdom, for example – are already running successful HSR systems, and have been doing so for years. Many lessons can be learned by inviting representatives from those nations to attend a summit-level U.S. HSR security conference and to share, behind closed doors, the security methods and systems that have worked successfully in the past. There is much that the United States would gain by comparing notes and hosting such a high-level dialogue.

Similar efforts at previous passenger rail international conferences have proved to be highly valuable. Learning what is working in other systems would help the United States to adapt and adopt accordingly, thus saving money, improving defenses, protecting U.S. citizens (and visitors from other nations), and anchoring the current project designs.

At the end of these and other efforts, HSR security planning may still have the outward appearance of a relatively "small footprint," but behind the scenes will actually represent a highly sophisticated and effective strategic plan. Whatever else happens, security must ultimately be a strong and sturdy "pillar" in the design foundation for any HSR project. In short, it is not too early to start talking about security. In fact, given the size of this rather large and sometimes clumsy elephant in an already crowded room, it is becoming increasingly difficult, and now probably impossible, to ignore it.

William Rooney retired from the Central Intelligence Agency (CIA) after a 35-year career as a senior executive and field operations officer, which included assignment to various key posts in the CIA's Directorate of Operations. Most recently, he served as the chief of the Military and Special Programs Division, and as chief of the Latin American Division. He also received a number of awards, including a Distinguished Career Medal and the Donovan Award. After retiring from the CIA, he worked for a number of years at Amtrak, where his last position was Vice President for Security. He is the author of a fictional novel, entitled "Repeat: Whiskey Tango Foxtrot."

The Dangerous New World of the Social/Anti-Social Media

By Joseph Cahill, EMS

The use of social media has become so common that many people could not think of going through the day without using one or more of them for at least a few minutes – or several hours. Social media have in fact been used not only to keep citizens better informed about almost every topic imaginable but also to organize small groups, major cities, and entire nations on matters as diverse as family picnics, major weather events, and the overthrow of dictators. In short, social media are the new landscape of information, and emergency managers would be well advised to make better use of them.

Using social media effectively, however, should not start on the day of a major incident. The nature of social media is to cultivate a following that allows the user to communicate with his or her personal as well as professional connections. By creating a special brand for their agencies, therefore, public information officers (PIOs) and emergency managers alike can build a following that, on the day of an incident, enables information to be quickly pushed out to the public in a quick and frequently successful attempt to influence the actions and reactions of scores of individual citizens.

Each person represents his/her company or agency both on and off duty. Careful consideration is needed before any information – both professional and personal – is shared through any social media outlet.

The staff assigned to carry out this task have increased responsibility because they are now speaking for their entire agency – and everything they say or write will reflect directly on that agency. As with any other type of communications to the public, staff must ensure that the information they provide about an incident is as accurate as possible. Of course, they must also stay on message.

The Dark Side of the Force

Many users do not realize it, but there also is a darker side to the ability to instantly share one's own thoughts, witty comments, and other observations with the entire world. The Fire Department of New York (FDNY), to cite but one example, has been much in the news recently about certain posts made by FDNY members on certain social media outlets.

Although people have always "blown off steam" in various ways – complaining about their frustrations, for example – the big difference today is that social media posts are very public and long-lasting. Unfortunately, many users seem to have the illusion that social-media posts are private, and that unjustified assumption often leads to at least some people posting comments that they would never actually say aloud in the work environment.

The first amendment of the U.S. Constitution guarantees freedom of speech to all citizens, and even unpleasant speech is protected. For that reason alone, although public agencies and private businesses alike want to maintain their image, employers should check with legal counsel prior to announcing or agreeing with any proposed policy that may be perceived as infringing on the freedom of speech of their own employees.

A Uniform Policy Worth Considering

There is another legal reality that should be taken into consideration in such situations. Namely, that the posts may display the writer's actual feelings or the writer may simply be conforming to a group dynamic – but employers can still require staff to display professional behavior when representing the agency. Legal counsel should be consulted, therefore, to help determine what specific policies, current or proposed, meet the legal definition of "representing the agency." One example that might be cited: Listing an employer in a social media profile may constitute representing the agency

in much the same way that wearing a uniform off duty does.

Like private businesses, public agencies have the responsibility both to protect their own proprietary information and to ensure that confidential information – e.g., protected medical information as defined under the Health Insurance Portability and Accountability Act (HIPAA) – also is protected. Employers also have a right to expect their employees to be actually working while "on the clock" – and for that reason alone the company should be able to put in place the reasonable rules and/or technology controls needed to ensure an honest day's work from their employees.

Considered collectively, social media are an important and powerful new tool that today: (a) is changing how, when, and how much the world communicates; (b) is used by a steadily growing number of emergency agencies, businesses, and everyday citizens; and (c) requires the use of legal terms and the reasonable control of any proprietary information that is broadcast.

Following is a brief summary of some but by no means all of the more important "rules of the road" that official (or unofficial) spokespersons should remember when using social media:

- Nothing should be said or posted unless it is appropriate for the world to hear or read.
- The internet is forever.
- Information that is passed on should be fact checked, with authoritative sources – and the more a statement conforms to and/or reflects one's own personal beliefs or sympathies, the more thoroughly it should be vetted.
- When at work, staff should be actually working – not posting to social media sites (unless that is one of their official duties).
- Bosses and/or co-workers may want to keep professional relationships professional and have the right to turn down "friend requests."
- There is a reasonable expectation on the part of employers that any information that staff members have access to as part of their jobs will be held confidential – and may be required by some statutes.
- When representing an agency, what is done and said reflects on that agency in much the same way staff represent their agencies when they travel to and from work in uniform.

For additional training on social media for emergency managers, planners, responders, and receivers, the Federal Emergency Management Agency offers an online course (IS-42: Social Media in Emergency Management). Social media can, with proper training, serve as a valuable outlet for reaching the public in times of emergency.

Joseph Cahill is a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Prior to that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He 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 Montefiore Hospital.

Catastrophic Planning vs. Conventional Disaster Planning

By Dennis R. Schrader, CIP-R

There has been a debate over the past 10 years about the need to improve catastrophic planning at all levels of government. State and local jurisdictions are obligated to plan for higher probability non-catastrophic incidents, whereas the federal government is often perceived by the public as being the resource of last resort for low probability catastrophic incidents. Therefore, there is good reason to perform some pre-incident catastrophic planning to ensure that all parties can quickly and effectively carry out response and recovery operations in any major incident that would occupy the national media stage. The public will not tolerate slow reaction perceived to be a result of ineffective intergovernmental coordination.

To make matters more challenging, even when a low probability event occurs, the ability to predict that it will directly affect a specific geographical point on the national map is not realistic. So if a state or local jurisdiction invests resources for a specific catastrophic incident, there is still a chance that that area will not be the target when such an incident actually occurs.

The Differences in Planning Strategies

Claire B. Rubin, a social scientist affiliated for over a decade with The George Washington University Institute for Crisis, Disaster, and Risk Management, and co-founder of the *Journal of Homeland Security and Emergency Management*, has been researching the field for 34 years. In her book, *Emergency Management: The American Experience 1900-2010*, she defined "focusing events" as those that are so traumatizing they cause significant changes in the nation's approach to incident management. These focusing events include such calamitous incidents as the 1900 Galveston Hurricane, the 1906 San Francisco earthquake, the 1919 Spanish Flu Epidemic, the 9/11/01 terrorist attacks, and Hurricane Katrina in 2005.

Each time one of these events has occurred, the nation has attempted to improve its response capabilities. However, it could be argued that some of these events might be more easily described as not truly catastrophic – and, for that reason, the response system already in place would be capable of handling it.

The National Incident Management System (NIMS) and the Incident Command System (ICS) that evolved historically over the past 40 years – i.e., since development of FIRESCOPE in Southern California in the early 1970s – are based on the assumptions that: (a) There is a continuum of incidents that can be managed through a scalable system of structure and resources; and (b) Among those resources will be a broad spectrum of mutual aid that is often supported by federal resources.

The role of the federal government changed dramatically with passage of the 1950 Disaster Relief Act, which gave the President permanent authority to order appropriate federal action in such times of crisis. This authority was modified and changed in 1966, 1970, and 1974. The 1988 Robert T. Stafford Act not only expanded the Presidential authority to declare disasters but also made it much easier for state governors to obtain such disaster declarations. It might reasonably be argued, therefore, that the Stafford Act was not only a major step in a long-term movement to nationalize emergency management but also gives the federal government a strong incentive to manage pre-incident plans and activities to reduce future risks.

Incident Planning Efforts

Since the early 1990s, in fact, there have been several major efforts by the federal government to put more rigor into incident planning. The focus on catastrophic planning has gained greater momentum, of course, in the years that have passed since the 9/11 attacks and Hurricane Katrina. The 2006 Post-Katrina Emergency Management Reform Act actually prescribed certain very specific planning requirements.

The Regional Catastrophic Preparedness Grant Program was established in 2008 to explore these issues in 12 major urban areas in different states and regions of the country. The results of that 5-year exploration are now being reviewed, and the concepts involved, as well as their probable results, will be examined very carefully going forward.

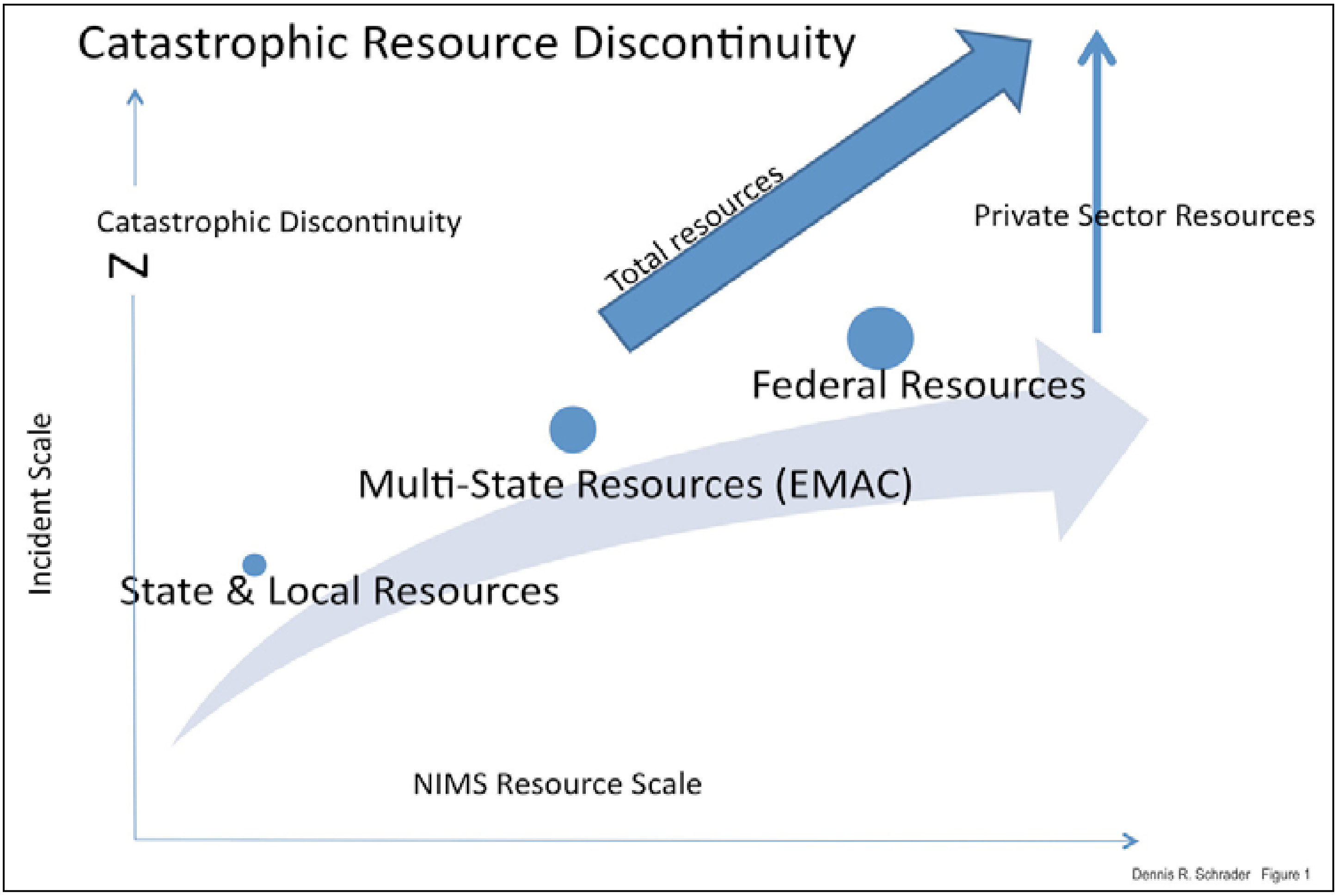
There still are several threshold questions that must be answered, though, including the following: (a) "Is catastrophic planning really necessary?" (b) "If so, how does it differ from conventional – i.e., previous – disaster planning?" (c) "Again, if so, how, and how much funding will be required to support and sustain the actions determined to be necessary?" The answers to those questions may well be included, or at least implied, in certain assumptions about the scalability of the NIMS and ICS concepts.

As shown in the chart below , there appears to be at least a few discontinuities – in the resource requirements and logistics processes postulated in the NIMS and ICS framework – that require a different thought process to plan for the response and recovery operations likely to be needed. These same discontinuities might also affect the approach taken to catastrophic planning – a still relatively new specialty skill that many jurisdictions below the federal level cannot afford to maintain. Moreover, a truly catastrophic incident would obviously require a multi-jurisdiction, multi-state response effort. One viable approach that might be taken, therefore, would be to maintain a small nucleus of people, experts in this field, who could maintain cotinuity over a number of years and share their collective capabilities both regionally and nationally.

Guarding Lifeline Infrastructures

Another important point to remember is that the rapid recovery of private-sector lifeline infrastructures is a key to catastrophic recovery. In the National Capital Region's 2012 Strategic Playbook, Philip J. Palin, a staff member of the Center for Homeland Defense and Security at the Naval Postgraduate School, examined the probable impact on supply chains caused by a catastropic incident affecting infrastructures. Solving what might loosely be called "the infrastructure problem" would require, among other things, he said, full and effective cooperation between and among officials of the U.S. Department of Homeland Security's Federal Emergency Management Agency, the states and urban areas directly involved, and the private sector.

The most difficult challenge here, probably, might be that the federal government cannot and should not unilaterally


Catastrophic Resource Discontinuity
Catastrophic Discontinuity
Total resources
Private Sector Resources
Federal Resources
Multi-State Resources (EMAC)
State & Local Resources
Incident Scale
NIMS Resource Scale
Dennis R. Schrader Figure 1

direct the alignment of the many other political jurisdictions directly involved. There must be, though, both a horizontal network and a cooperative effort that makes state and local governments also responsible.

It may also be prudent to spend more time in the research and analysis phase of the planning process used to deal with many catastrophic events. For example, in the mid-Atlantic region, there is already a Fleet Movement Group sponsored by the All Hazards Consortium studying the effects of moving power-sector mobile assets such as trucks and crews through multiple jurisdictions to speed the recovery process for power and thereby facilitate the rapid recovery of lifeline sectors, such as food, water, and telecommunications. This type of analysis makes the planning process yield more effective and tangible results.

The correct approach to resolving this problem may lie in resourcing the planning effort through cooperative working relationships and intergovernmental personnel agreements between the different levels of government. These tools already exist and may hold the key to resolving the dilemma caused by the cost and personnel considerations involved in planning even some low probability events.

The preceding factors and a number of other issues should continue to be studied, obviously, especially in light of the results of the Regional Catastrophic Preparedness Grant Program that are starting to emerge from various jurisdictions around the nation. The notion of catastrophic discontinuity and the differences that it produces bear particularly close scrutiny in the long-running debate over catastrophic planning. Only after generally accepted answers and solutions are agreed upon, it seems, can the threshold questions mentioned above be answered.

Dennis R. Schrader is President of DRS International LLC and former deputy administrator of the Federal Emergency Management Agency'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. Dennis currently provides Senior Consulting services at Integrity Consulting Solutions, LLC.

Avoiding the Threat Posed by Predictive Certainty

By Michael Vesely, Emergency Management

The University of Maryland Center for Health and Homeland Security (CHHS) was recently tasked with developing the security plan and value assessment for a large metropolitan transit agency that uses close to 400 transit coaches to carry almost 30 million riders annually. During peak travel hours, the agency (which for propietary reasons cannot be identified more specifically) has more than 300 of its 30- to 40-foot coaches in service at any given time.

The intent of developing a security plan was to establish a broad spectrum of strategies that could be implemented over the course of several years. To develop such a plan, it was determined that an initial assessment of the various sites controlled by the agency would be needed and should include the agency's executive building, depots, transit centers, bus stops, and various park-and-ride lots as well as the agency's training academy. In short, the agency had to deal with all of the typical problems and operational issues facing any other large local agency. Because of its proximity to one of the nation's largest metropolitan areas, however, the number of potential targets significantly increased the risk profile.

The CHHS effort highlighted several fundamental concerns with potentially far-reaching effects including the fact that risk modeling often uses extremely technical and complex formulas with limited value and can actually increase risk, rather than reduce it. Such models also can be both expensive and time-consuming. Another major concern was that it is extremely difficult to predict acts of terrorism – and efforts to do so can lead to a false sense of security. Moreover, the use of highly complex risk models to accurately forecast future events can sometimes lead to higher levels of risk exposure simply because of a false belief in the accuracy of what is almost always an extremely complicated assessment.

Quick Overview of a Complicated Process

In developing the threat profiles of the various sites analyzed, the CHHS team used many of the usual sources of information that transit agencies across the country would be able to access within their own jurisdictions. The first step was to consider the types of assets involved – for example, operational centers, staging areas, transit staff personnel at those locations, as well as their current duties and responsibilities.

Also taken into consideration were flood maps and the crime statistics for each area, the number of commuters likely on any given day, after-action reports of previous incidents, and the opinions, insights, and recommendations provided by agency employees. The team also took careful note of the number of vehicles and passengers likely to be present at each site at any given time.

Although risk assessments come in a variety of forms and employ different approaches, there are certain core elements common to most of them, including: (a) a careful analysis of the value of the physical assets involved; (b) the potential impact of a dangerous incident or event; and (c) the probability of such an event occurring. The value of the assets involved is then quantified in economic and operational terms based on variables such as the construction costs of the facility, the revenue generation provided by the site, the potential cost of using alternate sites in times of sudden emergencies, and the contributions that the site brings to the company's operations as a whole.

To understand the possible impact of various types of incidents, the first question usually asked is, "What would happen if the company were to lose all or part of this site?" After that question is answered, the next steps are to consider the severity of past events, physically inspect the sites involved, and determine as accurately as possible what various types of incidents would adversely affect the physical integrity and operational status of the site. By using this reductive approach, the CHHS team was able to make certain reasonably accurate determinations about the impact that various types of incidents could have not only on the individual sites but also on the transit agency as a whole.

The likelihood that a certain type of incident will occur, though, is much more difficult to determine. Even the most detailed and accurate consideration of crime and usage statistics, flood maps, and after-action reports to determine probable trends will usually generate a number of best-guess answers and estimates. As the project team discovered while researching the data sources for models and formulas used by other jurisdictions, the more technical models offered more accurate results. Unfortunately, the more technical models are more difficult to fully comprehend, interpret, and act upon the results.

Earthquakes & Overcoats – Limits of Prediction

This was not nor should have been a surprise. Experience shows that the use of predictive models is often not worth the time and/or effort involved if only because the world at large is so incredibly complex. Moreover, most people including experts tend to overestimate their own ability to predict what is likely to happen in or because of certain assumptions and/or circumstances.

This tendency is both reasonable and understandable. When people choose their clothing based on the weather prediction for the day, they can quickly adapt to sudden changes by donning a sweater, doffing a winter coat, or using an umbrella to compensate for an inaccurate prediction. However, earthquakes, terrorist attacks, and other major unexpected incidents are much more difficult to prepare for. Although planners have long understood that long-term projections must be reasonably flexible, they often fail to incorporate enough flexibility into their projections of potential risks and likely threats.

> *Although there are few if any absolute certainties in today's increasingly complex world, it is often easier to assign a specific value to certain assets than to predict, from a broad range of possibilities, what might happen to them.*

There is another risk factor involved in such projections that is not always acknowledged: human nature. Whether considering crisis management, stock market predictions, or the outcome of various sporting events, the theoretical "lesson learned" is usually the same: The analysts and planners involved ascribe correctly predicted outcomes to their own insights and personal expertise. But when the outcomes are incorrect, the same experts are quick to point out previously unknown (or misunderstood) factors that adversely affected the outcome. Unfortunately, there are far too many factors and variables involved in major projects to fully identify, let alone quantify, the numerous future risks, potential dangers, and a broad spectrum of probable, possible, and/or unlikely results needed to produce the reasonably accurate risk scores needed and expected. The false expectation of at least some planners, therefore, is that if more refined – i.e., more complex – risk models are used, more accurate predictions can be developed, the correct actions can be recommended, and the overall risks can be reduced.

The Dangerous Use of Overly Complex Predictive Models

There are, in short, numerous concerns involved, specifically including the inefficient use of increasingly scarce resources, when overly complex risk models are used. These concerns are magnified when planners overestimate the ability of such models to fully capture the nature and types of risk involved and recommend the spending of additional resources to develop increasingly complicated formulas designed to capture the essence of such risks within a particular context. Adhering more closely to some of the basic values – especially flexibility and adaptability – postulated in the National Incident Management System (NIMS) would significantly mitigate such concerns.

Another risk involved in developing relatively complex risk assessments is the creation of misplaced confidence. As such assessments become even more complex, and consequently less understandable, a perplexing inversion sometimes takes place: Those who use the assessments to develop operational plans often gain more confidence, irrespective of the fact that they may not fully understand the additional complexities involved. Deciding how to best use resources to reduce risk can be a daunting task in any circumstances, and an accurate assessment should provide at least a starting point that is supposedly grounded in hard numbers. But when an assessment is completed that does not provide a comprehensive understanding of all possible risks, the managers and decision makers involved may fail to fully consider threats that receive lower or no priority in the assessments.

Additional problems develop, of course, when risk assessments are so general in their doctrinal approach that the results and recommendations developed are little more than speculation. Another danger that should be taken into consideration is that highly technical assessments seem to provide a solution to the problem by defining a course of action that is solely quantitative – ignoring the fact that the underlying reality of today's dangerous world defies classification in simply mathematical terms.

The Way Forward: Numbers Are Not Reality

In some ways, models are a necessary evil. Ideally, planners would consider a broad spectrum of scenarios, recommend approaches that would be taken when unlimited time and resources are available, and postulate flexible protocols that would provide helpful guidelines without adversely affecting emergency needs. However, the usual scarcity of time and lack of material resources make it impossible to bring all necessary participants into the more detailed type of planning structure needed to consider and implement the actions required to counter the dangers that must be confronted.

In short, when analyzing the risks facing various assets and operations, it is necessary to: (a) categorize various overarching risk levels; (b) facilitate a comprehensive and accurate discussion of the various types of risks involved; and (c) establish a common nomenclature that would facilitate both an understanding of the various risks involved and the promotion of an open discussion of the actions that must be taken.

Fortunately, the CHHS project team adopted a numerical approach for classifying the various risks involved for the transit agency, but also recognized that it was important to adhere to a single guiding principle – namely, that reality cannot be expressed in numbers alone. To be both useful and significant, the numbers used must be accompanied by enough descriptive language to build an understandable and "doable" context for the decision makers responsible for using the assessments made by the project team.

Conscientious Avoidance to Enhance Operational Resiliency

Because some of the predictive quantities were so amorphous, and therefore somewhat unreliable, the team put special focus on determining the value of the assets in question. From there, the team used reductive reasoning to measure various impacts that could affect each of the assets involved. While maintaining an all-hazards approach, the team focused on determining what capabilities were in fact needed to enhance the resiliency of the various assets being considered. Finally, after these foundational principles had been determined, the team considered the probability of various potential events – but conscientiously avoided the development of specific predictions. The goal from the beginning was to: (a) define understandable protocols that would focus on minimizing loss, no matter what the cause; and (b) ensure that the valuable insights and information that staff members possess were fully and effectively integrated into a robust and useful assessment.

Today's world is an extremely complicated place and there are too many complex factors, too many variables, and too many random events and circumstances to accurately predict exactly what will happen in the future. As various risk models become increasingly complex, the information developed by those assessments also becomes more complicated – and thus less useful to those responsible for implementing and acting upon them. In addition, overconfidence in an agency's understanding of its risk profile can lead to courses of action that may dramatically increase an organization's exposure to risk.

A more effective approach might be to begin an assessment from the perspective of valuing the asset and determining the impact likely if it were damaged, destroyed, or otherwise made unavailable. Plans, procedures, and protocols could then be developed to enhance the resiliency of the asset. The bottom line is that, by emphasizing flexibility and adaptability, most physical assets and resources can become more secure and less exposed to threats across the full all-hazards spectrum.

For a thorough discussion of risk and the limits of forecasting, please see Nassim Nicholas Taleb, Antifragile: Things that Gain from Disorder (2012).

Michael Vesely is a certified instructor of COOP, Incident Command Systems (ICS), and other DHS homeland security courses. He led the team responsible for rewriting the Homeland Security Strategic Plan for the National Capital Region, and also worked as a planner for the Mid-Atlantic Regional Center of Excellence for Biodefense and Emerging Infectious Diseases Research. He holds a J.D. degree from the University of Maryland School of Law and currently plays a leading role on economic security issues in the University of Maryland's Center for Health & Homeland Security.

protected by emergent biosolutions™

Emergent BioSolutions Inc.
2273 Research Boulevard, Suite 400 • Rockville, MD 20850 • USA
Phone: 301-795-1800 • Fax: 301-795-1899 • www.emergentbiosolutions.com