domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 9 Issue 9, September 2013

New Normals?


THE UNTHINKABLE HAPPENED
WHAT'S NEXT?
SALAMANDER
WHEN IT MATTERS
When the unthinkable happened in Van Buren County, Arkansas, Salamander was there. Click below to learn more.
FIND OUT MORE | TALK TO AN EXPERT
Salamanderlive.com/VanBuren | 877.430.5171

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

Susan Collins
Associate Publisher
scollins@domprep.com

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

Catherine Feinman
Editor
cfeinman@domprep.com

Carole Parker
Customer Service Representative
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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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 their use or interpretation.

IMR GROUP

Editor's Notes

By James D. Hessman

Floods, earthquakes, tornadoes, tsunamis, hurricanes, and various other natural disasters have been plaguing communities for millennia and will continue to do so far into the foreseeable future. Millions of lives have been lost, entire cities have been destroyed, crops have been ruined, and the cumulative financial cost is incalculable.

Floods have caused the greatest damage – both in terms of the lives lost and the material resources destroyed. In the United States itself, more than 95 percent of all federally declared disasters in recent years have been accompanied by at least some measurable amount of flooding. Joseph Cahill spells out the unique flooding problems affecting smaller town and villages – which sometimes are reduced to the status of "island communities."

Current attitudes must change, according to Terri Turner and George Deussen, two of the authors contributing to this month's "roundup" issue of *DPJ*. Fortunately, new and more advanced technology is now available – geographic information systems (GIS), for example. If used early and properly, says Stephen McElroy, GIS not only will save lives and money but also will help communities cope successfully with a broad range of other problems. Natalie Lehr ups the ante by pointing out that the mitigation of all types of risks will lead to many other benefits – some are intangible, some will reduce government expenditures, and some will add significantly to the private sector's collective tangible resources. And Charles Werner discusses how use of the DHS Homeland Security Information Network is already helping one city in Virginia upgrade its own pre-disaster contingency plans.

The future can and will be even brighter, say Dane Egli and John Contestabile, who provide an insider's look at ten "key findings" that were developed by thought leaders from communities throughout the nation at a high-level Capabilities Analysis Exercise. That exercise focused not only on what could and should be done in pre-disaster planning but also addressed possible problems that might be encountered and the steps that should be taken to resolve those problems.

In addition, Jamie Stowe points out the many ways in which the U.S. Department of Defense has been helping many local communities – and U.S. allies as well (Haiti, Japan, and Chile, to cite three recent examples) – cope with a broad spectrum of major problems before, during, and after numerous weather-related disasters. Jennifer Ryan discusses the broad spectrum of problems associated with various special events throughout the nation – the Boston Marathon attacks are perhaps the best recent example. William Anderson rounds out the issue by enumerating seven key suggestions developed by The Infrastructure Security Partnership (TISP) to upgrade the "national strategy for critical infrastructure security and resilience."

About the Cover: Jamestown, Colorado, a small Boulder County mountain town of about 300 citizens, was among the communities cut off by the massive flooding earlier this month in that much beleaguered state (FEMA photo by Steven Zumwalt). This month's printable issue of DPJ focuses special attention on mitigating and recovering from floods and other major disasters – both natural and manmade.

DomPrep Writers

Raphael M. Barishansky
Public Health

Joseph Cahill
EMS

Craig DeAtley
Public Health

Kay C. Goss
Emergency Management

Stephen Grainer
Fire/HazMat

Rodrigo (Roddy) Moscoso
Law Enforcement

Corey Ranslem
Coast Guard

Glen Rudner
Fire/HazMat

Richard Schoeberl
Law Enforcement

Dennis R. Schrader
CIP-R

Joseph Trindal
Law Enforcement

Saving Lives & Protecting Property: A Flood of Helpful Information

By Terri Turner & George Deussen, Building Protection

Flooding is the most pervasive, geographically distributed, and closely regulated natural disaster in the United States. Nonetheless, the damaging trends continue despite such safeguards and efforts as: (a) the creation of a National Flood Insurance Program (NFIP); (b) billions of dollars (and significant manpower) invested in flood management efforts; (c) numerous scientific analyses and official reports dedicated to alleviating the flood problem; and (d) the enactment, at all levels of government, of numerous laws and regulations.

Since 2011, more than 95 percent of all federally declared disasters have been water-related in one way or another. That total includes 96 of the 99 major disaster declarations issued by the Federal Emergency Management Agency (FEMA) in 2011 – and 44 of the 47 similar FEMA declarations in 2012. Occurring in those same two years, thousands of smaller flood events – also damaging, but below the level of a declared disaster – caused a massive loss of life and property, the disruption of numerous goods and services, and a major decline in the overall "well-being" of the citizens living in many large and small communities throughout the nation.

According to a 1998 article, *Secular Trends of Precipitation Amount, Frequency, and Intensity in the United States*, published by the American Meteorological Society, flooding events in the United States have been increasing in both frequency and intensity over the past 50 years. The National Oceanic and Atmospheric Administration (NOAA) estimates that the 30-year flood loss from 1983 to 2012 averaged $58.2 billion in damages and caused an average of 89 deaths per year over the same time frame. The highest losses were inflicted by two major hurricanes that also, according to FEMA, were the two most costly flood-related disasters in the nation's history: Katrina in 2005 ($145 billion in property damage and 1,833 deaths); and Sandy in 2012 ($68 billion in property damage and 148 deaths).

What Might Have Been, But Was Not

What in retrospect made those two hurricanes even more damaging, unfortunately, was that: (a) both of them passed through areas that had been long predicted by weather experts to flood; (b) the states most heavily damaged had carried out a number of pre-event exercises focused primarily on floods; and (c) despite several days of advance warning prior to landfall, the states most severely affected were still relatively unprepared.

The effects of Katrina on the lower income and more vulnerable housing areas in New Orleans were clear both from the air and on the ground, especially in the Crescent City's Lower Ninth Ward. Sandy made landfall much farther north, destroying entire communities in both New Jersey and

New York. Lower Manhattan, in fact, suffered some of the heaviest damage and was still using temporary cell towers nine months after the flooding of Wall Street.

Moreover, billions of dollars of critical assets were left totally unprotected during these and a number of other national flood events. In short, thousands of lives throughout the United States have been lost, shortened, and/or diminished in quality in recent years, largely as a result of government officials failing to adequately plan, prepare, and mitigate *long before* such catastrophic events actually occur.

Creative Innovations, Plus a Map to the Future

FEMA, the federal agency holding the greatest responsibility for disaster preparedness, defines mitigation as "the effort to reduce loss of life and property by lessening the impact of disasters." The agency has worked to reduce the harmful impact of floods (and other natural disasters) by, among other things:

1. *Developing and promulgating* a rigorous mitigation education and outreach campaign;

2. *Sustaining* an ongoing mitigation planning program, which identifies various policies and preventive actions that can be implemented over the long term to reduce risk and future losses;

3. *Making available* to communities throughout the nation such innovative programs as Risk MAP – the "vision" for which, FEMA says, "is to deliver quality data that increases public awareness and leads to action that reduces risk to life and property"; and

4. *Creating* a National Mitigation Framework that provides context for how a "whole community" can and should work together, as well as how mitigation relates to other aspects of national preparedness to foster a culture of preparedness that is centered on risk and resilience.

The Nation as a Whole – And All Local Communities

The nation as a whole, and communities large and small in every state, can learn some valuable lessons from the retail, distribution, and service industries on how to mitigate the threat to the collective critical infrastructure. A key goal in the management of supply chain networks, for example, is to pre-stage critical assets and material resources in locations where they can be used immediately or shipped quickly to another location in advance of, in the eye of, or immediately after a flood event or major storm actually occurs.

Major storms and the floods that follow are inevitable, and undoubtedly will be so for many years to come. Nonetheless, researchers, economists, city planners, and mitigation experts are in general agreement that such events will have a less damaging impact only if the federal government and the nation's state, regional, tribal, and local communities take the proactive steps needed to mitigate – by effective planning, pre-staging of mitigation tools, and preparing to engage – these potentially devastating storms through the development and early implementation of effective solutions.

The most sustainable and most resilient communities are today, and will be for the foreseeable future, those that use every mechanism available to deal with the various threats and hazards facing them. Flooding has been, is, and undoubtedly will continue to be a major threat to almost all U.S. communities, whatever their size and importance, for many years to come – unless and until the nation as a whole, and all of its communities, significantly improve their mitigation and preparedness efforts in advance of the next Katrina, Sandy, or as-yet unnamed hurricane (or similar disaster).

Terri Turner, AICP, CFM, (pictured) is the development administrator for the Augusta (Ga.) Planning and Development Department and is also the community lead for Augusta's Resilient Neighbors Network. Additionally, she serves as the liaison on the Urban Water Sustainability Council, the Region IV director and NAI (No Adverse Impact) Committee co-chair of the Association of State Floodplain Managers (ASFPM). She previously served as a member of the CRS Outreach Criteria Review Team and on the PPD-8 – National Mitigation Framework – Core Writing Team. She has received many awards for her work, including the 2012 Champions of Change Award given by the White House.

George Deussen is vice president of Muscle Wall, LLC, and a member of the Non-Structural Flood Proofing Committee of the Association of State Floodplain Managers. He possesses special expertise in flood control, containment, storm water management, mitigation, business continuity, emergency management, environmental risk management, business development, sales, marketing, and strategic development.

Building Resilience Early & Geographically

By Stephen McElroy, Emergency Management

Geographic information systems (GIS) have become standard tools used for addressing large-scale disasters. Following the 2010 earthquake in Haiti, the 2011 tsunami in Japan, and the fast-moving tornado in Moore, Oklahoma, earlier this year, GIS and other geospatial technologies helped relief workers prioritize their efforts, supported natural resource assessments, assisted in insurance and damage assessments, and provided officials with the data they needed to make crucial decisions.

The common denominator in these and other applications is that all of them involve inter-related aspects of remediation and repair operations. However, although geospatial technologies are a major asset during the rescue and restoration phases of an operation, they also can play an important role before disaster strikes. As a proactive tool, for example, GIS has helped not only to develop and improve community resilience to disasters and dangers of all types but also to prepare communities, disaster professionals, first responders, government agencies, and private citizens to deal more effectively with the potential consequences of specific disasters.

Documenting before and after a disaster, identifying threats, and planning for egress of residents – as well as ingress of relief efforts – are the three sturdy legs of the geographic information systems readiness tripod.

The shift from reaction to anticipation encompasses three major areas of emphasis: documentation; threat identification; and evacuation and relief planning. Following are a few specifics about each.

Documentation – Comparing the Before & After

When a disaster transforms what was once familiar into the unfamiliar, the ability to pinpoint the location of essential resources can be a major challenge for responders. Violent forces of nature – typhoons, earthquakes, etc. – have the ability to totally reshape landscapes and destroy well-known landmarks, leaving even local residents disoriented. The floods caused by Hurricane Irene in 2011, to cite but one example, washed away several roads and even shifted the courses of some rivers in New England.

In addition, after-action reports about various tornadoes that have devastated several areas in the U.S. Midwest over the past several years described the unforeseen ways in which entire blocks of homes and businesses were completely destroyed, making navigation through a devastated neighborhood always difficult and sometimes impossible. Knowing in advance where various "things" are, or were, is therefore the first and perhaps most important step that must be taken before any effective action can be initiated after a major natural disaster. Among the key initial tasks that must be carried out are: (a) locating utility poles (for electrical crews); (b) identifying hydrants and/or other reliable sources of water (for firefighters); and (c) avoiding natural gas pipes, water mains, and electrical cables – particularly when construction crews are digging.

Traditional maps are static and show an area of a specific city or town only as it previously appeared. By combining a GIS database with critical related information and global positioning systems (GPS) to determine a more precise location, emergency crews can be helped to maneuver their way through what might otherwise be simply piles of rubble, tree branches, and other debris. Moreover, rather than working with only pre-disaster information available, a GIS system that can deliver additional and/or updated information to mobile devices, as quickly as possible, can provide emergency personnel with visuals of the same area overlaid with images of current conditions. Important and/or visually

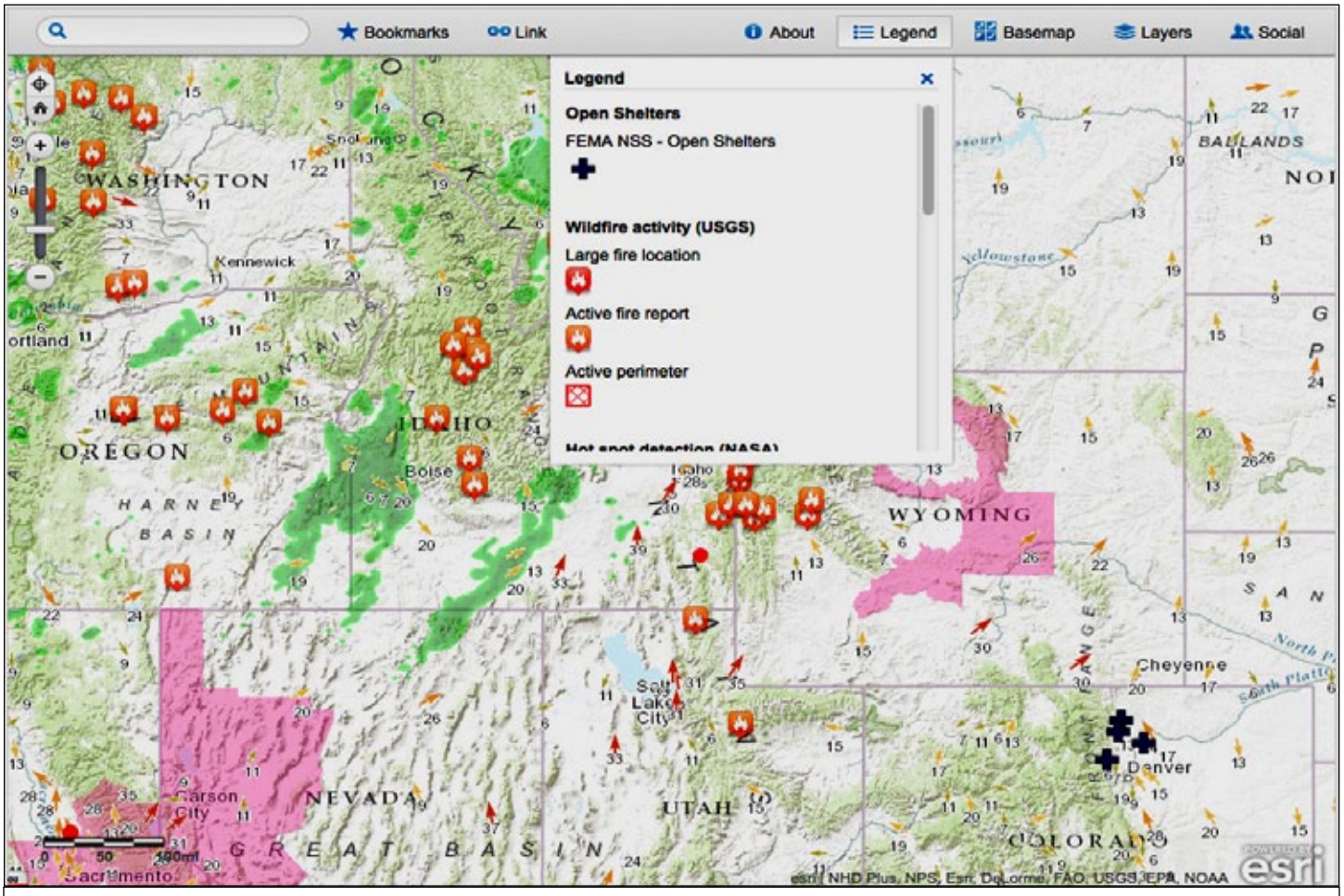
prominent features, natural resources, and potential dangers could be highlighted to help emergency crews work safely and more efficiently.

Threat Identification – Beyond Terrorism & Security

For a response team, being spatially oriented within a specific geographical area is a vital step in coping with a natural disaster or any other type of emergency situation. But any response effort will undoubtedly be stronger if more time has been taken, in advance, to anticipate a potential problem and to plan accordingly. In that context, it should be emphasized that specific threat identification – although usually associated with terrorism and security issues – is actually a broader concept that also can be used as a powerful tool for advanced readiness. Even a weather report is, in a sense, an early warning system for potentially adverse meteorological events.

GIS provides substantial sophistication and nuance to any type of threat identification – weather, for example. Almost all weather forecasts offer general predictions of the most likely weather conditions that can be expected over a fairly large land area in the next several hours or even days. But most actual weather events affect each smaller area within the large area in at least somewhat different ways, depending on such variable factors as the ground cover involved, the type and location of local drainage systems, the sewer or septic services available, ground stability, the structural design of large buildings, and land use. Because each and all of these factors vary dramatically over distances as short as a few feet, the impact of weather on two places relatively close to one another may differ significantly in terms of flooding, wind and heat conditions, and the potential damages likely in the aftermath of a major storm.

For all of these reasons, it is imperative that well-prepared community and response teams have a clear



View of an interactive map of U.S. wildfire locations. This map is part of ArcGIS solution services provided by ESRI.

sense, to the utmost degree possible, of oncoming danger – whether or not that danger is caused by natural conditions, industrial accidents, and/or human intervention. To prepare for any and all of these dangers, GIS models deliver capabilities that: (a) show, in geographic detail, several ways in which various scenarios might play out; and (b) then provide impact updates as an event unfolds.

GIS models take into account such variables as terrain, building plans, and even such rapidly changing factors as high winds. Modeling can identify relatively small differences that can send a major fire in one direction, for example, thereby allowing decision-making officials to position their resources accordingly. Modeling also can show the level at which a certain amount of rain or surface water overflow would cause sewers to back up, which would suddenly push the flooding danger into high gear. The basic rule to remember is that, the more information that is available, the more effectively responders and decision-makers can react.

Evacuation & Relief Planning – Building on a Solid Foundation

The third leg of the GIS readiness tripod is evacuation and relief planning. Under particularly adverse conditions, it may become necessary to evacuate residents from any given neighborhood. But different types of events might require different types of evacuation. An industrial accident at a power plant, for instance, might release hazardous materials that, given an uncertain wind or storm pattern, would make travel in a particular direction more dangerous or even impossible. To make evacuation planning more effective and more comprehensive in scale, such planning should ideally be initiated in conjunction with full threat identification and modeling. Later, as the specifics of any given threat become clearer, the most appropriate evacuation plan can be determined.

In a similar way, resilience means the ability to recover and recuperate from trouble – but that ability requires that the proper resources are brought to bear, as quickly and safely as possible. Whether already locally positioned or transported into the affected area, those resources must be moved along the fastest and safest path available. Again, thanks to the help of GIS, planners also can develop efficient reverse-evacuation routes, using such factors that can be tracked within the system as: (a) the size, nature, and number of delivery vehicles; (b) the weight limits for certain roads (including those with potentially degraded conditions); (c) the clear travel paths most likely to be available; and (d) the most efficient pre-staging locations that should be used.

As with the evacuation plans mentioned earlier, the transport of needed resources requires the use of real-time updates on what might well be changing weather or other conditions. However, with the bulk of the groundwork already done, officials usually would be able to concentrate their attention on a flexible adaptation of strategies rather than creating a new response plan to cope with a new threat.

The GIS Readiness Tripod

Without full documentation of an area created in advance of a disaster, emergency and relief personnel must work with blinders on. Threats that are recognized only upon arrival restrict the ability of emergency teams to respond in a coherent and effective manner. Moreover, the logistics of evacuation and the transportation of relief resources can vary significantly, depending on the nature of the disaster and how it unfolds.

The most important aspect of creating a resilient community is being as prepared as possible, as early as possible, so that response and recovery personnel do not lose unnecessary time while making decisions and altering general strategies when the clock is already ticking. Because unforeseen events and responses often are deeply affected by geographic specifics, the use of GIS adds a helpful degree of insight, specificity, and flexibility – important albeit unquantifiable variables that are not possible, to the same extent, with the use of strictly conventional tools.

Stephen McElroy, GIS program chair at American Sentinel University, has been in the GIS field for more than 15 years, working as a GIS technician for the U.S. Department of Agriculture, Agricultural Research Service, Southwest Watershed Research Center, and as a senior research specialist for the Udall Center for Studies in Public Policy and the Department of Soil, Water, and Environmental Sciences at the University of Arizona. He holds a Ph.D. in geography from the joint doctoral program at San Diego State University and the University of California, Santa Barbara, and a certification from the GIS Certification Institute.

Mitigating Risk: Protecting & Defending Critical Infrastructure

By Natalie Lehr, Private Sector

Leaders of various critical infrastructure sectors – such as energy, telecommunications, electricity generation, gas production, water supply, and waste disposal – must be able to effectively manage the vulnerabilities associated with providing high-quality services to the public while at the same time securing those sectors from physical and intellectual harm. Unlike companies that provide tangible products and traditional services, the owners and operators of critical infrastructure do not have the luxury of sequestering their assets.

In fact, simply by supplying important services that are essential for society to function properly and without interruption, these firms are both physically and virtually exposed. Moreover, because the same companies fill a critical role in managing business operations and facilitating economic recovery, they must also carefully balance: (a) pursuing new investments that take advantage of global sourcing; and (b) mitigating problems related to and/or caused by geopolitical volatility and competitive risk. For example, a dramatic increase in demand for mobile Internet, smartphones, and PDAs (personal digital assistants) has caused several U.S. telecommunications companies to shift a significant share of their capital investments to capture increasingly higher revenue streams.

Leaked information poses a serious threat not only to the operations and financial stability of critical infrastructure but also to their short- and long-term brand value.

Developing a flexible and robust infrastructure that meets the increasing demands of a globally interconnected community becomes essential in the short term as well as in the long term because of the anticipated growth in service revenue desired by customers. To satisfy this demand and to best position themselves for a continuing evolution, telecommunications firms must leverage international vendors and supply chains while at the same time defending their own infrastructures from risks that overseas collaboration ventures inevitably create. In addition, after initial investment decisions are made, the next steps – required maintenance, installation, and training – will almost always extend the risk timeline into the lifecycle of the equipment used as well as the overall operating network.

Two Notorious Examples: Google and WikiLeaks

In 2010, revelations of network intrusions at Google – preceded by the massive WikiLeaks exposure of countless sensitive government documents – vividly illustrate how the blurring of politically and financially entangled circumstances poses major risks for business and government alike. In the WikiLeaks exposure, Bradley Manning, a 22-year-old intelligence analyst, was able to download and disclose/distribute literally hundreds of thousands of classified documents before he was detected – and later sentenced to 35 years in prison.

The Google incident was considerably different, but nonetheless harmful to U.S. interests. It started when the company experienced a six-month advanced persistent threat (APT) attack, dubbed "Operation Aurora," that apparently originated in China. The lesson provided by both situations was much the same: Regardless of origin and/or intent – and whether state or criminally sponsored – such threats dramatically illustrate the myriad of challenges that the private sector now faces in seeking to protect essential information.

Such events may seriously impair operations, financially harm any company involved, and/or damage the value of the brand. U.S. government agencies have the ability to retreat and segregate their most sensitive material in ultra-secure facilities, at a cost unknown to U.S. taxpayers. But private-sector companies do not have this same privilege, so must operate their geographically distributed personnel, facilities, and networks as

securely as possible, even when: (a) engaging an ever growing number of partners; (b) outsourcing additional elements of the business (to further enhance the bottom line); and (c) meeting the profit expectations of their ever vigilant shareholders.

The same two examples illustrate an increasingly difficult problem – namely, that numerous foreign and domestic malefactors are now profiting from, disrupting, and/or otherwise harming the nation's critical infrastructure. Experience shows, though, that the best defense against such activities is a vigorous and proactive offense. Not in the sense of a competitive espionage program but, rather, in the active and unified management of unwanted exposure within the public sphere.

The Growing Danger Posed by Insider Threats

In various ways similar to those common in other knowledge-intensive industries, U.S. critical infrastructure companies are particularly vulnerable to insider threats. Individual employees as well as subcontractors have access to and understand the market value of the materials, systems, and operations entrusted to them. Even properly sanctioned work may be vulnerable to information spills and/or inadvertent disclosures that not only create and expand vulnerabilities but also result in regulatory or compliance liabilities.

Much more threatening, however, are the deliberate and calculated efforts of persons with access, capability, and intent to harm a company. As the 2010 WikiLeaks' case demonstrated, the financial cost and physical resources needed to cause incalculable harm to any given company, and/or to the federal government, are nominal – even to individual "lone wolf" attackers. But the damage caused by just one angry or disgruntled employee of a gas or power company, for example, could be devastating to an entire community, and could disrupt normal operations for an extended period of time.

To guard against such threats, the nation's entire critical infrastructure industry now manages a veritable mountain of custodial data and regulatory compliance information. The protection of such custodial and personal information is obviously growing in importance, particularly given the increasing liabilities associated with the disclosure of custodial data – as was vividly demonstrated by the aggressive Massachusetts Data Breach Law of 2008.

A Comprehensive Approach & Proactive Plan of Action

With no sign that such dangers are abating, and with limited resources dedicated to "security," critical infrastructure managers must ensure they are positioned to protect their companies from not only a broad range of liabilities (fines, lawsuits, adverse publicity) resulting from the spillage of toxic data but also from the loss or pilferage of valuable corporate secrets (financials, partnerships, technologies).

As critical infrastructure companies assess opportunities to transfer, reduce, or accept risks in the operation of their various businesses, they also must position themselves to optimize their options based on a unified organizational examination that is both broad and deep. Only through the unified management of a company's capital assets and business relationships can it optimize future selections from the broad range of actions that simultaneously mitigate risks and proactively layer the legal and structural defenses.

Although the costs created by and arising from compliance activities are more readily measured, the long-term losses associated with the exposure of valuable corporate secrets are, in fact, far more extensive and expensive. Those responsible for ensuring the security of critical infrastructure assets – from an economic point of view as well as from public health and safety perspectives – cannot afford to provide more protection for one asset than another. The time has come for a truly comprehensive approach to protect and defend critical infrastructure organizations.

Natalie Lehr is a co-founder and director of analytics at Tailored Solutions and Consulting (TSC), an enterprise risk consultancy based in Washington, D.C., specializing in intellectual asset protection. With more than 15 years of experience as an intelligence professional, her expertise spans both the government and commercial sectors. Her work for the U.S. government includes extensive experience in the identification, acquisition, and development of critical information, supporting high-value national security interests. In the commercial arena, she led the development of innovative methods to acquire and analyze critical information to protect specific interests and high-value intellectual assets. She holds a master's degree in International Relations from Yale University.

Operationalizing the Nation's Critical Infrastructure Resilience

By Dane Egli & John Contestabile, CIP-R

Bringing together the nation's public, private, and academic stakeholders from diverse preparedness communities – and the owners and operators of U.S. critical infrastructure facilities – is a daunting but necessary task. That becomes even more challenging, though, when trying to implement resilience plans at the local, regional, state, and federal levels.

To address these challenges, Johns Hopkins University's Applied Physics Laboratory (APL), already designated as a University Affiliated Research Center (UARC), hosted a Capabilities Analysis Exercise (CALEX) last month in Laurel, Md., attended by approximately 60 thought leaders from across the country. The participants included representatives from the private sector, academia, various government agencies, the U.S. military, and a broad spectrum of other entities and organizations. Their collective goal was to determine, more precisely, how to define the abstract concept of resilience and, more specifically, move beyond: (a) the lessons learned from Superstorm Sandy in 2012; and (b) the rote crafting of grant proposals submitted to the Federal Emergency Management Agency (FEMA) after every major disaster to restore things "as they were before."

Broadening "Resilience" & The Prevention of Future Tragedies

The exercise began by broadening the definition of resilience from the relatively common but necessarily abstract concepts of redundancy, adaptation, and robustness to a more general statement. APL presented its definition of resilience as "anything done – physically or virtually – before, during, or after a disruptive event to improve the ability to adapt, withstand, and recover." The 27-28 August CALEX presented critical infrastructure resilience as a public good that many Americans simply expect to be provided. Drawing from the inspirational work of the late Elinor Ostrom, the U.S. 2009 Economic Nobel Laureate, APL focused on the importance of engaging in collective action in order to avoid such social dilemmas as "free riders" and the "tragedy of the commons" – i.e., individuals depleting shared resources.

The CALEX presented a systematic methodology known as the Resilience Implementation Process

(RIP) to validate and help forge a consensus that resilience can in fact move from theory to practice across the nation's many preparedness and homeland security enterprises. Two basic assumptions were used for that exercise:

1. "Mega regions," which are defined here as major socioeconomic areas in the country that generate a majority of the nation's gross domestic product and represent the locations of highest population, are where the nation's principal economic and demographic strengths are most evident; and

2. The interconnectedness within and among the infrastructure sectors can cause the unanticipated cascading of system failures.

Those assumptions – which focused special attention on the persistent threats posed by natural disasters, terrorism, and climate change – allowed attendees to work with a unified purpose on what most agreed is a somewhat fragmented topic.

APL also asserted that, for resilience, the most important awareness to have before a disruptive event is anchored in risk-mapping the current dependencies and interdependencies of a bounded geographic or organizational area. Used in a systematic and structured manner, the risk-mapping process is designed to provide the information needed to help leaders and planners make better-informed decisions when facing asymmetric threats in a resource-scarce environment.

By emphasizing the need for collective action, use of the RIP methodology helps operators and planners focus greater attention on their own specific *areas of influence* – i.e., elements outside their normal area of control that, because of interdependencies, can and often will impact their operations. The recognition of such connectedness prepares operators and planners to manage any incident of significance more effectively, while at the same time reducing the level of uncertainty involved. Although the infrastructure sectors seem to be largely governed and operated independently, they are in fact highly interdependent and therefore must be understood and managed as common-pool resources that benefit society as a whole. To do that, of course, requires "smart" resilience and the use of both public incentives and private investments to support the shared interests of all sectors involved.

The CALEX Results: Ten Key Findings

The preliminary findings of the CALEX are that the collective national, state, local, and regional enterprises must address the following recommendations:

1. *Improve communications* within the community of interest through the use of standardized terms and a common language when referring to resilience. Making communities better prepared calls for a clear nomenclature that unifies public, private, academic, and other stakeholders across local, state, regional, national, and international levels.

2. *Expand the RIP framework* by identifying the specific variables needed to capture connectedness, dependencies, and interdependencies in both physical as well as virtual terms. The current RIP is considered to be too abstract and too theoretical; it needs to be structured more effectively – to map the landscape of a bounded geographic area, for example, in order to demonstrate the practical value of long-term risk mitigation.

3. *Apply rigorous analytical methods* to the RIP concepts by leveraging existing models, tools, and frameworks more effectively. Building a reliable and more general framework will help planners and decision makers answer questions about what the key variables are, for instance, how to prioritize scarce resources, and why action is needed – thus offering benefits at the personal as well as organizational level.

4. *Operationalize the RIP* by applying the approach to a specific real-world region or facility laboring under the stress of a disruptive event. Operational field-testing allows prototyping and testing with measurable impacts to identify the elements of connectedness and to better understand essential functions.

5. *Close existing gaps* between operational practitioners, policy planners, and analysts by applying specific metrics, standards, and measures of effectiveness. Operationalizing resilience with owners and operators at the local, regional, state, and federal levels requires "selling" preparedness as much more than an insurance policy – primarily because it offers a daily value with a personal and organizational return on investment.

6. *Establish new mechanisms to bridge the private-public divide* by expanding information sharing and building trust. A holistic, integrated, and cross-sector approach unifies and complements the private and public sectors – not only by addressing major disasters and catastrophic events, but also by applying the process to routine disruptive events such as financial hardship, traffic congestion, and severe weather.

7. *Introduce the RIP to a broader consortium* of potential users, analysts, and planners in the private, public, academic, and international communities. The CALEX revealed that the RIP has the potential not only to inform national policy, but also to be generalized to broader geographic and organizational applications. (The RIP still requires field-testing, though, to model, simulate, test, and exercise the concept under a broad spectrum of various conditions.)

8. *Establish a regional-based resilience strategy* that focuses primarily on risk management, preparedness guidelines, and key data sources given the mega-regions' importance to the nation. The investments in risk mitigation, visualization models, decision support tools, and data sciences should significantly advance overall community resilience.

9. *Establish a clear linkage to collective action principles*, emphasizing the separate but synergetic roles of the public and private sectors in implementing resilience as a public good from which everyone benefits. As shared interests in the global commons, resilience and preparedness must be managed collectively (as in clean air, national defense, clean water, and fisheries resources) to avoid what is euphemistically described as a "tragedy of the commons." This requires accountability to reduce "free riders" on one hand and, on the other, to build the incentives needed to bring new private investors into the resilience "market."

10. *Increase the emphasis on individual* resilience through the use of such guiding principles as personal responsibility, family-level incentives, low-cost human preparedness measures, and local investments in practical resilience actions.

The Future of Resilience

The next generation of preparedness leaders must make better informed decisions by optimizing resilience and mitigating risk in the face of receding budgets; or, in business continuity terms, "remaining viable under conditions of duress – no matter what the cause" (quote from personal interview with Alan Berman, President of Disaster Recovery Institute [DRI] International, on 4 September 2013 in Laurel, Md.). Managing risk involves dealing with uncertainty and associated threats and opportunities. The RIP is designed to systematically quantify those variables well in advance of an event in order to help leaders regain control of a crisis more quickly and more effectively.

Finally, the CALEX attendees recognized the need – locally, regionally, and nationally – to invest in preparedness to maintain safety and, of perhaps greater importance, to actively learn from real-world events – and then use the lessons learned to achieve common goals. When resilience efforts lead to preparation and dependability, the nation as a whole will be significantly safer, more secure, and more economically prosperous.

Dane Egli, Ph.D., (pictured) is a senior advisor at the Johns Hopkins University Applied Physics Laboratory, a career U.S. Coast Guard Guardian, and a member of the DomPrep40. His forthcoming book, "Beyond the Storms: Strengthening Homeland Security & Disaster Management to Achieve Resilience," will be published in November 2013.

John Contestabile is the assistant program manager for Homeland Security for the Johns Hopkins University Applied Physics Laboratory and a member of the DomPrep40. He previously held positions at the State of Maryland Department of Transportation (MDOT) and also was the director of the Maryland State Communications Interoperability Program (MSCIP).

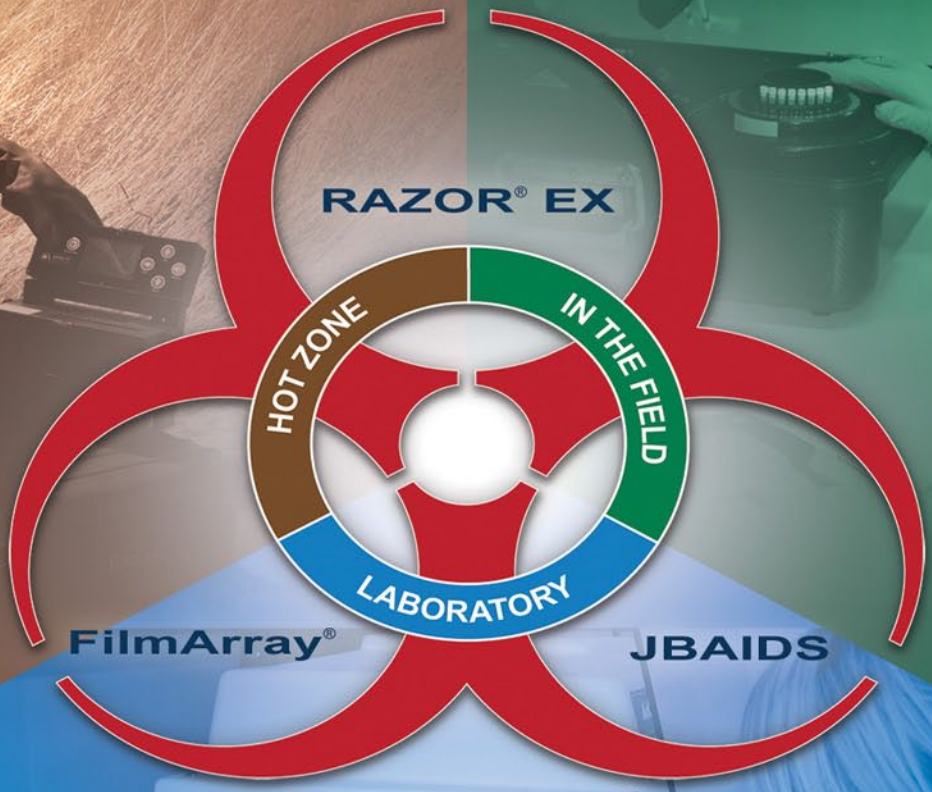
Significant contributions to this article were made by:
Richard "DJ" Waddell, a principal staff systems analyst at the Johns Hopkins University Applied Physics Laboratory. He has extensive experience developing and managing technology solutions and is currently focusing on homeland protection projects on the technology needs of state and local first responders and emergency managers.

Brian Donohue, a senior analyst at the Johns Hopkins University Applied Physics Laboratory. As a licensed officer in the U.S. Merchant Marine, he has extensive experience related to the maritime industry.

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

BIOFIRE DIAGNOSTICS, INC.

Discover the system for your mission.

WWW.BIO-SURVEILLANCE.COM

Worst-Case Scenarios: Sudden & Total Isolation

By Joseph Cahill, EMS

Cornwall, New York, is a mid-sized town in the Hudson River Valley, served by a volunteer ambulance corps and two volunteer fire departments. During Hurricane Irene in 2011, a critically important bridge washed out and most major roads in the area were flooded, leaving the town separated from the vital resources and services essential to any community. The Cornwall situation played out over and over again throughout the entire northeastern United States, in areas ranging in size from single homes to crowded neighborhoods, and from small towns to medium-sized and larger cities.

Key Goal:
Maintaining Access to Emergency Services

From the perspective of EMS (emergency medical services) teams and individual volunteers, this sudden isolation meant not only that local residents were unable to reach aid stations, shopping malls, and other community centers, but also that hurricane victims, and others requiring urgent medical care, could not be quickly and safely transported to hospitals or other medical facilities.

In some situations when the local transportation infrastructure is impacted, *no* medical facility is accessible. In other situations, though, medical facilities may be accessible and functioning but are not equipped to provide full-scale responses. Although many community hospitals have on hand the medical resources needed to cope with a flood or other natural disaster, other facilities – particularly those in remote or sparsely populated areas – are more susceptible to "isolation" risks than the more fully equipped facilities in larger and less remote communities.

Under those circumstances, outpatient clinics, urgent care centers, and other non-emergency facilities must do the best they can; but there are certain risks involved. These facilities have the ability to treat and stabilize patients, for example, but they usually do not have the same quantity or variety of medical resources that community hospitals possess. This means that critically ill or injured patients must be transported – by

a medevac helicopter, for example – to other facilities for the more complicated/advanced care they might need. Use of that option shortens the transport time, but also entails other risks, particularly in difficult weather conditions.

Flooding is not the only hazard that may isolate a community immediately after a natural or manmade incident. Any factor that disrupts the efficient functioning of one or more of a community's "lifeline" sectors – energy, water, communications, transportation, or emergency services – could create what for all practical purposes would be a virtual island. For that reason alone, it is important to: (a) fully evaluate each facility in a given jurisdiction during the planning process; and (b) use the findings to determine how the loss of services from each lifeline sector might adversely affect the response and recovery phases of an incident.

Plan for the Worst, Hope for the Best

Even in towns or other communities that do not have the geography or topography conducive to being almost literally cut off from the outside world, emergency response agencies must have a useful planning tool for identifying all potential risks and developing the contingency plans needed to cope with various incident scenarios. In larger jurisdictions, this "thought exercise" could be applied when considering smaller areas within

the jurisdictions that lend themselves to being cut off. By postulating a scenario of total isolation from the outside world – including such resources as hospitals and/or mutual-aid centers – emergency managers can create effective action plans robust enough to respond when either a single resource or multiple resources are lost.

In the late 1990s, the New York City Fire Department deployed spare paramedic equipment sets by following, in part, this same type of analysis. The Department deployed the equipment by using several factors based not on population or call volume but, rather, on the likelihood that a particular area could become isolated, and/or one of several bridges was lost or at least temporarily not accessible.

By involving other agencies in the planning process, emergency managers can both gather and evaluate the information needed to develop mutually acceptable interagency agreements and procedures. For example, the Department of Public Works may use the information to determine the priority levels required for opening specific routes based on such factors as: (a) the usefulness of each route; (b) the ease of access available to emergency vehicles; and/or (c) the relative isolation of the various areas served by each route.

Isolation is one risk that planners must evaluate, and a scenario they should plan for even if it seems unlikely. Although most U.S. communities may never experience the "island-effect" that Cornwall lived through, planning for such worst-case situations can nonetheless improve the overall response effort needed when any or all resources are no longer fully available.

Joseph Cahill is the Director of Medicolegal Investigations 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.

Unknown Chemical or BioHazard?

AP4C Handheld Chemical Detector

Known Solutions

AP4C-F Fixed Location Chemical Detector

- Unlimited, Simultaneous Detection
- Fast and Easy to Use
- Always Ready with Very Low Operation Cost
- Rugged Construction for Harsh Environments

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

A Network of Interoperability

By Charles Werner, State Homeland News

Managing an incident response in today's complicated, and interconnected, world requires a high degree of interoperability – i.e., the coordination and communication of vital information with numerous responders at all levels of command and both across and within many organizations. The goal, of course, is to ensure that all hands within an organization and their counterparts in other organizations have the most up-to-date information they need as soon as possible.

In the past, meeting that goal was a difficult challenge for the Charlottesville, Virginia, Fire Department. And, in practice, connecting with federal partners, public safety officials in other states, and/or anyone else with a need to know in the broader homeland security community, has required a lot of manpower. Moreover, when information was shared, it frequently was *not* the most current information available. In short, maintaining communications in general was a difficult, time-consuming, and often frustrating process.

Improved communications are the key to providing and receiving the timely as well as accurate information needed by fire departments and other emergency services to respond both quickly and effectively.

Building & Using Secure Communications

For fire departments, maintaining and improving communications with colleagues in the fire service – and with other local responders – has become a high priority. In Charlottesville, use of the U.S. Department of Homeland Security's Homeland Security Information Network (HSIN) has helped to significantly improve such communications over the past several years. The latest iteration of the network, called HSIN R3, became available earlier this year and the full migration of all users and content was recently finalized in August.

Although the HSIN has been in service for a decade, and has become a particularly valuable information-sharing tool both in Virginia and in many other emergency responder departments and agencies across the nation, the R3 version has gone through a major upgrade. As a secure online system made up primarily of mission-focused sites, for example, the HSIN enables many different communities of homeland security professionals to collaborate and share sensitive information with other trusted members both across state lines and between organizations. Obviously, this information sharing also helps to build better, more cordial, and more helpful working relationships among different disciplines and at various levels of government.

Today, members of the HSIN community routinely use the network to support incident management operations, while also delivering regularly scheduled as well as emergency alerts, warnings, and other important intelligence information. In April 2013, to cite but one example recently in the news, HSIN was used to provide vital unclassified information to law enforcement professionals nationwide both during and after the multi-agency response to the Boston Marathon terrorist attack. The network also has, for many years, supported major operations centers during such national events as Fourth of July celebrations, the National Scout Jamboree, weather disasters (Hurricane Sandy was a prime example), and even the Super Bowl and other major sporting events.

A Routine Task – With Life-Saving Benefits

By using HSIN each day, officials can quickly and easily: (a) view situational assessments from the public safety community in general; (b) access invaluable background information about what is going on both in a particular locality and around the country; and (c) help establish trusted relationships with other public safety officials from the local, tribal, state, federal, and private sectors.

The upgraded HSIN R3 version will provide a new set of collaboration tools for secure web conferencing, instant messaging and chat, and both document and image sharing. There already have been many success stories, of course – from law enforcement, incident response, and public safety agencies – that can be attributed to improved information sharing via HSIN. Daily use of the network by public safety officials across the nation will assuredly save even more precious time in the event of a national crisis when accurate real-time information is urgently needed for response operations.

The relatively easy steps to access HSIN are as follows: (a) email the HSIN Outreach Team at HSIN.Outreach@hq.dhs.gov; (b) connect with a Mission Advocate; and (c) locate an existing HSIN site – or establish a new one. Connecting and collaborating with other HSIN members has already greatly benefitted the Charlottesville Fire Department, and undoubtedly, when the R3 version is online, will provide even greater benefits in the future.

Charles Werner is a 39-year veteran of the fire-rescue service who now serves as chief of the Charlottesville, Virginia, Fire Department. He also serves on the HSIN Advisory Committee as a representative of the fire service. He can be reached at wernerc@charlottesville.org.

Defense Department Plays Key Role in Disaster Resilience

By Jamie Stowe, DOD

The Mayo Clinic defines resilience as the "ability to adapt well and recover quickly after stress, adversity, trauma, or tragedy." Helping a community overcome extreme challenges is exactly what the Department of Defense (DOD) strives to accomplish when it is requested – under the Defense Support of Civil Authorities (DSCA) parameters – to respond to domestic disasters. By working with its state and federal partners, DOD serves as a significant force multiplier for resilience during catastrophes directly affecting the United States. Moreover, many military personnel actually consider the ability to provide emergency assistance to their fellow citizens to be a distinct honor.

If properly used, the U.S. military can in fact be a key contributor to the whole-of-community approach during state and/or national emergencies. Both the National Guard and the nation's active-duty (federal) forces can quickly help build shelters, provide medical treatment, transport supplies and people, supply electrical power and fuel, and much more to mitigate some of the most devastating effects of major disasters – both natural and manmade.

Supporting Civilians at Home & Abroad

U.S. naval and military forces have certainly proved their usefulness during major peacetime crises throughout history – including, in recent years, such disasters as Hurricane Katrina (2005), Hurricane Sandy (2012), the Fukushima tsunami and nuclear meltdown (2011), and the 2010 earthquakes in Haiti and Chile. In the United States itself, both National Guard and federal troops provided security and material resources – food, water, and medical supplies, for example – for the victims of both Katrina and Sandy; during the latter superstorm, they also assisted with water pumping, fuel distribution, and environmental sampling.

During major disasters overseas, DOD supported the civilian authorities of Haiti, Chile, and Japan with crucial supplies, transportation assets, medical assistance, search and extraction operations, aerial surveillance, and both road and debris clearance – all of which would

also be available, of course, during a domestic disaster response within the United States.

Support activities such as those spelled out above can certainly help reduce stress on the survivors, the local areas impacted, and – to at least some degree – the nation at large, as local citizens and the American people watch cascading events unfold both on television and through social media. There also is a huge albeit unquantifiable psychological benefit derived from DOD participation – for example, in the form of a large hospital ship such as the USNS Comfort berthed offshore – in the response to a major catastrophic event. Recognition during a response that help is on the way, or already on the scene, can generate a strong psychological boost and serve as a clear signal of hope to those in need.

DOD operations in recent years have proved to be a valuable tool in building resilience: (a) by better preparing personnel and their family members prior to, during, and after deployment; and (b) by coping with other unexpected contingencies. Over the past several years, in fact, DOD has substantially increased its "bounce back" resources in the form of additional chaplains and mental health personnel, the better utilization of resources, and increased access to outside and nontraditional methods of support. This trend toward a higher focus on and funding of behavioral health support is expected to continue into the foreseeable future.

Nurturing Relationships & Growing Awareness

One benefit of an increased awareness of how important resilience is to the warriors returning from overseas is that DOD is now emphasizing resilience during domestic support operations as well. The inclusion of traumatic-stress response teams – specifically mental health specialists and chaplain counselors – in DOD's own disaster response planning not only helps survivors and their family members, but also the first responders themselves, in their efforts to cope with and overcome extremely stressful circumstances.

The same DOD stress response teams are also available to help civilians – if and when requested under the guidelines spelled out for DSCA response operations – and DOD officials consider such teams to be a core element of many DSCA contingency response packages. Current DOD catastrophic domestic response planning is also now focusing more attention on the disabled, diabetics, the elderly, and other at-risk populations, because they are often the people immediately and most seriously affected by a sudden disaster. However, the tragic Washington Navy Yard shooting on 16 September 2013 is a recent example of just how important stress response teams are to all survivors of and those impacted by disasters.

Considering the future resource constraints the nation as a whole is now facing, the Department of Defense may well play an even more important role in the nation's overall response construct, particularly in the intangible aspects of building and maintaining resilience. Fortunately, many former obstacles to using a truly effective and integrated civilian and military approach to domestic emergency responses already have been addressed and resolved. For example, a high priority in any DOD support provided to civilian authorities is to maintain and/or restore public confidence in the government's ability both to handle crises quickly and effectively and to provide prompt emergency support.

As an increasingly important partner in the whole-of-community approach to responding to and managing catastrophic events, DOD helps to instill confidence and to provide concrete assurances that the nation as a whole will be able to successfully overcome even the direst of circumstances. To build an even greater resilience capacity – and even, in a worst-case scenario, be able to handle the fallout of a nuclear detonation within its borders – it is imperative that the nation's civilian and military authorities continue to expand and improve their current working relationships and to coordinate their planning efforts for the future. By joining forces, the nation can and will overcome any future challenge the U.S. homeland may face – now, and for many years to come.

The views expressed in this article are solely those of the author and do not necessarily represent the views of the U.S. Department of Defense, the U.S. Air Force, or any other federal agency.

Major Jamie Stowe, USAF, is a medical plans and operations officer who has more than 14 years of experience in emergency planning and response operations with the U.S. Air Force and the U.S. Army. He has not only completed a Department of Defense planning fellowship but also has been directly involved in numerous contingency operations – including those following Hurricanes Rita, Ike, Gustav, and Sandy, the Japanese tsunami and nuclear plant responses, and the 2010 earthquake in Haiti. He holds a master's degree in Business Administration and is currently pursuing a master's degree in National Security and Strategic Studies from the U.S. Naval War College.

NANORAIDER™
Personal Spectroscopic Radiation Detector (SPRD-CZT)
for under than $10k

BECAUSE IT'S NOT JUST YOUR JOB, IT'S YOUR LIFE.™

The difference between life and death is in your hands. FLIR CBRNE threat detection products provide lab-caliber analysis where you need it most – in the field. When lives are at stake you need fast, accurate results you can trust.

FLIR®

www.FLIR.com/gs

Risk Assessment & Management: The Overlooked Component

By Jennifer Ryan, Special Events

The bombing attacks at the Boston Marathon finish line in April 2013 highlighted the importance of including special events when determining and managing the various risks facing communities throughout the nation. Planning products used to meet federal requirements, such as a state's Hazard Identification and Risk Assessment and/or the Federal Emergency Management Agency's Threat and Hazard Identification and Risk Assessment, will help to quantify, to some extent, the risk a state or local jurisdiction faces from all types of natural, manmade, and/or technological threats.

These same assessments, though, do not always apply to and/or account for the literally hundreds of thousands of pre-planned special events of various sizes and importance that take place across the nation annually. As the Boston Marathon attack demonstrated, such events can no longer be overlooked by the emergency management and homeland security communities.

Federal, State & Local Events

For more than a decade, the U.S. Secret Service has used the term "National Special Security Events" (NSSEs) to designate major activities or observances that, under federal law, give the Secret Service the authority and responsibility for all security planning associated with such events. NSSEs usually: (a) include the presence of national political dignitaries, foreign heads of state, and/or large crowds; or (b) have other major national or international significance. For events that do not rise to this level, there is an additional ranking protocol used at the federal level – the Special Events Program of the U.S. Department of Homeland Security.

DHS leads the overall Special Events Assessment Rating (SEAR) process for the federal government. Co-chairs of the Special Events Work Group, which represents 50+ other federal agencies, work through a risk assessment methodology of special events reported through an annual data evaluation that takes into consideration the numerous types of threats, vulnerabilities, and potentially adverse consequences associated with each event. The result is assigned a SEAR level 1 through 5 designation that is used to help determine the level of federal awareness of and support given to the event.

However, there are many events that have local- or state-level significance, but do not quite rise to the level of an NSSE – or even to a high SEAR level. Nonetheless, major gatherings of participants and/or spectators within a state, city, or local community can quickly and easily overwhelm the capabilities of a jurisdiction if a natural, accidental, or intentional incident occurs at or near the event. For that reason alone, jurisdictions at all levels of government have a continuing responsibility: (a) to develop and maintain their own situational awareness, from start to finish, of all special events; and (b) to support and fully participate in the planning process well in advance of the start date of such events. What most jurisdictions currently lack, unfortunately, is a formalized and standard methodology to complete the risk assessments needed to manage (and thereby protect) special events in a meaningful and useful way.

A New Protocol From The National Capital Region

In Maryland, as well as the National Capital Region (NCR) – which encompasses the District of Columbia and the adjacent jurisdictions in both Virginia and Maryland – efforts are currently developing a formalized protocol for reporting special events, risk assessments

associated with those events, and preparedness and operational support required. As a region with numerous unique security challenges as well as a heightened sense of vulnerability – because of its proximity to the nation's capital and other resources of national significance – the NCR jurisdictions recognize the importance of assessing the risks associated with special events in order to effectively reduce or eliminate the potential for jurisdictional resources to become overwhelmed.

At the state level, the assessment of risks for special events also has become increasingly important. Although pre-planned events might not have seriously alarmed most law enforcement and public safety officials in the past, that level of concern seems to have changed. Because of the many worldwide and domestic terrorist attacks in recent years, as well as the occurrence of natural disasters that also seem to be steadily increasing, pre-planned special events are now recognized as having potentially drastic consequences for any host jurisdiction. In short, the need to manage risk is already at a fairly high level, and still climbing.

The Boston Marathon bombings have had a significant impact on risk assessments as they relate to special events. A new protocol is being developed to address this concern.

The development and implementation of an effective risk assessment process, as well as a preparedness and operational support program, will be no small undertaking for any state, regional, or local jurisdiction involved. An effective process will have to be developed for the collection of data that is not limited to a mere format, but also includes a robust information collection plan that takes into account factors to be quantified in later analysis.

Although certain aspects of a special events risk assessment program could be modeled after the DHS and NSSE prototypes, individual states and localities should be cognizant of the accompanying data limitations as well. States may rely to a certain extent, for example, on fusion centers to assist with threat information, but the more comprehensive and detailed threat data available to the federal government that allow for truly quantifiable analysis may have restricted accessibility and thus be unavailable to states.

Various consequences and impacts of special concern may also differ considerably when assessing the risk posed by a special event from the state or local perspective rather than from a federal perspective. The participation of various dignitaries may well be defined in a different way for a local jurisdiction than it would be at the federal level. For example, although a major event in which all members of a county's elected leadership are in attendance would perhaps never rise to the federal level of qualifying as a SEAR or NSSE event, there still could be potentially devastating consequences for the local government if an incident would occur that incapacitates most or all of its elected leadership.

Additionally, the projected attendance will have to be analyzed carefully. Postulating a simple numeric value will not be enough for a state to fully assess the potential vulnerabilities and consequences related to a specific event. The concentration of attendees at a particular time in the event, the location of the event – and its proximity to trauma centers and/or acute care facilities – and the availability of temporary emergency sheltering for attendees should all be taken into account to fully assess, and thereby manage, the risk associated with any given event.

Potential Obstacles & The First Steps

As previously stated, the development and implementation of a special-event risk assessment methodology at the state level is a major undertaking. Because of the usually classified nature of detailed threat information, ensuring the availability of such intelligence can be one major challenge, but there are others that states also will face. Even at the federal level, participation in the annual request for data is voluntary, and as such the information provided may be limited; in other words, not all pre-planned special events will be captured through the data request process.

However, risk management is necessary regardless of the event being reported, which means that states will be forced to identify alternative mechanisms to obtain information, or create some type of regulatory requirement to report special events. The lack of situational awareness may, under any given circumstance, have a variety of root causes – ranging from jurisdictions wanting to limit participation in planning and preparedness by outside entities to a failure to recognize the inherent risk associated with special events. Such sensitive issues must therefore be addressed early and then be carefully managed for a successful and effective risk assessment program to function.

States also may be faced with issues of funding and resource expectations. For events that rank higher (and/or are simply identified, for a variety of reasons, as being of higher risk), local planners and organizers might reasonably expect to receive at least some resources and technical expertise, or funding support, to help manage the risks and supplement any gaps identified through the risk assessment process. In today's world of limited funding and more careful resource allocation across all levels of government, states must be prepared to at least help provide the additional resources needed to meet the risk levels anticipated.

A Necessary Next Step

Numerous federal reporting requirements are already in place for states and UASI (Urban Area Security Initiative) regions that assist in the process to assess and quantify both the risks involved and the levels of preparedness needed for each state and the region as a whole. The previous emphasis in emergency management and homeland security planning has focused on the highest-risk, highest-consequence, and highest-probability categories of natural, technological, and manmade threats that any given jurisdiction might face. Very few jurisdictions, though – the NCR is a notable exception – specifically address pre-planned special events when assessing the overall spectrum of potential risks.

Events that do not rise to the level of federal involvement through NSSE or SEAR designation still have the ability to overwhelm local resources and, therefore, to increase the need for state-level risk management activities. The development and implementation of comprehensive risk assessment methodology will not be without its challenges, but should significantly increase the ability of all states and regions – and the nation as a whole – to manage risk and enhance preparedness.

Jennifer Ryan is a preparedness planner at the Maryland Emergency Management Agency. She holds a B.S. from Towson University and an M.S. in Emergency Health Services and Epidemiology from the University of Maryland Baltimore County. She is a lifelong resident of Baltimore, Maryland, where she currently volunteers as an emergency medical technician in her spare time.

Updating the National Infrastructure Protection Plan

By William Anderson, CIP-R

Over the past few months, The Infrastructure Security Partnership (TISP) has been participating in a public-private collaborative effort, led by Robert Kolasky of the U.S. Department of Homeland Security's (DHS) Office of Infrastructure Protection, for the purpose of updating the National Infrastructure Protection Plan (NIPP). Public-private sector collaboration and partnerships are now frequently mentioned in case studies, reports, policy directives, and articles addressing topics related to regional and infrastructure security and resilience. There are many reasons for companies and agencies of all sizes to work together for the common goal of building resilience.

Reports such as the *Hurricane Sandy Rebuilding Strategy* – released in August 2013 by the Hurricane Sandy Rebuilding Task Force, which is chaired by Secretary of U.S. Department of Housing and Urban Development Shaun Donovan – show that there is a positive relationship growing between collaboration and regional resilience achievements. TISP was established 13 years ago and has focused on the skills related to building public and private sector collaboration for the primary purpose of advancing regional and infrastructure security and resilience.

Protecting the nation's critical infrastructure requires sharing information among various individuals and groups that are dedicated to building a more resilient nation.

Partnering to Discuss Resilience

To support NIPP collaboration, TISP has helped develop a partnership between the National Resilience Coalition (NRC), which was co-founded by TISP, and the Homeland Security Policy Institute (HSPI) of The George Washington University. As a result of this partnership, senior leaders from the public and private sectors met to discuss the application of risk-based approaches to improve the security and protection of critical infrastructures and systems on which the resilience of the nation and its major metropolitan regions so greatly depends. Conducted on behalf of DHS and sponsored by ICF International, the full-day forum was held on 25 July 2013 at the Elliott School of International Affairs at George Washington University. Attendees explored the role that the NIPP has served as both a guide and catalyst for: (a) advancing the resilience of the nation's infrastructure; and (b) determining what industry and government leaders have learned along the way that will help DHS to update the NIPP.

As mandated by the Homeland Security Act of 2002 and the 2013 Presidential Policy Directive on Critical Infrastructure Security and Resilience (PPD-21), DHS is responsible for developing and updating a national plan that takes a risk-based approach to address significant threats and hazards to the nation's critical infrastructure. To do so, it must capitalize on the collective experience of: infrastructure owners and operators; federal, state, and local governmental agencies; and major users of infrastructure services, all of whom bear both the burden and the cost of ensuring the resilience of their individual operations. The effort by TISP, NRC, and HSPI has helped to support DHS's efforts by facilitating a dialogue among senior executives with firsthand experience with the NIPP, the NIPP's risk management framework, and/or the executives' own infrastructure resilience programs.

To help advance efforts toward national resilience, the purpose of the forum was to: (a) establish a common understanding among participants on the intent and evolution of critical infrastructure protection policy and programs; and (b) outline initial questions concerning the NIPP update and implementation of PPD-21. TISP tracked the dialogue of the forum and later presented DHS with information from the proceedings. Many of the stakeholders offered unique perspectives on leading threats and hazards, the challenges faced in managing associated risks and achieving a higher level of resilience, and the implications for future policies and programs.

Meet colleagues, hear experts and see the latest technology in Emergency Management at IAEM 2013 in Reno!

IAEM International Association of Emergency Managers

www.iaem.com

IAEM 61st Annual Conference & EMEX

EMEX EMERGENCY MANAGEMENT & HOMELAND SECURITY EXPO www.emex.org

www.emex.org

Emergency Management IN A Changing World

Silver Legacy Hotel & Reno Events Center | Reno, Nevada

Conference: October 25-30, 2013 | *EMEX:* October 28-30, 2013

www.iaem.com/conference

Seven Key Takeaways

By the end of the forum, seven key suggestions had emerged, which have been principally embraced in recent drafts of an updated NIPP as a national strategy for critical infrastructure security and resilience. The updated NIPP will also serve as a potential model and educational tool for regional, state, and local organizations to follow. Each of the suggestions is described below.

1. The original national policy framework, which was built on a risk-based architecture, is still relevant. However, the framework should be enhanced to emphasize the importance of protecting and preparing lifeline infrastructures and economic stability/development systems at the state and local levels in order to maintain infrastructure and regional resilience. There should also be a link to regional, state, and local critical infrastructure/key resources networks.

2. Regional public-private partnerships are necessary for: (a) addressing the integration of cross-sector dependencies and operations; (b) collaborating and setting priorities for withstanding the consequences of manmade and natural hazards; and (c) rapidly bouncing back from failures, disruptions, and destruction.

3. The NIPP should be concise and brief, yet still explain the national strategy for critical infrastructure security and resilience as well as transfer knowledge to state and community leaders for establishing their critical infrastructure security and resilience programs.

4. The NIPP should include and fully explain the reasons that government agencies and businesses would want to participate in a national unity of effort that mitigates risks, builds resilience, and sustains resources.

5. The NIPP should include a list of actions that can be implemented at various levels – for buildings, systems, communities, states, regions, and federal agencies, for example. The NIPP also should motivate these stakeholders to develop plans for: infrastructure protection, continuity of operations, emergency preparedness, and disaster recovery.

6. The DHS Office of Infrastructure Protection should develop educational, training, and certification programs to drive the increased human resource capabilities with competencies in engineering, design, construction, and security operations.

7. The NIPP should support networking and relationship development by: (a) sharing lessons learned from exercises and disasters; and (b) building relationships before a disaster strikes to reduce response times, save lives, and reduce costs.

After the conclusion of the forum, various experts – from ICF International, the Great Lakes Hazards Coalition, the National Association of Counties, ABS Consulting, the Bay Area Center for Regional Disaster Resilience, the University of Southern California, DRS International, and the Brashear Group – joined a TISP comment-drafting team to work with DHS and their public and private sector collaborators. TISP has since been convening this group twice a week to discuss and draft language revisions for various sections of the NIPP.

On 18 September 2013, TISP committee and board members, along with NRC partners, will be holding a conference call to specifically discuss "Section 6, Taking Action: Specific Steps to Advance the National Effort" in the NIPP. The actions addressed in that section will be implemented over the next several years to reduce risk to the nation's critical infrastructure and will be based on different priorities and perspectives – within sectors, at the state and local levels, in multi-national corporations, as well as among small business owners and operators. Specific roles and responsibilities for taking these actions will be articulated within subsequent planning efforts in collaboration with each community. The deadline for submitting the next round of comments/suggestions to DHS about the NIPP was 20 September 2013. President Barack Obama is expected to have the final draft by mid-October.

Moving Forward – Implementing Critical Infrastructure Security & Resilience Programs

As a next step to advancing regional and infrastructure security and resilience, TISP is forming five leadership roundtables:

1. *Resilience Standards and Measures Roundtable*, facilitated by Kevin Morley of the American Water Works Association and Michelle Deane of the American National Standards Institute;

2. *Mission Assurance and Resilience Roundtable*, facilitator to be determined;

3. *Legal Issues Around Resilient Communities and Buildings Roundtable*, facilitated by Ernest Edgar of ATKINS Global and Denise Krepp of Penn State University;

4. *Pre-Logistics Planning for Preparedness Roundtable*, facilitated by Charlotte Franklin of the Arlington County, Virginia, Office of Emergency Management; and

5. *Climate Change Adaptation, Sustainability and Resilience Roundtable*, facilitated by Paula Scalingi of the Center for Regional Disaster Resilience and Jerry Brashear of the Brashear Group.

Each roundtable will develop an understanding of the subject, identify benefits and challenges, and recommend actions for TISP to take in the future. The roundtable discussions can be followed on the TISP website (http://www.tisp.org) and the TISP LinkedIn subgroups. Resilience begins with each person and such discussions bring those key people together.

William B. Anderson is director and chief operating officer for The Infrastructure Security Partnership (TISP). Before TISP, he served as director of transportation operations and program assessment for the Intelligent Transportation Society of America (ITS America), where he directed program development and project management for numerous forums, including the Homeland Security and Public Safety Forum, and managed various tasks in cooperation with the departments of Homeland Security and Transportation. Prior to that, he worked as a program analyst, infrastructure security and regulatory coordination, for the Transportation Security Administration. He currently holds a master's degree from the University of Maryland and a bachelor's degree from Roger Williams University in Rhode Island. For more information about TISP, member benefits, support of the drafting of the NIPP, the 2011 Regional Disaster Resilience Guide, and the supplemental Understanding Resilience booklet, contact Bill Anderson, director, at wanderson@tisp.org or at 703-549-3800, ext. 190.