domestic preparedness .com

DomPrep Journal

US Annual $100 Volume 8 Issue 1, January 2012

SHARING


PROVEN
--TEST RESULTS--
ANTHRAX DETECTED
Power
Brightness
Up
Back
Select
Down
BIODETECTION
RAZOR™ EX The Complete Field BioThreat Solution
www.RAZOREX.info
Idaho Technology Inc.
Innovation Amplified
390 Wakara Way, Salt Lake City, UT, 84108, USA | 1-800-735-6544 | www.idahotech.com

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

Staff
Martin Masiuk
Publisher
mmasiuk@domprep.com

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

John Morton
Strategic Advisor
jmorton@domprep.com

Susan Collins
Creative Director
scollins@domprep.com

Catherine Feinman
Associate Editor
cfeinman@domprep.com

Carole Parker
Database Manager
cparker@domprep.com

Advertisers in This Issue:

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; and also available at www.DomPrep.com

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 Manuscripts are original work, previously unpublished and not simultaneously submitted to another publisher.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

IMR GROUP

Editor's Notes

By James D. Hessman, Editor in Chief

A senior leader promoting public-private partnerships, a private citizen concerned about certain (but important) "locational" problems, and an Air Force officer providing international aid are all among the baker's dozen of writers who have contributed their insights, experiences, and special expertise to this information-packed issue of *DPJ*.

W. Ross Ashley III starts the issue with an illuminating report on various cyber security problems – a topic much in the news these days – and the several ingenious systems and devices that have been developed and manufactured to prevent cyber attacks. He also asks a key question for which there is as yet no totally satisfactory answer: Do these systems and devices fully protect the national "knowledge base"? Jordan Nelms addresses the same potentially cataclysmic problem: information technology capabilities have grown exponentially in recent years – but the immense gains achieved have made the IT systems themselves much more attractive targets for terrorists (or homegrown criminals).

There has been considerable talk about earthquakes recently. It took months for news about the New Madrid and San Francisco earthquakes to reach the U.S. east coast – but only a few seconds for news about last year's much less damaging Mineral (Virginia) earthquake to reach California. Separate articles by Christina Spoons and Jordan Scott give credit to the truly seismic growth, and use, of the new "social media" – and strongly recommend much more of the same.

Other equally impressive types of progress bring with them a few unwelcome problems. Raphael Barishansky discusses the much improved homeland-security capabilities, at all levels of government, that have been achieved in recent years – at a fairly high – but absolutely necessary, cost to American taxpayers. What happens, he asks, when the funding stream slows down? And that, he says, seems to be an absolute certainty – unless there is another 9/11 disaster. Michael Jacoby takes a careful look at the estimated 2.8 million records available in the EPA's "Envirofacts" database and points out that not all of the information in each and every one of those records is positively no-doubt-about-it accurate. The EPA concurs – very much to its credit – and offers a few helpful suggestions for improvement.

Shifting back to the positive: Jamie Stowe provides an upbeat and, appropriately, "friendly" report on how the U.S. military stepped in to help Japan recover after the 2011 Fukushima earthquake/tsunami shattered that nation's infrastructure – and the morale of its citizens. Sheri Donahue discusses the close-knit operational (and personal) relationships developed between and among 47,000 close friends now enrolled in InfraGard. Jerry Brashear comments on the advantages provided by the Census Bureau-enabled shift to a regional approach in resilience and recovery operations. Cortney Streets focuses on the growth, usefulness, and accessibility of the multipurpose RKB (Responder Knowledge Base). Geoff Brown talks about the unforeseen intricacies of mass-evacuation plans – horses and trailers included. And Joseph Cahill comments on the sad but absolutely necessary requirement for careful and comprehensive investigations that by law must follow almost any and all fatal accidents and incidents – but help ensure that there are fewer such incidents in the future.

About the Cover: "Words, words, words!" That exasperated "sentence" (sort of) from Eliza Doolittle's lament in My Fair Lady is also an apt description for what is called "word clouds." This cover – through varied sizes, styles, and placements of "key words" – illustrates some of the more important topics, concepts, issues, and contents of the articles contained in this information sharing issue. (Wordle™ concept and design created by Susan Collins.)

Public Health Preparedness Summit
Anaheim, CA | February 21-24

Regroup, Refocus, Refresh: Sustaining Preparedness in an Economic Crisis

Why is the Summit the Largest Gathering of Public Health Preparedness Professionals?

The goal of the Public Health Preparedness Summit is to strengthen and enhance the capabilities of public health professionals and other participants to prepare for, respond to and recover from disaster and other public health emergencies.

The 2012 Public Health Preparedness Summit will focus on how to move forward in an environment of limited resources. Public health professionals and our partners from across the nation will present new research, new tools, and new practices to build and sustain a progressive public health preparedness infrastructure at the local, state, tribal, and territorial levels. Join your colleagues at this year's Summit and take the opportunity to ***regroup, refocus***, and ***refresh*** your approach to public health preparedness.

To learn more about the 2012 Public Health Preapredness Summit, visit www.phprep.org

Disinformation: The Real Cyber Security Challenge?

By W. Ross Ashley III, Cyber & IT

In the early 1930s, when intelligence information was collected primarily by intercepting foreign embassy cables, U.S. Secretary of State Henry L. Stimson expressed his disapproval by stating that the act was an "ungentlemanly business" and a "travesty to diplomacy." Despite Stimson's disdain for such shocking behavior, the art of cyber exploitation and the countering of the cyber security measures of other nations was just beginning.

Today, most cyber security challenges and initiatives focus primarily on protection of the information itself and of the highly sophisticated networks used to transmit, store, and manipulate that information. Although this change is certainly an important aspect of cyber security, it does not address several new and/or emerging challenges that the emergency management community is beginning to face.

In recent years, social media such as Twitter, YouTube, and various "Rich Site Summary" (RSS) feeds have become more widespread in their use and still growing capabilities. Moreover, the same social media outlets have become the new norm for sharing information and are rapidly replacing the several ways that government agencies and everyday citizens have been using in recent years to learn about and communicate with one another – and with other agencies, both public and in the private sector.

Beyond & Sometimes Because of the Worst-Case Scenario

Because of the mostly positive implications for the emergency management community, many companies also are developing and using the technologies needed to enable that community, and others, to use the "new media" as effectively as possible. Individual citizens already can: (a) follow and post feedback to local, state, and federal agencies and organizations on Facebook and Twitter; (b) subscribe to local alerts; and (c) most important of all, perhaps – use many of the other services provided to inform and build confidence in preparedness and response efforts during sudden times of crisis.

To ensure the continuity of information, the primary cyber security focus typically addresses the worst-case scenario – content no longer being available (as a result of service attacks, perhaps, and/or other malicious behaviors designed to destroy or disable valuable networks). Other important planning initiatives focus on preventing the hacking of power grids, attacks on nuclear facilities, and the destruction of other high-value/high-consequence infrastructures.

Such protection is of course both necessary and extremely important, but fails to address the most vulnerable area of cyber security – namely, *the information itself.* An even greater threat than not being able to communicate at all would be the communication of erroneous, inaccurate, or misleading information, thereby creating widespread doubt and eroding community confidence in the ability of government (state and local as well as federal) to provide the leadership needed in times of disaster.

Misinformation Problems Increase as Societal Buffers Deteriorate

Before use of the social media became so prevalent, the societal buffers were much stronger and usually able to quickly dispel inaccurate rumors – typically passed either by word of mouth or by handwritten and/or typed documents. However, as information began moving not only much faster but also more freely and in massive volume, the situation started to change significantly.

There are two factors in particular that have emerged to reduce the traditional effectiveness of the societal buffer: (1) The societal buffer is constantly being bombarded with information – transmitted in large quantities every millisecond; the transmission rate for such transmission is already astounding – and that problem may be only just beginning. (2) The societal buffer is usually working in close proximity to nontraditional media on the other side of the societal buffer. Reports by the so-called fringe media, the growing dissemination of unverified (and sometimes even manufactured) "facts," and even the unintentional negative consequences caused by simple typographical errors are: (a) difficult to control; (b) can lead to the ruin of careers and companies; and (c) are rapidly leading to a "crisis in confidence." To cite but one example: On 12 December 2011, some residents in New Jersey received an alarming text message stating "Civil Emergency in this area until 1:24 p.m. EST Take Shelter Now."

"Within about 90 minutes," according to CBS News, "the state homeland security and emergency management offices posted on Twitter that no emergency existed, but by then people had called a variety of local, county, and state agencies to express their concerns."

A later investigation determined that what was originally thought to be a malicious "spamming" type of text turned out to be an error, by Verizon, in not describing the alert as a "TEST." Whatever the reason (or excuse), some unquantifiable social damage was done and citizens' reactions in that state may be considerably different the next time an emergency alert is issued.

Greater Costs & Higher Consequences

The emerging threat that emergency managers now must consider is coping with anyone wanting to do harm and exploit a disaster by turning it into a higher-consequence event. Last summer, emergency management agencies took appropriate actions across many states and municipalities as Hurricane Irene roared its way up the East Coast. Evacuations were timely and orderly, and information to the public was available on, among other outlets: municipal websites; Facebook accounts: RSS feeds; and email/text alerting subscriptions.

However, in a matter of seconds, these and other efforts might just as easily have been "hijacked." Using any of a growing number of relatively unsophisticated techniques, an organized group that wanted to disrupt or otherwise harm preparedness and response efforts might easily have: (a) rerouted websites to "mirror" sites providing erroneous information; (b) created other error-crammed websites appearing to be credible; (c) posted bogus Facebook comments from "expert sources"; and/or (d) "spammed" alerting mechanisms into the cellular network. All of these and other harmful actions could be coordinated in a mutually assuring way to misguide literally millions of private citizens, many of whom would probably behave in ways that could have potentially very harmful consequences.

Protecting the privacy of information – and the security as well as the continuity of operations – is and must continue to be a very high priority for successful emergency management. However, any failure to protect the quality and accuracy of the information itself poses yet another dangerous threat that might sometimes be overlooked by those responsible for creating hazard-mitigation and continuity-of-operations plans for the communities they serve.

For additional information on:
The CBS News report, visit http://www.cbsnews.com/8301-201_162-57341882/mistaken-verizon-emergency-alert-scares-n.j/

W. Ross Ashley III is the Executive Director of the National Fusion Center Association (NFCA). He also serves on the Board of Advisors of numerous corporate clients. He was confirmed by the U.S. Senate in December 2007 and served as Assistant Administrator of the Grant Programs Directorate until August 2009. Previous roles include: Chief Executive Officer of the National Children's Center (NCC), founder of the Templar Corporation, Director of Law Enforcement Technologies at ISX Corporation, and other private-sector positions. A retired Air Force Intelligence Officer, he also has served in both the Virginia Air National Guard and the U.S. Air Force Reserve.

RR/SAP: The Process of Building Resiliency

By Jerry Brashear, CIP-R

Hurricanes Irene, Katrina, and Ike, the floods of the Mississippi and Cumberland rivers, the Joplin and Tuscaloosa tornados, the Minneapolis bridge collapse, the Northeast Blackout, the Deep Horizon oil spill, and, of course, the terrorist attacks on 11 September 2001 – all of these major disasters underscore the value of providing and improving resilience and security on a metropolitan regional scale. In that context, the term "region," as used here, refers to a metropolitan region – defined by the U.S. Census Bureau as "a geographic entity containing a core area of at least 100,000 persons plus adjacent communities having a high degree of social and economic integration with that core."

At the core of any region's resilience and security capabilities and resources are its critical infrastructures, its core public services, and its economic base – which include but are not necessarily limited to such tangible and intangible resources as water and wastewater, energy, transportation, telecommunications and cyber systems, public health and safety, state and local governments, banking and major industries, healthcare, food, and shelter.

The numerous dependencies within and between infrastructure systems – services, business, and economic sectors – affect not only societal wellbeing but also the ability of communities within a region to rebound from potentially catastrophic events. Identifying and addressing these dependencies can prevent a series of "cascading" failures that can quickly compound and exacerbate the negative effects of a natural or manmade disaster. Dealing effectively with these dependencies usually requires, therefore, a uniquely *regional* approach wherein larger systems converge and work together to serve the greatest number of people. This is not an easy task, because the interlocking dependencies are almost always extremely complex, and dealing effectively with disasters becomes – again, almost always – an immediately high priority.

Two Decades of Continuing But Sometimes Halting Progress

The vital role played by interdependent infrastructures has been understood since the early 1990s, but practical tools have yet to be developed to: (a) systematically assess the levels of security and resilience of infrastructures within a specific region; and (b) evaluate the numerous options available for enhancing their security and resilience. An objective, quantitative process is therefore needed for identifying and evaluating the various ways that regions can enhance security and resilience – within the limits of the financial and human resources available. To ensure that the results of a quantitative process are used in the practical world, such a process should, at a minimum: (a) fit integrally with the budget process of the public and private organizations that make infrastructure decisions; and (b) produce results that are directly comparable with infrastructure investment proposals for purposes other than security and resilience.

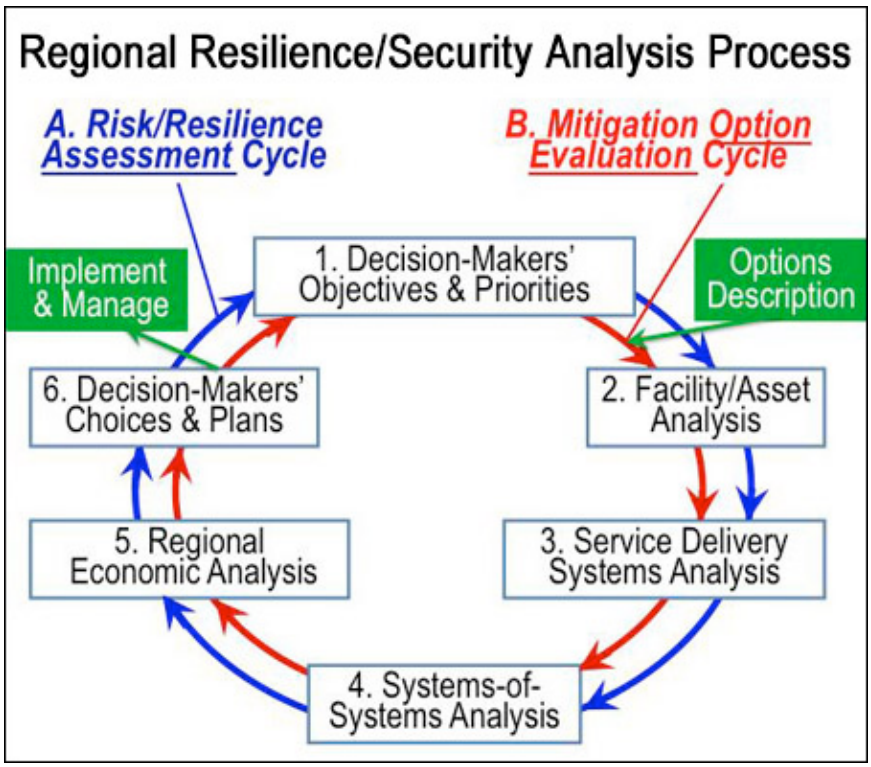
These budget processes are themselves in need of reform, particularly in the field of public infrastructures. As pointed out in a 27 March 2006 report, *Guiding Principles for Strengthening America's Infrastructure*, "We are both under-investing in infrastructure and investing in the wrong projects: *new investments are critically needed, but we lack the policy structures to make correct choices and investments* [emphasis in original]." Adding to both the credibility and urgency of that report, which was issued by the Center for Strategic & International Studies, is the fact that it was written, edited, and otherwise "vetted" by an expert team that included a number of sitting and former state governors, U.S. senators, and nationally recognized experts in infrastructure investment from areas throughout the country.

On 11 October 2010, the White House's three-member Council of Economic Advisers prepared, in cooperation with the U.S. Department of the Treasury, a complementary report, *An Economic Analysis of Infrastructure Investment,* which concluded that "Federal funding for infrastructure investments is not distributed … using rigorous economic analysis or cost-benefit comparisons. … The [current] process virtually assures that the distribution of investment … is suboptimal from the standpoint of raising national productive capacity." It is now obvious, partly because of that review, that there is a compelling need to develop a more rigorous analytic process for infrastructure investment that includes the added value to economic productivity, as well as improved security and resilience, that might reasonably be expected.

The Business Process – Its "Most Critical Components"

Last year, the Infrastructure and Geophysical Division of the U.S. Department of Homeland Security's Science and Technology Directorate sponsored the Regional Resilience/Security Analysis Process (RR/SAP) to meet this challenge. ASME Innovative Technologies – working in close cooperation with a team from The Brashear Group LLC, the Alion Science and Technology Corporation, Virginia Tech University, and The George Washington University – developed and tested the initial RR/SAP design, which is largely based on concepts and tools developed since 2002.

Among the most critical components of RR/SAP, which have been in development and testing stages since that same year, are: first-hand experience in nine infrastructure sectors and subsections; three national standards; four regions ranging in population size from 50,000 to several million people (the National Capital Region, Hampton Roads and Danville, Virginia, and Nashville-Davidson County, Tennessee); and numerous and varied regional disasters. The feasibility of RR/SAP also has been tested and assessed by key stakeholders (regional leaders, managers, operations and engineering personnel of critical infrastructure systems, core community services, and key elements of the business base) at all levels of government and industry, and has proved to be practical, reliable, and useful for supporting difficult public and private decisions.



Basically, RR/SAP consists of two cycles of analysis: (a) a *baseline risk/resilience assessment cycle* to quantify the primary risk and resilience challenges to a specific region (and its infrastructures and critical public functions); followed by (b) an *option evaluation cycle* to estimate the value of the specific options proposed and/or available for enhancing productivity, resilience, and security.

Six Phases, Numerous Variables, And Alternative Solutions

Both cycles follow the same six analytical phases, wherein the assessment cycle estimates current risk and resilience conditions – and the evaluation cycle estimates how, and how much, the proposed options would improve these conditions. The principal differences, usually, are the benefits expected from the various options available. The six tasks (illustrated in the accompanying figure) are carried out in the following order:

1. Decision-makers define and rank objectives, criteria, metrics, and priorities for productivity, resilience, continuity, security, and other factors. In the first cycle (risk/resilience assessment), these are developed through a rigorous paired-comparison process (called the Analytical Hierarch Process – a carefully structured method for ranking objectives and alternatives that has become widely used in the military, private industry, and even player selection in the National Football League). In the second cycle (mitigation option evaluation), the initial objectives may be refined, but the primary emphasis is setting priorities for developing the options needed to enhance resilience and security.

2. Key facilities and their assets undergo a *static* in-depth, confidential risk/resilience analysis using an all-hazards, all-quantitative American National Standard Institute (ANSI)/American Water Works Association Standard No. J100-10, Risk and Resilience Management of Water and Wastewater Systems, 2010 approach. That approach uses methods consistent with the Department of Homeland Security's

own National Infrastructure Protection Plan wherein risk is a function of threat likelihood, vulnerability, and consequences – resilience is a function of service outage severity and duration, and there is the same vulnerability and threat likelihood. In the first cycle, the current risk and resilience are estimated. In the second, the risk and resilience that would exist if the options were implemented are factored into the equation; the difference is considered to be the "gross benefit" of the option.

3. Service delivery systems operating under current configuration and control systems are modeled, using a systems-dynamics approach to refine the owners' estimates in a dynamic analysis that captures the effects of the system's ability to cope with emergencies. This analysis also identifies the specific geographical locations of outages – a critical factor in identifying and understanding where *other* infrastructures may be impacted.

4. Various dependencies among the systems are analyzed using a combined-systems dynamics model to determine where one system's difficulties might adversely impact other systems' operations, quantifying direct dependency risks and resilience issues for other owners as well as for the region as a whole.

5. Estimated service outages and shortages are analyzed using a regional input-output economic model to estimate the total economic impact – including "ripple effects" and multipliers – on the regional, state, and possibly national levels. This model also estimates the impacts on revenue and output of each major industry sector in the region as well as the probable regional impacts on jobs, wages, and local tax collections.

6. Decision-makers review the results. In situations where the baseline assessment cycle's results are unacceptable, the option evaluation cycle defines a range of new capabilities, projects, programs, and/or investments that might be needed, and used, to enhance productivity, resilience, continuity, and security; these possibilities usually are analyzed by revisiting all of the preceding analytical phases to estimate the possible ways in which (and the extent to which) the programs and investments required will generate identifiable improvements (expected benefits) and the associated capital and operating costs involved. The benefits and costs are estimated from the perspectives of *both* the owners of the respective systems *and* of the region's public. The respective decision-makers will review these evaluations to determine which (if any) should be included in their own budgets and operational plans.

The Distinguishing Features of RR/SAP

RR/SAP is designed to exhibit several highly desirable features, including the following operational virtues and capabilities:

- Being technically sound, quantitative, objective, and repeatable;
- Possessing estimated values relevant and related to decision-makers' objectives, risks, resilience, benefits, and costs in terms that are directly comparable and consistent throughout – and directly comparable as well to other, unrelated, investment options, to support budget and program decision-making;
- The ability to report decision-relevant results from the perspectives of *each* – the owners and the regional community, respectively – using data based on the common "physics" of specific threats to specific assets and their physical impacts;
- The complementary ability both to estimate risk/resilience vulnerabilities and to incorporate the likelihood of unwanted events and the various additional vulnerabilities that might be associated with each;
- Inclusion of the explicit effects of dependencies and interdependencies both on owners and on the region as a whole – along with a supporting analysis of how best to limit/mitigate such effects;
- The capability of being carried out and maintained by on-site, non-specialized, non-expert staff; and
- The inherent ability to permit periodic re-analyses, over a certain period of time, for accountability and progress measurements.

Rollout, Results, and Recapitulation

RR/SAP has already been demonstrated to be feasible, but requires additional development and testing to bring it to its full potential to rationalize infrastructure investment. These refinements could be carried out in a combined testing-development-enhancement program by any of several entities. Major metropolitan regions could adopt RR/SAP, for example, as the operational vehicle needed to rationalize and vindicate their own infrastructure investments.

Jurisdictional issues in some metro areas might reasonably suggest that states initiate and manage the process – or establish multi-jurisdictional authorities to do so.

RR/SAP also could serve as the basis and foundation of a national "bottom-up" program to use risk analysis to increase the preparedness, value, security, and resilience of infrastructures, to stimulate self-help and local determination, and/or to include as an indispensable element of federal grant programs – maintaining a set of highly comparable regional assessments by which national progress could be measured.

In similar fashion, related efforts by user communities and cross-regional information sharing could help spread innovative options and develop best practices models. The 2011 Presidential Policy Directive (PPD-8) on National Preparedness issued by President Barack Obama mandates risk-informed, decision-making for "all-of-nation" resilience and security; RR/SAP could and probably should be, therefore, evolved into an ongoing standardized process linking newly integrated homeland-security grants programs. Or it could become a service and/or integrated service-product offering provided by a forward-looking technology or consulting firm.

Whatever else happens, the results of the refinement and widespread use of this revolutionary new business process will be: (a) rational, public-private collaboration toward local-preference, risk-analysis-based priorities; and (b) future investments that make regional infrastructure systems and community facilities more valuable, resilient, secure, and reliable – and, in aggregate, create a more productive, resilient, secure nation that is able to protect all of its citizens, businesses, and society as a whole.

For additional information on:
The Center for Strategic & International Studies' "Guiding Principles for Strengthening America's Infrastructure," visit http://csis.org/files/media/csis/pubs/060327_infrastructure_principles.pdf

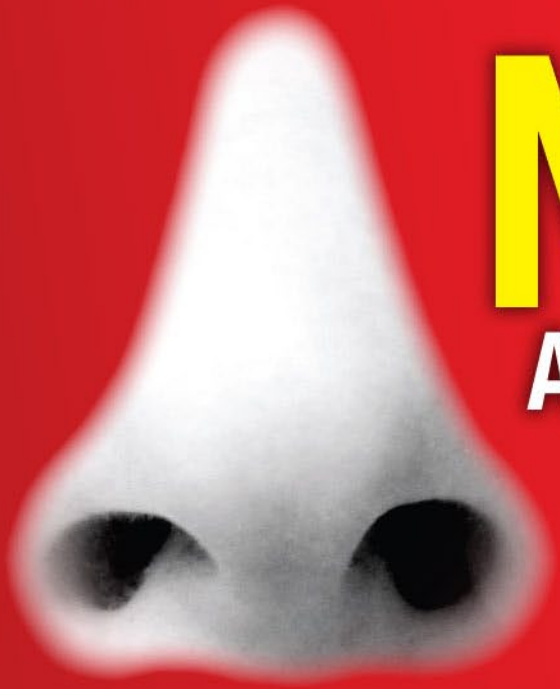
The White House report "An Economic Analysis of Infrastructure Investment," visit http://www.whitehouse.gov/sites/default/files/infrastructure_investment_report.pdf

The American Water Works Association Standard J100-10, visit http://apps.awwa.org/WaterLibrary/ShowAbstract.aspx?an=0072080

The Southeast Region Research Initiative, visit http://www.serri.org/dhs/Documents/October%202011/ASME%20Project%20-%20October%202011%20Review%20Meeting%20-%20Presentation%20Version%20(Brashear).pdf

---

Dr. Jerry Brashear is a researcher and consultant on infrastructure risk/resilience policy, analysis, and management processes. He has led risk-consulting and R&D programs at ICF Consulting, The University of Texas at Austin, George Mason University, the American Society of Mechanical Engineers, and The Brashear Group LLC to advance the practice of infrastructure and regional risk/resilience analytic methods and processes. He consults to senior management in infrastructure and homeland security agencies and on infrastructure services at all levels in the United States and internationally. He holds degrees from Princeton, the Harvard Business School, and the University of Michigan.



NOT A CHEMICAL HAZARD DETECTOR

BUT THIS IS!

AP4C HANDHELD CHEMICAL DETECTOR

- No On-Shelf Cost
- Easy Operation
- Single-handed Operation
- Fast Start & Recovery
- Fast 2 Minute Response
- Simultaneous Detection
- Portable Compact Design
- Rugged Construction

ADVANCED SPECTRO-PHOTOMETRY TECHNOLOGY QUICKLY DETECTS:

Nerve, Blister & Blood Agents, TICs & TIMs, Precursors, Vomiting Agents, Homemade Agents, Hydrocarbons.

VEHICLE & FIXED VERSIONS ALSO AVAILABLE

PROENGIN

GAS & LIQUID CHEMICAL DETECTION

(954) 760-9990 • www.proenginusa.com • e-mail: sales@proenginusa.com

The Role of Social Media Before, During, and After a Disaster

By Christina Spoons, Fire/HazMat

Many people now use social networking tools such as Facebook, Twitter, and LinkedIn to keep in touch with friends, follow businesses they support, and expand their own personal and business networks. The integration of social media into the daily lives of so many has resulted in these same networking tools playing an increasingly important role in emergency preparedness and response, on multiple levels.

Members of the local community almost anywhere in the country, for example, are using social media to seek assistance during an emergency; others are using social media as a source of important – sometimes lifesaving – information before, during, and after a disaster; and response agencies are using social media, preferably before a disaster, to disseminate prevention and/or mitigation and recovery materials.

Using Social Media To Seek Assistance

A 2011 American Red Cross (ARC) online survey of 1,046 adults and telephone survey of 1,011 adults found that, if they needed assistance and could not reach 911, more than one in five of all respondents would attempt to contact authorities by using email, websites, or social media. Nearly one-fourth of the general public and one-third of the online population would also use social media to let loved ones know they are safe during an emergency.

A 2011 survey reaffirmed the importance of first responders "staying connected" to the public they serve. Hosting a continuous source of reliable information through social media channels will better prepare communities and assist responders before, during, and after a disaster.

In 2009, to cite but one unusual example, two girls lost in a storm drain in Australia, instead of calling for assistance, posted a Facebook status saying that they were lost. According to the Metropolitan Fire Service, one of the girls' friends was online, saw the posting, and called authorities to help the girls. Similarly, in 2011, trapped survivors of earthquakes in both New Zealand and Turkey used their cellphones to text messages to help rescuers locate them.

The ARC survey also found that respondents would not only use social media to request help, but also would expect agencies to be monitoring their own social media sites in order to respond to requests for assistance. In fact, at least one-third of the general and online populations, according to the survey, would expect such help to arrive within an hour after posting a request for help to a social media site.

Using Social Media as A Source of Information

Social media users are not only using sites to update their friends and family, they are also using their online sites as a major source of information. With cameras becoming a common feature on cellphones, as soon as an event occurs, onlookers can immediately: (a) post information about it to friends on Facebook; (b) tweet details to followers on Twitter; (c) upload video and photos to the world at large on YouTube and Flickr; and/or (d) call or text updates and observations to the media. It is not surprising, therefore, that the ARC survey found that social media sites are already the fourth most popular source for finding information about emergencies – often as those emergencies are actually occurring. Recently, in fact, more online respondents have used social media sites than have used NOAA (National Oceanic and Atmospheric Administration) weather radios to obtain information related to a broad spectrum of emergency situations.

Approximately half of the survey respondents said they sign up for emails, text alerts, or other means to receive information during an emergency. To keep up with the demand, many local jurisdictions now offer such services. Residents, business owners, and/or others who require and/or are otherwise interested in such information can register online to receive email or text alerts related to a long list of "typical" emergencies. Users can simply check the boxes of the top-

ics about which they wish to receive information. By using such technology, various political jurisdictions can program email or text messages, related to such incidents, that can be sent to those who have requested them.

The Federal Emergency Management Agency (FEMA) also offers a text message service. Users may text PREPARE to 43362 to sign up to receive monthly disaster safety tips, or text SHELTER+ ZIP code to 43362 to find the nearest shelter in the area. In addition, users may also text DRC+ ZIP code to 43362 to find the nearest disaster recovery center in the area. The text service not only allows users to be better prepared in the event of a disaster, it also provides a means for those caught in the middle of a sudden disaster to receive up-to-date information at the time they urgently need it.

Using Social Media for Prevention

Many organizations are now using social media to disseminate their own prevention messages. Social media networks allow organizations to spread their messages to a much wider audience through friends or followers re-posting, forwarding, and/or re-tweeting content.

FEMA itself has created a smartphone application (app) through which users can find information, for example, on: (a) numerous useful items that should be included in an emergency kit; (b) the storage of emergency information, such as pre-arranged family meeting locations; and (c) safety tips on what to do before, during, and after a disaster. The same app includes a map of shelters and disaster recovery centers throughout the United States. Much of this and other information is downloadable, moreover, so the information needed is available even if cellphone service is not.

In addition to the smartphone app, FEMA regularly posts prevention messages on the agency's own social networking sites. Recent postings include tips on severe weather and the updating of vehicle emergency kits. The National Fire Protection Association also regularly posts fire prevention messages.

National organizations are not the only ones active in social media. Many fire and police departments throughout the entire country, local chapters of national organizations, and numerous other agencies, public and private, and even a number of businesses post specific information on various emergencies and disasters to those they serve or represent in their respective communities.

Social Media Responsibilities – Of Course

Of course, with information comes a full measure of responsibility as well. To begin with, it is or should be obvious that not all information that shows up online is totally accurate. Individual citizens can and should share information responsibly by redistributing only information that has been confirmed, and by refraining from posting emergency information on sites that are not always watched and/or monitored. Response organizations can help in this area by posting their own hours of operation – by doing so, they will help individual citizens know if someone is "on duty" to see and, if necessary, act upon the information posted.

With more than five billion mobile phone subscriptions and more than one billion mobile broadband subscriptions logged in worldwide at the end of 2010, the International Telecommunication Union expects web access through laptops and smart phones to surpass web access from desktop computers within the next five years. In short, the integration of social media into the daily lives of so many people, in every nation in the world, has significantly changed the way people keep in touch, do business, and seek information.

Moreover, it seems inevitable that the role of social media in the emergency services will continue to increase in importance as the world as a whole becomes even more mobile, more connected, and more fully "on alert" – on a 24/7 basis – for the foreseeable future.

For additional information on:
The 2011 American Red Cross survey, visit http://www.redcross.org/portal/site/en/menuitem.94aae335470e233f6cf911df43181aa0/?vgnextoid=7a82d1efe68f1310VgnVCM10000089f0870aRCRD

Christina Spoons holds a Masters Degree in Public Administration with a concentration in Homeland Security from Walden University, and is currently completing her Ph.D. in the same discipline with a concentration in Terrorism, Mediation, and Peace – also from Walden. Her emergency services experience includes several years as a firefighter/EMT and as an instructor with the American Red Cross. She has been active in the development of firefighter curricula at both the state and national levels and also is active with several National Fire Protection Association committees. She teaches homeland security and public policy and administration courses at Ashford University, and fire science courses at Columbia Southern University.

IT Preparedness: At Long Last, a Major DHS Priority

By Jordan Nelms, Cyber & IT

Last year, just before Thanksgiving, the Curran-Gardner Public Water Plant in Springfield, Illinois, experienced a troubling event. A computer operated in a foreign country somehow gained control of the plant's Supervisory Control and Data Acquisition (SCADA) system, repeatedly turning a single pump off and on until the pump failed, causing disruption of the city's water system. Even though initial reports of malicious intent turned out to be proven false, news reports describing a foreign terrorist gaining control of a public utility infrastructure system spread like wildfire. The Springfield event underscores the increasingly ostensible threat that an intentional or accidental failure of an information technology (IT, or cyber) system poses to the nation's critical infrastructure.

The foundation of every jurisdiction's emergency preparedness program is threat or hazard identification, including the calculation of risk – as measured both in monetary cost and in the loss of human life. This fundamental public safety practice – also known as "THIRA" (Threat/Hazard Identification and Risk Assessment) – examines the comprehensive picture of natural, manmade, and technological hazards that have the potential to cause an emergency incident or disaster.

Common THIRA practice across the United States focuses on hazards that public safety officials can readily identify through historic occurrences and potential vulnerability. An often overlooked threat or hazard – for which considerable resources are just now becoming available to respond to and mitigate against – is an IT disruption.

Understanding Criticality and Vulnerability

Emergency preparedness geared specifically toward mitigating the consequences of an IT disruption requires a forward-looking and comprehensive understanding of what that type of disruption might mean in terms of criticality and vulnerability. In recent years, IT systems have become ubiquitous, and affect all aspects of the daily lives of everyday citizens, business owners, government managers, and public safety officials. There is a reliance on IT systems of some sort for powering offices, communicating with others, controlling critical infrastructure, and maintaining situational awareness in the event of emergency. In 2012, one would be hard pressed to identify a single facet of daily life in which IT systems do not play a critical role.

IT systems have experienced an almost unhindered expansion into the most vital processes of the nation's infrastructure, becoming an interconnected network that today literally reaches around the globe. A disruption of these systems may cause direct damage to computer networks that support a jurisdiction's vital services for its residents, as well as its local critical infrastructure – e.g., traffic systems, power and other utilities, and communications systems.

When one considers that a high percentage of the nation's critical infrastructures run on SCADA systems, it becomes obvious that an IT disruption to any of the aforementioned computer networks could be catastrophic, and would have major implications for not only a local jurisdiction but also for many other jurisdictions, entire states, and the federal government.

The Federal Approach: Increased Funding, an R&D Roadmap, NLE 2012

Over the last several years, the federal government has recognized the need for national cyber contingency capabilities by increasing this portion of the Department of Homeland Security (DHS) budget to $443 million – $80 million over the previous fiscal year's appropriation. The Quadrennial Homeland Security Review (QHSR) identified DHS as one of the components of the national homeland security enterprise that "possesses unique capabilities and, hence, responsibilities." DHS was built on the foundation of the National Response Framework's Cyber Terrorism Annex and now functions as the federal government's penultimate department for coordinating IT disruption activities. In late 2011, to help guide the federal cyber-security apparatus, DHS released two strategic documents outlining the cyber-security mission, and provided a roadmap for the expenditure of research and development funds.

DHS's National Cyber Security Division (NCSD) operates four key components of the federal government's IT

response program. The department's newly created National Cybersecurity and Communications Integration Center (NCCIC) serves as a 24-hour watch center (similar to the National Response Coordination Center) for all IT-related incidents. When an incident is identified and authenticated, an alert is published through the National Cyber Alert System. Such alerts are typically issued for potential terrorist activity and for sharing information with IT managers on potential security vulnerabilities in common software packages.

The operational arm of the NCSD is the United States Computer Emergency Readiness Team (US-CERT), which ensures the federal government's situational awareness to IT-related threats through constant vigilance, and the coordination of the federal government's IT emergency response. The National Cyber Response Coordination Group (NCRCG) serves as the overarching body that: (a) shares IT-related incident information with agencies throughout the federal government, and with state and local governments; and (b) coordinates the federal interagency response across all sectors and disciplines. Finally, the NCSD Cyber Cop Portal coordinates the intelligence gathering and prosecution of cyber crime and malicious cyber activity.

Although there is no historical precedent, the new "threat" of a disruption or failure of IT systems should not be overlooked. The nation's critical infrastructure depends on identifying this risk and developing public safety practices to mitigate it quickly and to the greatest extent possible.

Recognizing the potential damage an IT disruption may cause, the Federal Emergency Management Agency (FEMA) selected the National Level Exercise (NLE) 2012 to focus on identifying the current planning, organization, equipment, and training gaps in emergency preparedness to respond to a cyber incident in New England. Responding to a cyber incident with national significance requires coordination not only across a broad spectrum of federal agencies, but also through several vertical levels of government, managing the consequences of such an event on local towns and municipalities.

Strengthening Emergency Preparedness at State and Local Levels

The addition of a potential IT disruption on a state or local jurisdiction's critical infrastructure presents a new challenge in emergency preparedness at the ground level due to the threat's physical invisibility, and its potential to be just as disruptive and deadly as any traditional intentional threat or natural hazard. Emergency preparedness in response to an IT disruption requires a jurisdiction to take the steps required to enhance its contingency planning efforts to meet the needs of its residences and businesses as well as the community as a whole.

There are many players involved in the response to an IT disruption. Engaging these stakeholders through seminars, workshops, or public meetings well prior to a potential incident is critical to improving collaboration during an actual emergency. Either individually, or through stakeholder working groups, public safety agencies must meet with officials from surrounding jurisdictions, critical infrastructure providers, and other pre-identified organizations and agencies to form a collaborative team that can work to identify issues that might require a potential emergency response, either initiated or exacerbated by an IT disruption, and to develop solutions to those concerns.

Securing a universal stakeholder buy-in is essential if public safety response operations are going to be successful. In addition to developing an appropriate response, state and local law enforcement agencies must be tied in to the national network of homeland security fusion centers to ensure the proper reporting of suspicious activities – specifically including suspicious or malicious IT activity. This critical tool for prevention of traditional terrorist activity is equally applicable to the IT realm.

With an understanding of the criticality and vulnerability posed by an IT disruption, public safety agencies can begin to develop incident-specific and functional support annexes to their Emergency Operations Plans (EOPs). An IT Disruption Annex (titled Cyber Incident Annex by the National Response Framework) outlines the concept of operations, policies, and roles and responsibilities for agencies that have primary or supporting roles in identifying, responding to, and remediating the

consequences of a malicious or unintentional disruption: (1) of a jurisdiction's computer networks; or (2) the computer networks of critical infrastructure providers within a specific jurisdiction.

The Overwhelming Consequences of a Major Disruption

Because IT is often viewed as a component of communications, an IT Disruption Annex may stand as an attachment to a traditional Emergency Support Function #2 Annex (or communications Incident Command System unit) dealing with a jurisdiction's communications infrastructure. Where ESF #2 deals with the continuity of communications infrastructure critical for emergency response, that infrastructure (if privately administered through an IT communications provider) may become intentionally or unintentionally affected by an IT disruption incident.

Large-scale IT incidents may overwhelm a local or state government emergency response organization's resources by disrupting the internet, taxing critical infrastructure information systems, and/or infecting critical infrastructure information systems. In a widespread IT-related incident, DHS will activate its resources to coordinate the federal response. In order to ensure proper coordination between local and federal agencies, a local or state government's IT Disruption Annex would prepare nonfederal agencies to coordinate more effectively with DHS. Many state and local governments have chosen to develop, adopt, and exercise similar plans with great success.

NLE 2012 will involve members of the DHS-funded Boston Area Regional Catastrophic Preparedness Grant Program (RCPGP) multi-jurisdictional catastrophic planning group. The Boston Area Region chose, among other contingency planning efforts, to develop a Regional Cyber Disruption Annex to the Region's Catastrophic Emergency Coordination Plan (RCCP). In addition, RCPGP funds were used to develop corresponding Cyber Disruption Annexes for the individual states within the Boston Area Region. NLE 2012 will test this regional cyber response coordination model to determine the "best practices" – in planning and operational tactics – needed to mitigate the consequences of IT-related emergencies.

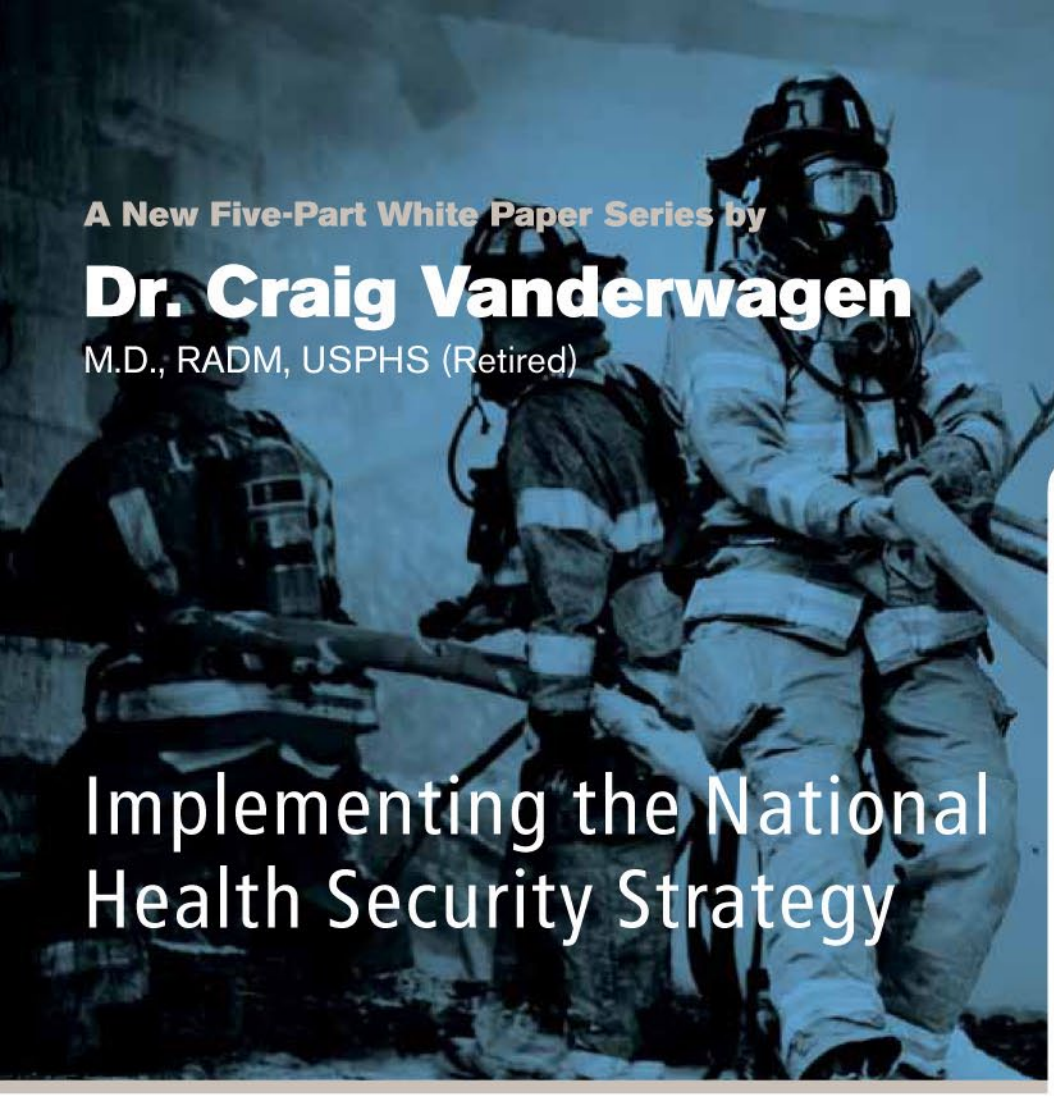
Although the consequences for Springfield's Curran-Gardner Public Water Plant may not have been catastrophic, they did highlight the increasing threat that IT disruptions pose to the government and private sector at all levels. This new lexicon of IT-specific emergency management components is becoming increasingly relevant. Today, although the federal government seems to have developed at least a preliminary strategy for organization and implementation of an effective IT emergency response program, many state and local homeland security and emergency management agencies are only just beginning their own planning processes.

For additional information on:
The 2009 DHS "A Roadmap for Cybersecurity Research," visit http://www.cyber.st.dhs.gov/docs/DHS-Cybersecurity-Roadmap.pdf

The 2011 DHS "Blueprint for a Secure Cyber Future," visit http://www.cyber.st.dhs.gov/wp-content/uploads/2011/12/blueprint-for-a-secure-cyber-future.pdf

---

Jordan Nelms is the Homeland Security specialist at Witt Associates, a public safety and crisis management consulting firm. He was on the Witt Associates planning team that developed the Boston Area RCCP and led the development of the State of Rhode Island's Cyber Disruption Incident Annex as well as a Cyber Annex template for the Commonwealth of Massachusetts. Prior to joining Witt Associates, he worked in the Emergency Operations Center and Emergency Public Information Office of Pinellas County, Florida. He is also a published researcher with Johns Hopkins University's Department of Homeland Security Center of Excellence: National Center for Preparedness and Catastrophic Event Response Center (PACER).



A New Five-Part White Paper Series by

Dr. Craig Vanderwagen

M.D., RADM, USPHS (Retired)

Implementing the National Health Security Strategy

"The public health mission to protect the health of the public and prevent disease is dependent upon effective and useful logistical systems designed specifically for the purposes of the public health practitioner."

From August 2006 until July 2009, **Dr. Vanderwagen** was the founding Assistant Secretary for Preparedness and Response (ASPR), U.S. Department of Health and Human Services.

The *Implementing the National Health Security Strategy* white paper series, written by the first Assistant Secretary for Preparedness and Response, Dr. Craig Vanderwagen, explores issues that affect the success of the public health practitioner in meeting the needs of the public's health, and by doing so, increasing the resilience of communities and the Nation.

White Papers Now Available for Download:

- The Role of Logistics in Public Health Practice
- The Role of Patient Tracking in Public Health Practice
- The Public Health Challenge in Mass Evacuation and Shelter Care
- Event Management: Visibility in the Fog of Response
- It is Time for Action

Scan this code to download the whitepapers

Download the White Papers today at
upp.com/vanderwagen

White Paper Series Underwritten by:
Upp Technology, Inc.
800.777.6092
upp@upp.com

innovative technology solutions

Social Media: A Seismic Opportunity

By Jordan Scott, Emergency Management

On 23 August 2011, a 5.9-magnitude earthquake struck Mineral, Virginia, and rattled a large area up and down the U.S. East Coast – an area unaccustomed to such seismic events. In the moments that followed, information and shocked reactions spread at an unprecedented rate. But the first reports were not on television or other traditional media. Rather, news of the quake was being reported through literally hundreds of social media websites, mobile applications on cellphones, and other electronic devices of those who had experienced the shocks personally.

In a conference room full of emergency planners in Eureka, California, the first news came to the group not from their own offices and headquarters, but from East Coast acquaintances posting messages to the Twitter and Facebook pages of the conference attendees. In fact, by the time the first official reports were released, responders across the nation were already well aware of the situation and were working on plans for the next steps that should be taken. The power of social media and its value as a viable communications tool in emergency response situations was once again made clear.

The past year witnessed many other events around the world that have further underscored the increased and still growing importance of social media. From communicating immediate information on such major disasters as the Joplin, Missouri, tornados and Japan's earthquake/tsunami, to the coordination of political movements in Libya and the United States (the various "Occupy" demonstrations), a higher percentage of the population is now accessing social media and relying on it for accurate and up-to-the-minute information.

The ARC Survey: Some Compelling Findings

In the summer of 2011, the American Red Cross (ARC) conducted a survey to determine how the U.S. public might use social media to its best advantage, particularly in times of crisis. Among the key findings in that survey were the following:

- The Internet is the third most popular way for people to gather emergency information – already, 18% of the population specifically uses Facebook for that purpose;
- About 24% of the general population and almost one third (31%) of the online population say that they would use social media to let their loved ones know that they are safe;
- A huge 80% of the general population, and 69% of the online populations surveyed, said they believe that, to improve their ability to act promptly in times of crisis, national emergency response organizations should routinely monitor social media;
- Among those who said they would post a request for help through social media, 39% of those polled online – and 35% of those polled via telephone – said they would expect help to arrive in less than one hour.

Because of the public's growing reliance on social media channels as an information source, it has become increasingly clear that emergency managers have not only a unique opportunity but also an almost moral obligation to exploit the many new tools now available to reach the American people "where they are" – online, in other words.

Quick Tips & Analytic Tools – At 5,500 Tweets Per Second

A major effort to do just that is currently underway in California, where the California Emergency Management Agency has teamed with the California Seismic Safety Commission and the California Earthquake Authority to create "Totally Unprepared" – an earthquake readiness campaign driven by the sharing of information through social media. Using popular social media websites such as YouTube, Facebook, Twitter, and others, the Totally Unprepared campaign is able to deliver valuable preparedness information in a format that meshes with the needs of the online community. Through short video clips, tweets, and quick tips, users receive regular doses of information teaching them how to prepare for, react to, and respond to an earthquake.

The campaign also is attempting to grab the attention of viewers by using an interactive "fun" approach that works in stark contrast to the more standard approaches that might otherwise overwhelm and/or frighten those who need to be reached. Totally Unprepared was developed following a study conducted by the University of California, Los Angeles, which showed that less than half of the state's residents had taken the steps needed to prepare for an earthquake. It was clear, the study also showed, that most Californians are in fact aware of the huge risks posed by earthquakes, but the previous preparedness messages had not inspired enough of them to take the actions needed to cope with those risks.

Although there are no official numbers yet available to prove whether or not a higher percentage of Californians are now preparing for earthquakes (and/or other disasters) as a result of the Totally Unprepared campaign, it seems clear that the thrust of that message is, in fact, being both seen and heard. By using the analytic tools that are built into many social media sites, it is now possible to track how many individuals are receiving, viewing, and sharing the preparedness messages. Moreover, with hundreds of video views, new "friends," and followers being tracked each day, it seems abundantly clear that "the official word" is getting out, and spreading at an impressive pace.

Twitter reported – to cite but one example – over 40,000 earthquake-related tweets were sent within the first minute of the Virginia earthquake – a rate of nearly 5,500 tweets per second. It is highly unlikely that government and/or any other organizations and agencies, public or private, would receive anything close to that type of response through a news release or press conference.

Controlling the Pace, Squelching The Rumors, Fulfilling an Obligation

In an emergency, information being distributed through more traditional means quickly becomes irrelevant and may quite possibly be smothered by the crush of online messages being sent at a frenzied pace. Rumors and false information can quickly dilute the facts. Without a reliable social media presence providing accurate information to temper/correct the masses of false or misleading information also being disseminated, an organization's reputation as an information resource can suffer among an online community seeking answers "right now."

A credible organization providing regular updates via social media sites can effectively control "the story" in real time, address rumors both quickly and accurately, anticipate the needs and concerns of the public, and provide accurate information throughout an incident. Social media communications can also become a valuable resource for the print and broadcast media covering an incident, thus providing an opportunity to further publicize the message.

Although there is still at least some reluctance within many emergency organizations to dive into social media environments, the value to be gained is growing more and more apparent to those agencies that are taking that additional step forward. Another factor to be considered is that, in an uncertain economic climate, it has become increasingly important to seek new opportunities to reach the public at little to no cost. Social media websites offer just such an opportunity because of their unprecedented ability to connect and communicate with a huge percentage of the population who are actively seeking the information provided by emergency management agencies.

Today, when an earthquake strikes in California, most of that state's population understands that the best way to avoid injury is to "drop, cover, and hold on" until the shaking stops. During the Virginia quake, however, hundreds and perhaps thousands of Americans up and down the East Coast ran from their buildings, placing themselves at much greater risk – while also grabbing for their phones to tweet relatives, friends, and neighbors about what had just happened. The quake created confusion, uncertainty, and an immediate large-scale need for information.

In the first minute following the quake, in fact, an estimated 40,000 people were on Twitter talking about what had happened – proving again what an extraordinary opportunity is now available for emergency management agencies to reach a broad audience. In an industry where information sharing is so critical, the opportunity to establish and maintain a social media presence is not one that these agencies can afford to miss. In that context, it is or should be obvious, social media networking is not simply another tool to help extend the reach of an organization but, rather, the means needed to carry out an ongoing obligation to the public that the organization is serving.

For additional information on:
The key findings of the 2011 American Red Cross survey, visit http://www.redcross.org/www-files/Documents/pdf/SocialMediainDisasters.pdf

The Totally Unprepared Campaign, visit http://www.totallyunprepared.com/

The study conducted by the University of California, Los Angeles, visit http://www.calema.ca.gov/NewsandMedia/Pages/Current News and Events/California-Earthquake-Preparedness-Study.aspx

The Drop, Cover, and Hold On Campaign, visit http://www.dropcoverholdon.org/

The California Emergency Management Agency, visit www.calema.ca.gov or www.twitter.com/calema

---

Jordan Scott is a Public Information Officer and the Director of Social Media for the California Emergency Management Agency (Cal EMA). In addition to his work building Cal EMA's social media presence, he also develops and maintains content for the agency's website and works with his team to coordinate public and media outreach efforts. Jordan joined Cal EMA in 2009 following thirteen years working with the California Environmental Protection Agency and some time in local radio conducting promotional outreach. In 2002, he received his Bachelor of Arts degree in Communications Studies and Digital Media from California State University, Sacramento.

Funding Realities & Emergency Preparedness: A Grim Outlook

By Raphael M. Barishansky, Funding Strategies

"The sky is falling" is no longer just a Chicken Little reference – but, rather, a timely warning about the state of U.S. public health emergency preparedness initiatives in the face of recent large-scale funding cuts by the federal government that may well continue for the foreseeable future.

Following the anthrax attacks in 2001 that created a near panic shortly after the 9/11 terrorist attacks on the World Trade Center towers and the Pentagon – and with the recognition that all responses to public health emergencies begin at the local level – Congress appropriated the funding needed by the Centers for Disease Control and Prevention (CDC) to improve the disaster preparedness capabilities of public health departments nationwide – at all levels of government. This dedicated funding – distributed in the form of Public Health Emergency Preparedness (PHEP) grants – was and is specifically intended for use by states, territories, and major U.S. cities throughout the nation. In most cases, the funding is provided to states and then distributed to local jurisdictions.

Included in the PHEP cooperative agreements is funding for the Cities Readiness Initiative (CRI), which helps state and local jurisdictions draw emergency medical supplies from the CDC's Strategic National Stockpile (SNS). This program focuses on enhancing preparedness for response to large-scale bioterrorist events by providing such supplies, within 48 hours or less after an official request is made, to the nation's largest cities and metropolitan statistical areas, where more than half of the U.S. population lives.

Between 2001 and 2008, there was a steady decline in the funding available from the CDC's PHEP cooperative-agreement allocation to support public health preparedness activities in state and local health departments. Meanwhile, the demands on public health emergency preparedness planning, preparedness, and response capabilities and workloads continued to increase. In fact, according to the CDC, PHEP funding declined from $970 million in Fiscal Year 2003 (FY03) to $689 million in FY09.

Large-scale cutbacks in Public Health Emergency Preparedness funds are raising concerns at all levels of government – from local health departments to the CDC. Sustaining the critical role that the public health community plays in emergency response depends primarily on a reliable and steady flow of funding.

Preserving Capabilities, Protecting the Core, Preparing for the Worst

As one example of how this decline affected readiness, the CDC distributed $325 million of emergency supplementary funding in FY07 that was specifically earmarked for pandemic influenza preparedness activities. Two years later, though, in FY09, not only was there a lack of new funding for pandemic influenza, but overall PHEP funding – which may have been used to cover at least some pandemic influenza initiatives – also declined.

Nonetheless, federal funding is still the core source of financial support for the public heath preparedness programs of many local health departments (LHDs). In 2007, the National Association of County and City Health Officials (NACCHO) pointed out that 41 percent of all state and local health departments that received funding from the CDC's PHEP grants reported that those funds comprised 100 percent of their budgets for preparedness activities – significantly including the cost of dedicated emergency preparedness staffing. A 2009 NACCHO follow-up survey indicated that, at approximately 68 percent of LHDs, the CDC's PHEP cooperative agreement funds constituted 90 percent or more of their preparedness budgets.

The LHD preparedness programs have received some additional, but limited, support from other sources of funding – unfortunately, those funds also have been declining. In 2007, 46 percent of the nation's LHDs

reported receiving at least some financial support from local, city, or county funds; that percentage dropped to 29 percent in 2009, however, and continues to decrease. Further complicating the picture is that several media reports indicate that state and local budgets for public health also have diminished significantly in recent years – primarily, it seems, because of the nation's overall economic decline.

Focusing on the Present – But Forgetting the Future?

One of the tangential but nonetheless critical issues related to healthcare funding is the need to fund the so-called "disease du jour." An ongoing pattern of ramping up funding for an emerging public health threat, therefore encouraging the development of additional internal structures and services, then later withdrawing access to federal support, is having a particularly harmful effect on preparedness. One of the best examples of this process of fiscal "management by crisis" can be found in the reaction to improving preparedness, at all levels of government, to cope with a pandemic influenza. In December 2005, Congress appropriated $350 million for overall pandemic influenza planning and response efforts on the part of state and local health departments, and allocated an additional $250 million to that fund in June 2006. Additional funds were made available in fiscal years 2007 and 2008 – but Congress abruptly discontinued that funding stream in FY09.

In FY10, though, Congress approved a $7.65 billion emergency supplemental appropriation for pandemic influenza response activities. Included in that total was $350 million for state and local health departments. This legislation was in large part a positive response to advocacy efforts that stressed the need to support the capabilities of state and local health departments to prepare effectively for, and respond to, the then-ongoing H1N1 influenza pandemic.

On an operational level, these funds were allocated to various initiatives related to H1N1 and, in retrospect, seem to have helped immeasurably in numerous state and local response efforts. However, considered at a more strategic long-term level, such irregular supplemental appropriations are not sufficient to maintain local public health preparedness and response capabilities in the long term, especially when almost all health departments, no matter what their size, rely heavily on regular federal funding to support permanent staff positions.

According to a December 2011 report – *Ready or Not? Protecting the Public from Diseases, Disasters, and Bioterrorism* – issued by the Trust for America's Health (a private-sector health policy organization), the cutbacks in this vital element of public health systems are occurring on three levels – state, local, and federal. Following are some of the particulars:

- ***State Cuts:*** 33 states (plus Washington, D.C.) cut funding for public health from FY09 to FY10. Of these jurisdictions, 18 were cutting public health preparedness funding for the second year in a row;

- ***Local Cuts:*** In January 2010, 53 percent of the nation's LHDs reported that their core funding had been reduced from the previous year, and an even higher percentage anticipated additional cuts in FY11; the local cuts have resulted in a weakening of the nation's overall "boots on the ground" public health infrastructure – best exemplified, perhaps, by the loss of approximately 23,000 jobs, or approximately 15 percent of the local public health workforces, since January 2008; and

- ***Federal Cuts:*** Since FY05, federal support for public health preparedness programs has been reduced by 27 percent.

"At Risk": The CRI, State Labs & Essential Field Officers

The same report identified a number of key programs considered to be "at risk" because of the continued cuts in federal public health emergency preparedness funds. More specifically:

(a) Of the 72 cities participating in the Cities Readiness Initiative (CRI), 51 are now at risk of being cut from a program that supports the ability of cities to rapidly distribute and administer vaccines and medications to a large number of people during unforeseen emergencies;

(b) All 10 of the state laboratories currently possessing "Level 1" chemical testing capabilities are at risk of losing their top-level status, a downgrade that would leave the CDC itself with *the only public health laboratory in the country* possessing the full ability to test for chemical terrorism and accidents; and

(c) There are 24 states also at risk of losing the support provided by Career Epidemiology Field Officers – i.e., CDC experts assigned to various state health departments to supplement state and local efforts to prepare for and respond to various disease outbreaks and other medical disasters.

Clearly, public health agencies and facilities across the country play a critical role in the nation's overall emergency preparedness and response capabilities. That role has grown even more important since the 2001 anthrax attacks as well as, in the decade since, numerous natural disasters, food-borne outbreaks, and other major public health emergencies (e.g., SARS and H1N1) that have been in the headlines in recent years. Local and state health departments are, in fact, better prepared for emergencies now than ever before in the nation's history. Since 2001, state and local preparedness capabilities have improved, both consistently and significantly, in such areas as mass vaccinations and prophylaxis planning, all-hazards preparedness training, implementation of the National Incident Management System and Incident Command System, and the installation and use of new or upgraded communication systems.

However, the lack of adequate funding, on a continuing basis, for these and other important programs remains a major concern for emergency planners. Decreases in federal financial support for public health preparedness programs already have resulted in significant staff layoffs. In addition, many state and local health departments are having difficulty managing their budgets, hiring and training staff, and conducting long-term strategic planning under the conditions of unpredictable fluctuations in funding.

Real-World Realities & Other Inconveniences

More specifically: According to NACCHO, 55 percent of the nation's LHDs reduced or eliminated at least one program between July 2010 and June 2011, and 20 percent of these programs were in or related to emergency preparedness. In addition, 53 percent of all health departments have experienced some type of negative job impact (e.g., furloughing of employees and/or an overall reduction of hours); this also reduces overall readiness. A continuation of this state of decline will have major implications for public health emergency preparedness efforts and may well result in a decrease in training efforts, an inability to drill or exercise, and/or simply a lack of the resources needed to support the real-world public health emergency responses looming just over the horizon.

The federal partners of state and local jurisdictions also are not immune to these long-running fiscal constraints. Since 2005, the CDC has seen its budgets for preparedness and response slashed by more than $350 million (to the current, FY11, levels of about $832 million). This significant cutback in funding directly, and adversely, challenges the CDC's own ability to respond to pandemics and other public health emergencies.

The future of the nation's health preparedness funding is, in short, uncertain – at best. The current outlook for potentially massive reductions in all federal grant funding streams – combined with state and local budget cuts – could have a huge, and harmful, impact on PHEP programs and activities across the board, and at all levels of government. Merely maintaining the current health preparedness capabilities requires not only flexible and sustained federal funding but also the ability, and statutory authority, to hire and train a large number of additional public health professionals in order to reap the benefits that have been built into the system in recent years. In short, without a strong national commitment, U.S. public health may quickly lose the capacity needed to meet current and future homeland security goals. In times of crisis, any reduction in capabilities caused by underfunding public health opens the nation to overburdened healthcare systems, overwhelmed response systems, and overloaded communication systems.

For additional information on:
The 2010 CDC Report, visit http://www.bt.cdc.gov/publications/2010phprep/background/funding.asp

The 2007 NACCHO Report, "Federal Funding for Public Health Emergency Preparedness: Implications and Ongoing Issues for Local Health Departments," visit https://eweb.naccho.org/eweb/DynamicPage.aspx?Action=Add&site=naccho&ObjectKeyFrom=1A83491A-9853-4C87-86A4-F7D95601C2E2&WebCode=ProdDetailAdd&DoNotSave=yes&ParentObject=CentralizedOrderEntry&ParentDataObject=Invoice%20Detail&ivd_formkey=69202792-63d7-4ba2-bf4e-a0da41270555&ivd_cst_key=00000000-0000-0000-0000-000000000000&ivd_prc_prd_key=9dd36007-e1cc-46b6-8a1a-136f7d60d0ff

The 2011 NACCHO Survey, visit http://www.naccho.org/topics/infrastructure/lhdbudget/upload/Overview-Report-Revised-Final.pdf

The 2011 report from the Trust for Americas Health, visit http://www.tfah.org/assets/files/TFAH2011ReadyorNot_09.pdf

---

Raphael M. Barishansky, MPH, is currently the program chief for Public Health Emergency Preparedness for the Prince George's County (Md.) Department of Health. Prior to establishing himself in this position, he served as executive director of the Hudson Valley Regional EMS (Emergency Medical Services) Council, based in Newburgh, N.Y. He is a frequent contributor to various journals, and can be reached at rbarishansky@gmail.com.

EXTRAORDINARY DETECTION FOR EXTRAORDINARY CIRCUMSTANCES

FOR MORE THAN 20 YEARS, FLIR RADIATION HAS BEEN KNOWN AS A WORLDWIDE LEADER IN THE DEVELOPMENT OF RADIATION DETECTION TECHNOLOGIES COVERING A WIDE RANGE OF APPLICATIONS, INCLUDING CUSTOMS AND BORDER PROTECTION, EMERGENCY RESPONSE, AND ENVIRONMENTAL MONITORING, AS WELL AS NUCLEAR RADIATION, CONTAMINATION, AND WASTE MONITORING AND CONTROL.

FLIR®
Extraordinary Protection

WWW.FLIR.COM/DETECTION

Emergency Responder 24/7 Information Tool Available Online

By Cortney Streets, Emergency Management

The concept now well known as "Information Sharing" grew and evolved significantly during the implementation, in October 2003, of Project Responder, which was jointly sponsored by the Oklahoma City Memorial Institute for the Prevention of Terrorism (MIPT) and the U.S. Department of Homeland Security (DHS). The project later evolved again – into the development and now widespread use of the Responder Knowledge Base (RKB) website (www.rkb.us).

The RKB, which is funded by DHS's Federal Emergency Management Agency (FEMA), is designed specifically to provide emergency personnel and organizations with a single source of integrated information on not only products, standards, certifications, and training, but also grants, publications, and equipment. The RKB currently makes all of this information, and more, available to almost 78,000 registered users – a number that continues to grow.

Almost if not all major disasters, incidents, and exercises are unique in at least some aspect and, of greater importance, require the involvement of various responder organizations at federal, state, and local levels of government. In order to maintain structure and illuminate a path forward, it is necessary for these organizations to collaborate with one another, both effectively and efficiently. To help them do so, the RKB provides emergency organizations, and individual responders, with huge quantities of information specifically related to products, publications, lessons learned, grants, and training that can be used to prepare for, as well as alleviate and eventually recover from, the impact of any type of disaster imaginable, either natural or manmade.

KLINKs, Focus Areas & A Multitude of Disciplines

Moving in lockstep with the escalating challenges and frequently changing needs of the nation's response community, the RKB itself has been steadily evolving in the past several years to become an increasingly robust source of information – and, for example, recently implemented a new "Focus Areas" tool that can be quickly and easily found on the RKB homepage. Focus Areas, which allow users to search for specific information in a timely manner, are organized by numerous disciplines, specifically including emergency management. After clicking on the "Emergency Management" icon, users will be redirected to "Publications & References," "Products," "Archived Grants & Assistance Programs," "Standards," "Training," "Web Links," and "Operational Assessments," as well as "Conferences" – all of which are focused specifically on various different but closely related aspects of the nation's Emergency Management doctrine and policies.

By clicking on the Products tab within the Focus Area, or on the homepage, users can view product specifics, as well as particularly important information associated with each product. Knowledge Links (KLINKs) are unique to the RKB and are located to the right of product details. KLINKs connect relevant content, allowing users to view a full circle of information. The KLINKs include items such as certifications, standards, safety notices, publications, and training that may be associated with specific equipment items.

One particularly helpful information-sharing tool available on the RKB is the *Volunteer User Opinion* module – the use of which gives first responders the opportunity to volunteer their individual and collective opinions about a specific piece of equipment. The only requirements are that the person giving his or her opinion: (a) is an active first responder; (b) has used the profiled equipment; and (c) is expressing an opinion about which he or she has no private or personal interest. If a user opinion is available for a product, the identification of that product will include a "user-opinion icon." (Because the RKB itself is not authorized to post any product opinions, users are forwarded to a request form that enables the user to directly contact one or more of the responders who has reviewed the product.)

What Funds Are Available? Where?

One of the more important questions emergency managers and responders must always address is how to pay for the equipment needed (a requirement that, in today's budget climate, probably will continue for the foreseeable future). To help answer this question, the RKB hosts grant information specifically provided by the DHS/FEMA's Grant Programs Directorate. The FEMA Preparedness Grants and Authorized

Equipment List (AEL) module provides a FEMA grants listing, as well as the AEL. The AEL is available only through the RKB, and indicates which equipment can be purchased with specific grant funds. One important caveat, though: The AEL does not state the specific product that is allowable; it simply lists the product category. In addition, users can also view the Standardized Equipment List (SEL), which spells out the various product categories that can be used to prepare for, and cope with, a broad spectrum of events and incidents that threaten the nation's security.

Numerous publications also are available to help emergency planners and responders in making difficult but nonetheless vital decisions. By selecting "Publications & References" via the Focus Areas tool, or through the "Other Content" tab, users can search through more than 2,000 publications – using the search tab will help responders search for specific documents. To further promote information sharing, the RKB has included a tab for Lessons Learned Information Sharing (LLIS) that will redirect users to a full list of the numerous documents developed by the LLIS team. LLIS is a DHS/FEMA program that serves as the national online network of lessons learned, best practices, and innovative ideas for the nation's emergency-management and homeland-security communities.

To help promote and provide information in real time, the RKB has also developed and implemented its own RKB Facebook page (http://www.facebook.com/ResponderKnowledgeBase), which provides, among other things, significant information related to upcoming conferences, news items, grant notices, and publications.

For additional information on:
How to use the RKB or register, contact the RKB Help Desk via e-mail at RKBMailbox@us.saic.com (or by phone at 1-877-336-2752).

Cortney Streets is a Web Analyst for the Responder Knowledge Base (www.rkb.us) website, the U.S. Department of Homeland Security/Federal Emergency Management Agency's principal online source of information available to First Responders. She received a Bachelor of Science degree in Business Administration from Towson University and is currently pursuing a Master of Arts Degree in Leadership and Management, with a concentration in Project Management, from the Notre Dame University of Maryland.

Scrubbing Source Data at the Local Level

By Michael Jacoby, Viewpoint

First responders and private citizens are the first line of defense, particularly in their local communities, in times of crisis or need. Ensuring that those people, particularly, and local response units are provided accurate and reliable information in times of sudden emergency is therefore extremely important. However, computer data errors and/or discrepancies – in names, addresses, site locations, contact information, phone numbers, and similar data – during an dangerous event or incident can lead to a response unit being dispatched to the wrong location, or responders and other citizens involved being totally unaware of hazardous conditions that require special attention. Waiting for out-of-area assistance to arrive, or for the initial responders to be re-routed to the correct location, could mean the loss not only of valuable minutes but also, in some situations, of human lives.

The Envirofacts website of the U.S. Environmental Protection Agency (EPA) says clearly that it "provides access to several EPA databases to provide you with information about environmental activities that may affect *air, water, and land anywhere in the United States* [emphasis added]." Those "activities" include but are not necessarily limited to "toxic chemical releases, water discharge permit compliance, hazardous waste handling processes, Superfund status, and air emission estimates." Unfortunately, numerous locational errors have been found over the past five years in the very EPA databases that are supposed to provide the helpful and precisely accurate information needed.

More specifically: Most but not all responders and planners referred to this type of data as FRS (Facility Registry Services) information. After the FRS addresses – which are based on collected or provided data – were plotted by the EPA's own people and/or other (non-government) researchers, a disturbingly large number of so-called "sites of interest" were found to be positioned in such improbable locations as the middle of intersections, on interstate highways, and even in farm fields. Among the other erroneous data found were a number of properties plotted as much as 20 to 40 miles or more away from their correct locations.

These data discrepancies were brought to the attention of U.S. Representative Todd R. Platts (R-Pa.), EPA Administrator Lisa P. Jackson, and other senior officials in the U.S. Department of Homeland Security (DHS) and its Centers for Disease Control and Prevention (CDC) as well as members of various private-sector groups. Last year, in a letter dated 7 January 2011, EPA Assistant Administrator/Chief Information Officer Malcolm Jackson concurred that the EPA data "is vital for the public, and should be as accurate as possible."

It is usually assumed, of course, that official databases such as Envirofacts are indeed "factual." The problem with that assumption is that the data stored in Envirofacts or other official databases can be only as accurate as the data that has been provided (by any number of sources) and then entered into the database. However, the locational source data for certain sites of interest are provided by a broad spectrum of state and local government agencies and organizations as well as private-sector groups and other "stakeholders" – e.g., state departments of labor and environmental departments that may have their own separate (and frequently different) filing and data requirements.

For that reason alone, it is particularly important that the information being provided by government systems – and shared not only with emergency services agencies but also with the general public – be as accurate as possible; that goal may best be achieved through incorporation into the current system of a rigorous validation process. However, verifying and updating such an extremely large volume of vital data also requires much more, and more effective, public-private collaboration – on a continuing basis – in order to fully and effectively address the obvious deficiencies within the current system.

Millions of Records – Each and Every One of Them "Unique"

According to the EPA's own website, the FRS now has available "over 2.8 million unique facility records linking over 3.0 million program interests, including data from over 25 national environmental data systems and over 45 state systems." However, after numerous examples of locational errors had been brought to the attention of both the EPA and state government officials, it was obvious that at least some of the data available is *not* as accurate as it should be for operational purposes, so a data-scrubbing process was started in south-central Pennsylvania to ensure that the locational data for any "site of interest" in that area would be both accurate and complete.

Obviously, knowing how to check the data and how to report an error to the EPA can help reduce delays during future emergency-response efforts. When creating a risk management plan

(RMP), therefore, it is just as obviously important to check the vital information already available for local facilities to ensure that such data is both accurate and up-to-date. In addition to the dangers that can affect the general public, there are also many cases where exposure to a substance may affect only a select group of citizens who may not be recognized by other organizations, or individual citizens, because it may fall outside their respective "domains" of control. For example, persons with "special needs" – or suffering from hypersensitivity or from allergic concerns to certain chemicals – may need additional assistance if those same persons are living or working near one of the facilities listed as having created an RMP.

Some local governments maintain lists of special needs residents – e.g., ECRIN is used in York County, Pa., to "Evacuate County Residents In Need." Other persons, afflicted with an even higher level of sensitivity, might already be on a state's "Hypersensitivity Registry" list. Having those lists available can help the response efforts considerably in sudden times of crisis.

DV, OTIS, OSWER & VZIS

The first step needed to correct current government data is to acquire basic knowledge about Data Verification (DV) procedures. A government employee sitting at his or her desk at EPA Headquarters in Washington, D.C., cannot, at present, accurately determine whether a site's locational data is correct – because that information usually can be verified only at the local level by persons familiar with the site's correct location. To rectify the errors discovered when incorrect (and/or incomplete) data is reviewed (and/or verified), the federal government has established a process, managed by the EPA, to report an error by using the EPA's Integrated Error Correction Process and Online Tracking Information System (OTIS). Among the principal users of such data are the EPA's Office of Solid Waste and Emergency Response (OSWER) and other agencies and departments, "Environmental Justice" organizations, and the general public.

Another tool offered through the EPA website by the Office of Emergency Management is the Vulnerable Zone Indicator System (VZIS), which provides a quick way to determine if a particular location might be affected by a chemical accident and/or is in the "vulnerable zone" of a facility submitting an RMP. The 1986 Emergency Planning and Community Right-to-Know Act, and certain chemical-accident "prevention provisions" in the 1990 Clean Air Act Amendment, help ensure that certain information on possible hazardous chemicals stored/warehoused at various businesses and/or other local facilities is publicly available from state and local governments.

True community preparedness requires the earnest and continuing efforts of all persons who live and work within the boundaries of that same community. When information related to various sites of interest in the community is in error – e.g., plotted in the wrong location, perhaps, and/or with incomplete or incorrect contact information, including phone numbers and addresses, etc. – the EPA's reporting process can help significantly not only in reducing the reporting times required for individual citizens but also increasing the processing time available – and needed by the EPA to correct any errors that have been discovered.

One example: After verifying the large number of locational errors in south-central Pennsylvania that had been researched, officials of York County became committed to scrubbing the EPA data for their jurisdiction, as already listed – in alphabetical order. By learning more about the process and the accuracy of federal databases, other local governments, agencies, and individual citizens can determine if the data about their own facilities and sites of interest also should be thoroughly scrubbed. Restoring trust in data systems that are used in times of crisis or unusual need must be a whole-community effort if total community protection is the goal that must be attained.

For additional information on:
To verify and correct information for sites of interest in FRS, use the following procedure: (a) visit the EPA – Envirofacts – Multisystem Query site http://www.epa.gov/envirofw/html/multisystem_query_java_bk.html; (b) in the "Geography Search" area, enter a local-area Zip Code number; (c) click "View Facility Information" next to the known facility name and address; (d) if the mapped location of the facility is incorrect, click the "Report an Error" button in the top right corner of page; and (e) follow the instructions provided by the EPA.

Vulnerable Zone Indicator System (VZIS) visit:
http://www.epa.gov/OEM/content/vzis.htm

"EPA Errors on Environmental Hazards Map Send York County Man – And Government – On a Quest" visit:
http://www.ydr.com/ci_19121036

EPA's Flowchart to describe the Error Correction Process, visit: http://www.epa.gov/enviro/html/error/flow_chart.htm.

Michael J. Jacoby is a resident of York County, Pennsylvania, who has been actively concerned for some time about various environmental protection and safety issues. York County is a major community in EPA Region III, and is represented in Congress by U.S. Representative Todd Platts (R-Pa).

"Scrubbing Source Data": The EPA Response

By The EPA Office of Information, Viewpoint

Thank you for the opportunity to comment on the article being prepared for publication in the *DomPrep Journal* by Mr. Jacoby. That article, "Scrubbing Source Data at the Local Level," raises a number of crucial points about the data quality in EPA databases and the vital need for high-quality data for emergency responses and other issues affecting human health and safety. In emergency response situations, minutes count and, when responders are dispatched to incorrect locations with insufficient information about potential environmental hazards, it increases both response time and the potential for loss of life and property.

EPA's Facility Registry Service (FRS) provides a comprehensive database of locations of interest for environmental issues, including some facilities that may pose a risk to life and/or property in certain disaster situations. The FRS is not, however, a primary data collection system. It is, instead, a data aggregator and, as such, integrates the data received from a variety of sources, including information reported by industry, as well as information reported and/or collected by state and federal governments. FRS provides a master record for a place of interest, under which are attached the individual source records – which contain the data reported from other sources. The source records are typically from a system of record and for legal purposes must remain unchanged – data contained in these source records is aggregated upward to compile a record that is then stored in the FRS file, which attempts to draw from the best available information contained within the source records.

The service also attempts to improve data quality of the master records in FRS through algorithmic validation and processing – for example, by checking on valid street address/city/state/ZIP code combinations; by comparing latitude/longitude values to given locations; and in various other ways. The validity of information is, however, not always the same as data accuracy. For example, the address that may have been provided might be valid, but may be accurate for the corporate office, as opposed to the actual facility location. Additionally, there are many other data challenges, such as incomplete addresses or P.O. Box locations, which by themselves cannot be used to derive a latitude/longitude value.

The FRS team also performs some data curation whereby incomplete, invalid, and/or unresolvable or ambiguous locations are researched and the master record for such data is corrected. However, in many instances the FRS stewards do not possess the adequate local knowledge needed to make fully and properly informed decisions about certain locations. Additionally, the sheer volume of records possessed by the FRS provides a significant stewardship challenge in and of itself.

In terms of technical approaches, a more ideal data stewardship paradigm would shift data validation and correction closer to its source – for instance, by providing instant feedback if invalid, incomplete, or ambiguous data is entered and/or, for example, by providing an aerial photograph for visual confirmation of the geographic location entered. This process would increase the likelihood of corrections being made by those reporting or entering data.

EPA is, in fact, beginning to pursue this process with some data collection systems within its purview. In addition, it is recognized that the greater engagement of local officials such as emergency response personnel, and others who are more intimately familiar with their own communities, could also improve data quality. As Mr. Jacoby notes, many corrections have in fact been provided by GIS staff in local governments in south central Pennsylvania. Ultimately, though, it also may become necessary to consider stronger mandates and to more actively promote "best practices" and more useful guidelines for the collection of high-quality locational data, as part of the basic facility lifecycle.

In closing, we broadly agree with Mr. Jacoby's assessment of the data-quality issues and the points that he raises. EPA's own FRS team: (a) is currently working with several EPA program offices to expand its front-end facility data "lookup and validation" processes as data is collected; (b) is working with state agencies to improving facility data flows; and (c) has recently established an FRS workgroup with monthly teleconferences, broadcast through the Exchange Network – these have typically been attended by 20 to 30 participants from state agencies as well as EPA program offices and regions.

In these ways, and others, the FRS team is seeking both to expand its current network of stewards and to enhance overall capabilities for facility data reconciliation and stewardship. These efforts are expected to improve tools for identifying invalid, duplicative, or incomplete data, facilitate the prioritization of data correction efforts, and help in various other ways to close the loop in terms of reconciliation of data in FRS vs. source systems. We are also evaluating ways to provide FRS information back to source systems, such as facilities researched and updated by stewards, or identified as incomplete, invalid, or indicating other possible problems that can be corrected in the source systems as well.

"Route PM": Building a Better Evacuation Plan

By Geoff Brown, Emergency Management

A new geographic information system-based software tool, developed under the direction of the Department of Homeland Security (DHS), gives emergency managers an unprecedented ability both to customize evacuation plans for the future and to create new plans as circumstances change. Beginning with a concept in early 2009, the Real Time Evacuation Planning Model (RtePM, pronounced "Route PM") was recently created by the Johns Hopkins University Applied Physics Laboratory (APL).

Richard Waddell, RtePM's Program Manager of the Homeland Protection Business Area in APL's Asymmetric Operations Department, discussed the start of the project as follows: "We were tasked and funded by DHS's Science and Technology [S&T] Directorate – the Program Manager is Herb Engle – to find out what the emergency management community in the southeastern United States needed in terms of technology … to help them plan for hurricane response."

During a conference call between APL and a State Emergency Manager Focus Group comprising representatives from 11 states, five primary needs were identified for evacuation planners. The number one need, they all agreed, sounded simple: "Give us a way to draw a polygon on a map, push a button, and get an evacuation clearance time for that area."

Although state emergency planners already knew several ways to generate the information needed, in many cases those "ways" were based on census and infrastructure data anywhere from five to ten years old. Information that is not current, though, is not useful, either, because most states, particularly those in the Southeastern area of the country, have experienced major population and infrastructure changes during the past decade. There was no way, therefore, said APL's Russell Strickland (APL's Project Lead for RtePM, and former Deputy Director of the Maryland Emergency Management Agency) "to change the parameters and develop a new clearance time estimate.

"Our conversation with users," he added, "also showed us the need to let them allow for seasonal populations, such as during summer beach seasons, and for single-event population increases, like racing at the Talladega Superspeedway [in Alabama]."

Three Drivers, an Engine, An Interface, and a Prototype

There are three fundamental "drivers" in the art and science of evacuation planning, Strickland also explained. "At the top end, there are the mandatory or regulation-required plans, such as for nuclear power plants, chemical releases, and dams. Next, plans for hurricanes – which may almost be considered mandatory in hurricane-prone states. Finally, there are those plans that a jurisdiction decides are particularly important for its region." Included in the latter group, he continued, are incidents such as wildland fires – " … which in the United States are the most frequent reasons for evacuations of 1,000 people or more. And there are the daily evacuations for hazardous materials releases that occur anywhere in the country and are our most frequent cause for evacuations."

Creating a tool that could prove useful for all three of these fundamental planning needs was not the original goal of the DHS request. However, as work progressed, the RtePM team realized they could create both a simulation engine and a user interface that would allow planners to handle almost any type of evacuation imaginable.

After a prototype had been developed, Strickland said, "We did initial field testing in Mobile [Alabama] and got great feedback. They really understood what we were trying to do, and they provided outstanding guidance to make sure it [the prototype] actually did those things. That's also when DHS told us, 'Listen to the people. If they want something in there, put it in there.'" Strickland said that the team has already presented interactive demonstrations of RtePM for representatives from all 50 states, and has incorporated their individual and collective feedback to further improve the program.

"We view RtePM as a critical component of the evacuation planning and crisis response toolset that DHS S&T will start to transition to local, state, and federal users over the next year," said DHS's Joseph Kielman, Chief Scientist for Disaster Management and Chief of the Visual Analytics Technologies Branch in the department's Infrastructure Protection and Disaster Management Division. "A common suite of integrated tools usable on multiple levels – that is, on a smaller scale for individual buildings, ranging to a

medium scale for large sports or entertainment venues, and ultimately to the large scale required for cities and even multi-state regions – is one of the objectives [that were established] for this work."

The Heart of the Program: How Many People & How Fast?

At the heart of RtePM is what is called a dynamic clearance time calculator, which uses two sets of data to estimate the length of time needed to evacuate/clear a specific geographic area. By combining data on roadway capacity with demographic information, and providing an easy-to-use graphical interface to set various parameters for certain aspects of human behavior, RtePM not only offers considerable flexibility but also requires little user training.

An individual user can, in fact, generate new simulations simply by drawing a line around an area, selecting from such variables as side streets and specific neighborhoods, and re-running the dynamic clearance time calculator. Additional improvements in estimating the clearance time have been achieved in the newest version of RtePM through the incorporation of daytime population data sets, thanks primarily to use of the LandScan High Resolution Global Population DataSet developed by the Department of Energy's Oak Ridge National Laboratory.

RtePM is able to run an evacuation simulation for a relatively small geographic area in the time it takes to refresh the screen; simulation of a larger – i.e., densely populated – area takes up to two hours. "We ran a large scenario for a Category 4 hurricane in the Houston/Galveston, Texas area," Waddell pointed out, "with a population of 1.6 million, and 922,000 of them evacuating, in a bit under two hours." Similarly impressive results were obtained for the Hampton Roads region of Virginia. (For the nation's largest metropolitan areas, Waddell says, the team would have to include models of public transportation and pedestrian evacuations.)

Listening to the Users – And the Biggest Challenge Ahead

Hearing and meeting the needs of numerous evacuation planning professionals – and incorporating into the program their individual and collective knowledge of regional differences, expectations, and experiences – has helped create a set of tools and options in RtePM that reflect real-life behaviors. "In speaking to hurricane planners in Florida," Strickland says, "we learned that if a hurricane is heading for Miami, many people don't head north. Instead, they head south, down to the Keys, to retrieve their boats, put them on trailers, and only then [do they] drive north. That creates much longer vehicles that move much more slowly. Sitting here in our ivory tower, we would have never thought about that possibility."

Thousands of miles away, in the West and Southwest, there is a similar behavior pattern, Strickland pointed out: "Working with the National Wildfire Coordinating Group, we learned that, during wildland fires in Western states, people will not leave without their horses, which means [they need] longer, slower vehicles. Because of this feedback, we added a toggle button to the screen that allows the user to adjust for greater-than-normal vehicle length, which changes the algorithm's calculation of evacuation times."

"We also learned that we can't always leave off small access roads in our mapping," Waddell added. "On the populated and developed coasts, we can do that, but in rural areas, all the roads are potentially critical evacuation routes, so we have to use the data available for all the roads [in any given area of the country]."

"Even North Carolina's Route 12, which is the only road that connects the Outer Banks towns, doesn't show up on mapping unless you go deep into the data," Strickland commented.

The RtePM team is still working on ways to more effectively address what is perhaps the most unpredictable variable: human behavior. "What will people's evacuation behavior be? It's our biggest challenge," Strickland said. "There is no absolute." Human behavior is, of course, an important issue that has always affected the nation's emergency planning community – but has only recently led to serious academic research. The team uses survey information from different areas of the country to develop informed judgments about different types of evacuation events (immediate and planned). "We look for the numbers of people who say they will evacuate," Strickland continued, "and when they will evacuate, to create our curves for volume and capacities."

"A lot of data needs to be collected that is not [presently] being collected," Waddell said. "But," he immediately added, "There is a good reason for that: Data collection in the middle of a disaster evacuation is understandably not a high priority." In fact, the team has designed RtePM to help solve its own problems

by, among other actions, encouraging users to help create larger and more relevant databases. "Users understand that, if they use RtePM to build an evacuation scenario, they would want to collect data to see how well it worked."

Planning for the Future – Transition Version in Three Months

Although the system is not yet fully real-time, owing in part to a dearth of real-time traffic monitoring data, RtePM is already able to generate new simulations quickly enough to be very effective in most cases, and has drawn praise from evacuation analysts and government agencies for its current capabilities. "It gives us confidence in the model," Waddell says. "DHS wants to get a planning tool into the hands of planners that they can use day-to-day," Strickland adds. "For now, that is more important than having real-time data."

Requests for RtePM information and trial use have also come from government, academic, and private agencies and facilities across the United States. RtePM is still in development for DHS, but a target delivery date of April 2012 has been set for a transition version that will be able to make the jump to a real-world tool for jurisdictions ranging in size from large metropolitan regions to rural counties.

"The idea is for this to be affordable," says Waddell. "It's all done with open source software, it's web-based, and it uses road-network data sets that local agencies can access free, thanks to the DHS initiatives. FEMA [DHS's Federal Emergency Management Agency] and the U.S. Army Corps of Engineers have worked closely with us during RtePM development and testing. Hurricane evacuation planners update their plans every five years or more based on data provided by the Corps; with our tool, they could do it monthly, and for less cost."

Geoff Brown is a science writer/public affairs officer at the Johns Hopkins University Applied Physics Laboratory (APL) in Laurel, Maryland. He provides communications support for APL projects ranging from national security programs to space exploration missions. Previously, he wrote about science and technology for a variety of publications as a freelance journalist; was executive producer for a live public radio talk show; and served as managing editor for Baltimore magazine.

Operation Tomodachi: The U.S./DoD Response to Fukushima

By Jamie Stowe, DoD

The Joint Task Force Civil Support (JTF-CS) is the U.S. Department of Defense's (DoD's) only command response organization specifically trained and dedicated to dealing with CBRN (chemical, biological, radiological, nuclear) incidents. In early March 2011, at the request of the U.S. Pacific Command, JTF-CS deployed a relatively small but highly qualified advisory team to the four-star command headquarters of U.S. Forces Japan (USFJ) at Yokota Air Base to assist with Japan's response to the earthquake/tsunami and subsequent Fukushima radiation leaks.

The eight-member team of what was called Operation Tomodachi (Japanese for "friend") comprised a specialty mix of U.S. Army, Air Force, Marine Corps, and civilian personnel, and served as the core of DoD's analysis and planning cell for radiation-related information, guidance, and advice. The team members monitored and reported on U.S. and Japanese radiation readings in the Japanese theater, and answered numerous questions from the field as well as headquarter commanders and other senior Japanese and U.S. officials.

The team also provided USFJ and Japanese Self-Defense Force leaders not only with threat assessments but also a number of protection and planning recommendations. In effect, the team served as a fusion center to provide U.S. and Japanese political and military leaders with the information needed – spelled out in layman's terms – to make correct and effective decisions during what turned out to be an extremely long period of crisis.

Among the specific problem areas, dangerous situations, and various related topics the team addressed were the following: radioactive water leaking into the ocean; false alarms on radiation levels; the need to ensure the safety of drinking water and food supplies; personal protective gear requirements; exposure limits and tracking mechanisms; several mitigation issues – e.g., minimizing the spread of contamination; the varying levels of decontamination required for personnel, vehicles, helicopters, and even ships; the use of potassium iodide, and the determination of who should receive it, when it should be administered, in what dosage amounts – and for how long.

A "Small Role" – Measured by the Ton

The team also played what was later described as "a small role" in development of the U.S. Department of Energy (DoE) radiation detection plan by: (a) prioritizing the areas to be monitored; and (b) crafting a notification process for radiation readings. Among the team's specific activities in this important operational area were the following:

- Providing initial USFJ dosimeter training and risk assessments for field operators;
- Advising on force health-protection measures (potassium iodide, sheltering, dosimeters, exposure limits);
- Providing operational health-risk assessments and protection support for more than one thousand personnel working in and around the "warm zone" and well over 90,000 U.S. troops and civilian personnel on Japan's main island (Honshu);
- Assisting with the planning of air and water testing locations and priorities, equipping personnel with radiation detection devices, and tracking exposure rates;
- Serving on several working groups – including teams that: created a joint U.S.-Japan radiation detection and protection plan; set the exposure-limits criteria for isotopes in the air, food, water, and soil; and established health hazard "triggers" to activate a worst-case scenario evacuation plan for more than 50,000 civilians; and
- Not only creating and disseminating radiation-education and risk-comparison criteria but also crafting a number of public affairs releases to ease certain anxieties of U.S. troops and many of the civilian personnel in the area.

Different Standards But a Common Goal – The Lessons Learned

The United States and Japan started the Tomodachi program with different decontamination and exposure standards, but U.S. representatives attempted to "align" with the host nation to the greatest extent possible. Certain aspects of international differences required that political considerations be factored into decisions – if only to prevent the misconception that the U.S. forces might have been caring more for their own people in the area (by, for example, setting more stringent standards for the safety of those citizens). In addition to supporting U.S. interests, therefore, the team provided a huge amount of specialized assistance to their Japanese counterparts as well.

The DoD's JTF-CS deployed a team in 2011 to assist Japan's response to the devastating earthquake/tsunami and radiation leaks at Fukushima. Operation Tomodachi sets an example for overcoming international differences and disseminating information for future radiological events.

Risk communications and education are imperative in a situation like Operation Tomodachi. Factual guidance (or the lack thereof) about likely or potential health hazards therefore should be disseminated quickly to all operational personnel, family members, everyday citizens, and the print and broadcast media. Otherwise, misinformation and fear can significantly degrade the operational capabilities of responders. In the Fukushima crisis, several opportunities to properly shape exposure fears were lost or ignored in the early stages of response. Many of the fears about radiation, for example, were not scientifically accurate, but nevertheless slowed operations, alarmed the public, and may have affected certain policy decisions as well.

Many phases of the operation did not go perfectly, of course – there were some initial delays in the sampling of analysis results, for example. Nonetheless, the combined U.S. and Japanese collaboration and dedication allowed the U.S. forces assigned to overcome numerous obstacles and make the overall operation much more successful than might otherwise have been possible. By pooling ideas, resources, and efforts – with, among other agencies and organizations, the U.S. Department of Energy, the Air Force's own Radiation Assessment Team, the U.S. Armed Forces Radiobiology Research Institute, and the U.S. Defense Threat Reduction Agency – the Tomodachi team members came up with several innovative ways to meet the major and continuing challenges they faced. The team also received significant around-the-clock "reachback" support from DoD and DoE nuclear experts, and from the U.S. Environmental Protection Agency.

Operation Tomodachi may well prove to be a watershed event not only for the United States and Japan, but also for their friends and allies throughout the world. The DoE and DoD personnel on the scene gained invaluable hands-on experience and developed new – and now "combat-tested" – tools and methods that can be added to the theoretical and scientific data collected. Although different in both nature and outcome, the Level-7 radiation event (highest rating on the International Nuclear and Radiological Event Scale) at Fukushima might reasonably be considered, therefore, to be the current generation's "Chernobyl."

To briefly summarize: Although no two events or incidents are identical in every aspect, many lessons can still be learned, to prepare more effectively for the next incident, not only by examining what worked during previous incidents, but also – and of perhaps greater importance, what did not work. Many of the lessons learned from Fukushima, and from Operation Tomodachi, will undoubtedly be applicable to the next major radiological event, whether that event is another Fukushima-level natural disaster or a terrorist attack.

Major Jamie Stowe, USAF, is a Medical Plans and Operations Officer at Joint Task Force Civil Support, a U.S. Northern Command unit that prepares for and responds to large-scale emergencies. He has 13 years of experience in emergency planning and response operations with the U.S. Air Force and the U.S. Army. He completed a Department of Defense medical readiness fellowship and has functional expertise in CBRN scenario planning and mass casualty treatment. He holds a Master's degree in Business Administration and is pursuing a Master's degree in National Security and Strategic Studies from the U.S. Naval War College.

The InfraGard Alliance: Personal Relations & Information Sharing

By Sheri Donahue, Law Enforcement

The terrorist attacks of 9/11 in 2001 demonstrated the need for information to be shared between organizations and agencies, in numerous disciplines, not only at all levels of government but also, and of perhaps greater importance, in the private sector as well. However, although it was and is easy to recognize that need, it was not quite as easy to implement the actions needed to achieve the informational goals implied. Terms such as "information sharing," for example, can be overused, making the precise meaning of that term somewhat vague.

From the creation of the U.S. Department of Homeland Security, which now has over 240,000 employees, to the development and implementation of cross-sector policies such as the National Infrastructure Protection Plan (NIPP), many efforts have been made not only to formalize information sharing but to mandate it. The now national awareness and use of such key words as partnership, coordination, integration, and alliance demonstrate how prolific such efforts have become.

Today, the homeland security posture of the United States continues to improve and in the past decade has become significantly stronger – thanks in large part to new technology, awareness campaigns, drills and exercises, etc. However, all of the state-of-the-art tools, organizations, marketing, and policies now in place are and would be of little use without one critical success factor: human relationships.

InfraGard, SMEs & Citizen Volunteers

Founded in the Cleveland, Ohio, field office of the Federal Bureau of Investigation (FBI) in 1996, as a collaborative effort with private-sector cyber professionals, InfraGard was later expanded by the FBI to every field office in the country to provide agencies, at all levels of government, with unmatched access to the expertise and experience of critical infrastructure owners and their key operating professionals. In 2003, the private-sector members of InfraGard formed the "InfraGard National Members Alliance" (INMA), which provides its members unmatched opportunities to promote the physical and cyber security of their organizations through access to a trusted national network of "Subject Matter Experts" (SMEs) – those public and private sector individuals working in the environment every day who possess an abundance of knowledge on any of a broad spectrum of topics.

As is true in many other organizations, InfraGard lists "information sharing" as its principal but not only purpose. With 84 InfraGard chapters in the United States and Puerto Rico and well over 47,000 members (as of 21 January), the national InfraGard program has already proved, many times over, its ability to quickly and comprehensively carry out its stated mission – namely, "to provide a trusted forum for the exchange of knowledge, experience, and information related to the protection of our nation's critical infrastructure from both physical and cyber threats." The organization's official motto, not incidentally, is "Partnership for Protection."

InfraGard, like many other organizations, has implemented programs and information technology (IT) systems and venues – such as meetings, the formation of special interest groups (SIGs), secure portals, listservs, websites, and secure mailing lists – to enhance what has become a highly respected and extremely trusted forum – and national asset. However, the true value of these tools lies not in the tools themselves but in the quality of information they deliver.

To become a member of InfraGard, an individual citizen must submit an application to the FBI for a records check. InfraGard itself, however, does not grant members security clearances, nor does it require clearance for open and trusted communications in, on, or about U.S. homeland security. In that respect, the organization's trusting attitude on such matters emphasizes the fact that the best information is not necessarily, or always, "Top Secret." What is often the most important piece of the puzzle, in fact – context – comes from the subject matter experts (SMEs). An intelligence analyst therefore may have access to state-of-the-art IT systems and the most highly classified data available, but without understanding such information in the proper context these systems and mountains of classified information may be all but useless.

Something of Value: The Official Reports

Gaining timely access to the knowledgeable volunteers in the organization and the context they can provide is one of the primary values provided by InfraGard. Numerous FBI reports confirm that there have been impressively higher numbers of cases initiated, cases enhanced, and intelligence products developed as a result of the InfraGard program and the trusted relationships that have been formed between FBI agents and

InfraGard members. The importance of these success stories lies in the fact that although most FBI agents have impressive academic and/or professional backgrounds – usually but not always in such fields as accounting, business, law, or engineering – very few if any of them can possibly possess *all* of the sometimes esoteric background knowledge needed to fully understand the intricacies of each and every case they investigate.

For example, an agent in the white-collar crime unit may be working on a case involving the commodities market. However, because he or she has only limited experience in that field, he/she contacts the local InfraGard coordinator in their field office (who is also an agent) to locate members with special expertise in securities and trading. The coordinator introduces the FBI agent to an appropriate SME, who is able and willing to share his/her knowledge of the commodities market.

The same agent could, of course, use internet searches and other knowledge-based systems to research the topic, but the InfraGard process enables the two principals to discuss specifics of the case, and the commodities market itself, more quickly, in greater detail, and with much greater confidence. (Here it should be noted that the SME does not necessarily know what the case is, or who it involves, but simply provides his or her specialized knowledge requested by the individual FBI agent.)

For practical purposes, what this means, among other things, is that the case has now progressed – usually faster and with a more accurate focus – without the agent having to make inquiries that might in at least some cases jeopardize the investigation. This scenario, and numerous other success stories (many of which cannot be made public because of the sensitivity of the subjects involved), highlight the importance of the personal, and trusted, relationships between FBI agents and InfraGard SMEs that have been and continue to be developed.

Although InfraGard is an FBI program, memoranda of understanding (MOU) between the private-sector side of InfraGard (the InfraGard National Members Alliance, or INMA) and other government agencies can be equally beneficial for everyone and all agencies involved. For example, an MOU with the Department of Homeland Security (DHS) propagated such efforts as regional conferences on sector-specific issues. Another beneficial effort has been the introduction of the 93 DHS protective security advisors (PSAs) to their local InfraGard chapters.

Today, the PSAs – which are now deployed throughout the United States (and Puerto Rico) to gain additional insights into the risks to critical infrastructures at the regional, state, and local levels – provide local perspectives, which are then incorporated into the development of national risk assessments to help ensure more accurate protection, mitigation, and response efforts. DHS provides its PSAs, who almost always become InfraGard members themselves, with information on the local InfraGard chapters in the geographic areas for which they are responsible. Not only are PSAs helped significantly, therefore, in carrying out their own responsibilities, the InfraGard members also benefit from the expertise of the PSAs and ensure that their concerns are addressed and communicated to those in DHS who develop the nation's risk assessments and protection plans.

The second value proposition then is the benefit that the InfraGard members and their organizations gain from these interactions. Physical and cyber security efforts are enhanced not only through the interactions these members have with the FBI and DHS, they are also improved through similar interactions with other SMEs both locally and nationally. Local members have access to individuals in other critical infrastructures whose proximity and environmental experiences also are shared. For example, members of the banking and finance sector may share information about a recent string of robberies at their branch ATMs. While at an InfraGard meeting, or through local information-sharing portals, members from the local transit authority share similar experiences occurring at their ticket stations. Comparisons of the information that each member of the InfraGard team possesses often leads directly (and quickly) to the law enforcement agencies for each of the shareholder entities involved in closing the case.

In addition to local sharing, members have the opportunity to interact nationally with SMEs within their own sectors through Special Interest Groups (SIGs). The SIGs are groups of InfraGard members subdivided by specialty in order to discuss and share ideas and information about their sector. These efforts are carried out primarily via a secure portal maintained by the FBI for InfraGard use. Current SIGs focus on such major national priorities and infrastructure resources as chemicals, food/agriculture, research & technology, and electromagnetic pulse (EMP).

Volunteerism: A Critical Infrastructure

Individuals, rather than organizations, are InfraGard members. These individuals are in some way affiliated with a particular sector of the critical infrastructure within their communities. Therefore, participation in the InfraGard program may benefit the individual's organization through knowledge the member gains via his or her membership. However, the individual member, as well as officers and directors, participates voluntarily and often sacrifices much of his or her personal time to do so.

In fact, a credible case could perhaps be made that "Volunteerism" should be regarded as the 19th critical infrastructure sector (in addition to the 18 sectors previously defined by the U.S. Department of Homeland Security). In fact, the USA Patriot Act of 2001 has already defined "critical infrastructure" as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The InfraGard National Members Alliance similarly believes that volunteerism is also an "asset[s] ... so vital to the United States that the incapacity or destruction ... would have a debilitating impact."

Whether the term "volunteer" is taken to mean offering services without expectation of compensation or freely providing information without first being asked, it is or should be obvious to all Americans that volunteerism is critical to securing the health and safety of the nation. Without volunteers, in fact, the technologies, policies, IT systems, and operational structures of the entire nation simply could not function at their full potential. It is the individual citizen, therefore – and his or her willingness to serve and share – that makes these other assets and resources, both tangible and intangible, so successful.

For more information on:
INMA's 19 April 2012 conference on volunteerism, visit www.infragardmembers.org

InfraGard, visit www.infragard.net

Sheri Donahue is the Program Manager for Security and Intelligence at the Indian Head Division of the Naval Surface Warfare Center. She previously served as: Director of Customer Support for DisastersNet, Inc.; Managing Director of the InfraGard National Members Alliance (INMA); and as Executive Director and President of the Cyber Conflict Studies Association (CCSA) at the Norwich University Applied Research Institutes (NUARI). She also served, for 16 years, as an Engineer and Special Programs Manager for the Department of the Navy – and has been an active member of InfraGard since 2003 and a member of the InfraGard National Board of Directors since 2004.

Surviving the End of the World

By Joseph Cahill, EMS

A firefighter is making a careful but nonetheless dangerous room-by-room search of a burning building when the roof suddenly collapses. A police officer is shot while carrying out a supposedly "routine" traffic stop. A paramedic is struck by a passing car at the scene of an auto accident.

In addition to the personal and emotional effects that these and similar tragedies have on the responders involved, and their families, such incidents also pose difficult planning and operational challenges for the responder agencies of each of these front-line professionals.

The death or severe injury of an agency member is one of the most difficult situations for other members, and agency leaders, to face. Although the many steps required to protect on-the-scene responders may be weighty in effort, political capital, and expense, providing a safe work environment is and should be the first and most important responsibility of any senior leader – in any agency of government, or in the private sector.

The agency involved almost always has numerous (and often competing) priorities and responsibilities to take into consideration. Nonetheless, the central and most obvious factor in meeting the all-important goal of providing and continuously improving workplace safety for staff is understanding events such as those listed above and the conditions that led up to each such incident. Fortunately, there is a relatively simple but not always easy two-step process that managers should follow. The first step is to immediately (if possible) carry out an initial analysis of what happened prior to the occurrence of such tragic events; the goal, of course, is to take whatever actions are needed to avoid similar injuries or deaths in the future. The second step is to carry out an in-depth and totally objective review of the specific incident being investigated.

Statutory Investigations And Agency Involvements

Law enforcement agencies and/or the medical examiner's or coroner's office will probably have the principal

responsibility of carrying out the formal investigation of a death; but that responsibility might sometimes be assigned to the National Transportation Safety Board (in the case of aircraft and/or some, but probably not all, traffic-related events). Other agencies, depending on the circumstances involved, may also have a statutory responsibility to investigate. In addition, certain events (terrorist attacks, for example, or attempted assassinations) may require a separate investigation by local, state, or even federal agencies and/or specially appointed commissions.

Although it is important that the agency directly involved review such incidents, it is at least equally important that such review not obstruct any statutory investigations required, if only because the agencies assigned responsibility for a statutory review usually possess (or should possess) the authority, resources, and experience required to carry out the primary investigation. In addition, once the statutory review is completed, the reports generated by these primary investigations can be a rich source of information to other agencies carrying out their own reviews and investigations.

When tragic events take the life of a responder, the family, colleagues, and supervisors all feel the devastating effects and face numerous challenges. Although risk cannot be eliminated, careful agency reviews can create a safer work environment to help prevent similar tragedies.

The purpose of an agency review differs from other investigations in that the primary goal of the agency review is to identify opportunities for systemic and/or policy improvement. In a case where the risk was previously recognized and planned for, and the safety plans were in fact adhered to, an analysis of the event still must be made to determine why those plans did not work to ensure the safety of the deceased or injured member of the agency. Some circumstances, of course, may justify deviations from so-called standard operating procedures; in that case, the existing plans should be modified to encompass such non-SOP possibilities.

If it turns out that the threat was a previously unrecognized risk, the results of the investigation should lead to the development and implementation of new plans – and/or, if necessary, even some equipment or policy changes – to reduce the risk of similar deadly results from future incidents. An agency review may also identify other issues that should be addressed – more effective and/or more frequent training drills for members, to cite one obvious example. It also should be remembered, and taken into consideration, for example, that a member cannot conform to a plan if he or she is unaware of its existence. Likewise, additional training would likely be needed if a new or modified plan is generated by the investigative process.

Human nature being what it is, there is often an understandable temptation to use an investigation to determine the possible culpability of a team member, or anyone with supervisory responsibility, for what has happened. Obviously, the question of who is or may be "at fault" *should* be determined, if possible, but a continuing and primary focus on that question also can become a barrier to frank and honest discussion of all aspects of the incident and can be counterproductive to achieving what should be the agency's primary goal: improving the process and, by doing so, upgrading overall safety in general.

The unspoken truth about many tragic events such as those mentioned above is that carrying out an emergency response is an inherently risky proposition. Those who plan for response operations are not in the business of eliminating all risks – an obviously impossible task – but, rather, controlling or mitigating the risk to the maximum extent possible. In order to do that, planners must: (a) fully understand all of the risks involved; (b) identify and implement the short- and long-term plans needed to mitigate those risks – again, to the maximum extent possible; and (c) stay focused on what should be, at all times, their highest priority – namely, creating a safer work environment for the front-line responders who routinely face the possibility of death or serious injury.

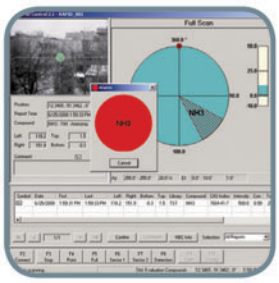
Joseph Cahill, a medicolegal investigator for the Massachusetts Office of the Chief Medical Examiner, previously served as exercise and training coordinator for the Massachusetts Department of Public Health, and prior to that was an emergency planner in the Westchester County (N.Y.) Office of Emergency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

Bruker Detection

RAPID

Stand-off Detector for Atmospheric Pollutants

- For the remote detection of atmospheric pollutants and chemical warfare agents
- Allows for measurements in the spectral wavelength range from 14 µm to 8 µm
- Four libraries of chemical compounds, can detect up to several kilometers line-of-sight



+1 (978) 663-3660 x 1418 • nbc-sales@bdal.com • www.bruker.com/detection

think forward

CBRNE Detection