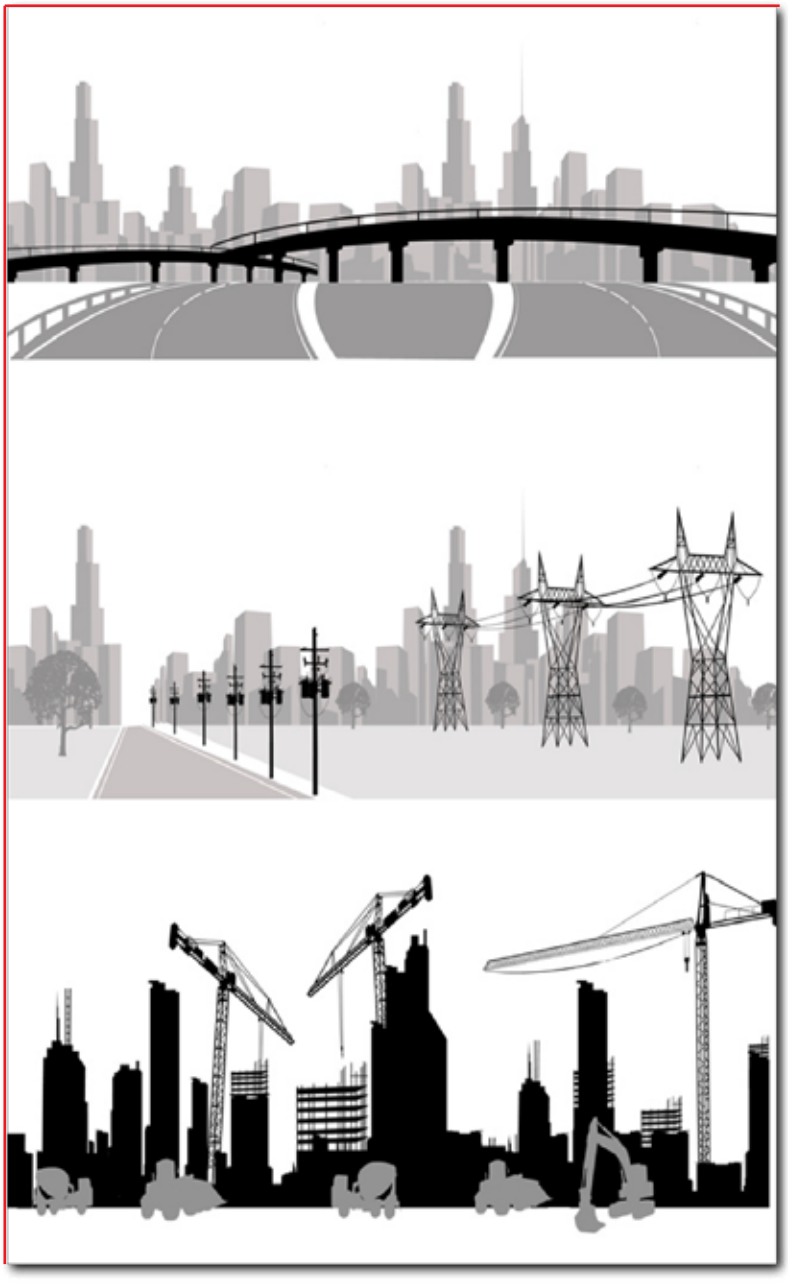
domestic preparedness .com

DomPrep Journal

Subscribe Volume 10 Issue 9, September 2014

Sustainability



POST-DETONATION...

Fallout is Coming Down.

Is YOUR Building Safe?

NukAlert™ Automated Fallout Measurement Station

The NukAlert™ Automated Fallout Measurement Station (AFS) can initiate ventilation system shutdown the minute dangerous radiation levels are detected, maintaining the building's shelter potential. Without it, the building could be rendered permanently uninhabitable by radioactive dust spread throughout the ductwork.

The AFS radiation readings can be seen live 24/7 on map displays. The station will send multiple text/email alerts to key building and response personnel whenever your preset levels are exceeded.

Both low-cost units offer extended range measurement- 1µR/hr to 700R/hr with no saturation below 1,000R/hr

NukAlert-ER™ Geiger Counter

With the companion, easy to use, NukAlert-ER™, you can quickly locate the safest areas in your building and scan people entering to take shelter.

NUKALERT™

Apogee Communications Group
159 Alpine Way/ Boulder, CO 80304/ 303.443.8473
Click Here: www.apogeecomgrp.com

GSA Advantage!®

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

Staff
Martin Masiuk
Founder & Publisher
mmasiuk@domprep.com

Susan Collins
Associate Publisher
scollins@domprep.com

James D. Hessman
Editor Emeritus
JamesD@domprep.com

Catherine Feinman
Editor
cfeinman@domprep.com

Carole Parker
Administrative Assistant
cparker@domprep.com

John Morton
Senior Strategic Advisor
jmorton@domprep.com

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

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 Manuscripts are original work, previously unpublished, and not simultaneously submitted to another publisher.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

IMR GROUP

Editor's Notes

By Catherine Feinman

Every four years, the American Society of Civil Engineers releases a critical infrastructure "Report Card," which is based on capacity, condition, funding, future need, operation and maintenance, public safety, resilience, and innovation. The average overall grade for U.S. infrastructure in 2013 increased to D+ from the 2009 grade of D, but the latest report still asserts, "The infrastructure is in poor to fair condition and mostly below standard." With critical infrastructure being "the backbone of our nation's economy, security and health," as stated on the U.S. Department of Homeland Security's website, subject matter experts address the topic of "Sustainability" of the nation's critical infrastructure in this issue of the *DomPrep Journal*.

Joe D. Manous leads this issue by addressing the overarching concepts of critical infrastructure, sustainability, and resilience. Since 9/11, many natural and manmade disasters have brought these concepts to the forefront of community preparedness, but there is still much to do. "Preparedness 101 & Beyond" presents findings from a nationwide flash poll on these concepts. A follow-on podcast of subject matter experts, led by Manous, provides a more in-depth review of the survey results, the development of career fields, and the bodies of knowledge.

Then, Kay C. Goss shares a chronological account of legislative efforts in critical infrastructure protection leading up to the new National Protection Framework, which the Federal Emergency Management Agency released on 30 July 2014. In addition to participating in this month's podcast, Marko Bourne discusses the need to eliminate operational and program silos and work with nontraditional community groups.

Wayne P. Bergeron and Charles Manto address threats to schools and lifeline infrastructure, respectively. One thing that active shooters and solar storms have in common is that they both can shut down critical infrastructure and have far-reaching effects in other jurisdictions. Even before an incident occurs, though, effective leaders – who are well aware of their roles, responsibilities, and consequences of their actions – must be in place, as discussed by Samuel Johnson Jr.

In addition, there is a growing need to ask and find answers to questions about assets that could have devastating ripple effects should they cease to function. Specifically, Joseph Cahill applies the Kipling Method to infrastructure protection and Aaron Sean Poynton goes in to detail about the law enforcement assets that Ferguson, Missouri, police officers received from the Department of Defense.

Richard Schoeberl rounds out the issue with a timely warning about citizens in Western nations travelling abroad. Practicing situational awareness and taking adequate precautions, both at home and abroad, can help reduce potential risks.

About the Cover: Critical infrastructure includes bridges, energy, roads, transit, hazardous waste, and other assets, systems, and networks, which must be sustained to promote the security, health, and/or safety of those who live, work, or travel within and around these communities.

Not If, But When?

Prepare Now

For Chemical & Biohazard Emergencies

AP4C

Handheld Chemical Detector

- Unlimited, Simultaneous Detection
- Continuous Detection for Fix Locations
- Low Maintenance and Operation Cost
- Compact Design for Tight Locations

PROENGIN

Chemical and Biological Detection System

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

Critical Infrastructure – Preparing for the "Long Haul"

By Joe D. Manous Jr., Viewpoint

Critical infrastructure, sustainability, and resilience have become key terms within the infrastructure design, emergency response, and governance communities over the past decade. Discussions on these topics began much earlier than 2001, but the 9/11 terrorist attacks on the United States certainly galvanized the discussion and, more importantly, provided funding for practitioners and academics to explore novel ideas and methods. The consequences of hurricanes Katrina and Rita in 2005 further shaped these discussions, which increased the focus on infrastructure.

Until those incidents, intelligence and law enforcement seemed to have a dominant role in national and regional discussions because of the 9/11 attacks. However, since the 2005 hurricanes, subsequent events such as the 2013 Boston marathon bombing and natural disasters – including the 2011 tornadoes in Joplin, Missouri, and Superstorm Sandy in 2012 – have broadened discussions on preparedness and response, while serving as test cases for the concepts and initiatives developed through multiple, broad-based, and parallel activities.

Testing & Exercising New Ideas

While additional "events" have served as laboratories to test novel ideas, academia also has responded by creating new courses and fields of study in the areas of critical infrastructure, emergency response, and resilience. The titles and topics for these courses and programs vary, including but not limited to: infrastructure protection, homeland security, infrastructure engineering, and critical infrastructure systems. Although these efforts are important and moving forward, they are still in their infancy.

An interesting exercise is to compare the new direction in infrastructure programs with the evolution of environmental science programs that emerged in the 1980s following passage of environmental legislation a decade earlier. For accreditation purposes, it is helpful to "benchmark" academic programs with programs from similar universities. When conducting such comparisons of environmental science programs during the early 2000s, the benchmarking process was found to be exceedingly difficult.

Those comparisons showed that even though the environmental science field had matured – as measured by a steady demand for graduates and the availability of course materials such as textbooks – there was no consensus or focus on subject material or agreement on "typical skills" for undergraduates. Environmental science programs seemed to reflect university-specific interests, which include microbiology, biology, ecology, geography, water resources, resource management, and legal subjects. As a result, it proved difficult to generally describe the interests or capabilities of a graduate or practitioner in the environmental science field, though many had demanding and rigorous curriculums. Although a lack of consistency proved inconvenient for an administrator preparing for accreditation, opportunities for college graduates from environmental science programs continued even though they were hired based on individual skills and work experiences rather than by academic degree or association with the environmental science field.

Developing Program Consistency

As programs of study that cross many disciplines, environmental science programs are producing graduates with skills that reflect institutional strengths and regional needs. In comparison, the civil engineering field has established a base level of subject matter understanding, which is combined with opportunities for additional focus based on student interest. At the undergraduate level, such focus typically includes additional courses in a focus area – such as transportation, structures, geotechnical, environment, and others – which builds on required, base-level study in these areas. For civil engineering, this process has led to the development of a "body of knowledge," which through 11 topic areas provides direction and a measure of consistency for the education of people entering the field and the continuing education of those working in this profession. In fact, civil and other engineering fields now have their own accreditation body, Accreditation Board for Engineering and Technology (ABET), which provides standards and assessment processes recognized by most university accreditation programs and state licensure boards.

Practitioners heavily influence the content of these standards. Similar accreditation bodies exist for chemistry, biology, law, medicine, dentistry, and other fields. A result of such standardization is a general recognition of these professions or career fields by both specialists and the public along with the creation of career progression pathways. Such establishment of work disciplines has the benefits of: providing a foundation for long-term research; developing methods, standards, and codes for practitioners; and consistently educating and training entry-level through experienced practitioners.

This discussion highlights the diversity of approaches that already exist within education, training, and career development in science, technology, engineering, and mathematics (STEM) fields. As critical infrastructure, sustainability, and resilience fields continue to develop innovative ideas and standard methodologies, academic institutions create programs of study, and practitioners develop their areas of expertise, many questions emerge. For example, "Should these 'areas' follow (a) the environmental science model that has significant diversity in academic content and practitioner identity, (b) follow a "body of knowledge" approach, or require the creation of a model to meet new fields of practice?"

Perhaps a fundamental question before addressing the structure of these new fields is whether critical infrastructure, sustainability, and resilience are fields unto themselves or, alternatively, represent fields of integration that crosscut several disciplines. In current crosscutting fields, college graduates and practitioners associate themselves with their undergraduate or primary fields of expertise. As a result, graduate study or a career working in a crosscutting field becomes a requirement for association in that area. In short, some fields of work are not entry level.

Establishing a Collective Long-Term Effort

This discussion leads to the central question, "Are the preparedness communities collectively preparing for the long-term?" Although it may be interesting to participate in discussions and read articles or policy guidance concerning new directions in critical infrastructure, sustainability, and resilience, the topics under consideration too often continue reviews of unresolved fundamental issues. Clearly, the United States has made tremendous investments and accomplished great work, but the work itself may not be "resilient" within the knowledge base of design professionals, policymakers, and financial institutions, much less the American public who must live with and be protected by the results. If the acceptance – or lack thereof – of definitions for common terms used in these fields is an indication, perhaps the knowledge base itself is fragile.

With more than 12 years since the 2001 attacks, multiple critical incidents since, and significant investments of time, energy, and funding during the interim, now is the time to evaluate directions forward in the identification of fundamental skills, responsibilities, and career paths. As observed from the environmental science example, such key elements within a field of practice do not necessarily resolve themselves. Some level of institutionalization in these areas could be significant in establishing generally accepted concepts for design, operations, and maintenance of critical infrastructure and the broad application of such approaches.

An admirable quality by many discussants on critical infrastructure, and notably by members of DomPrep, has been a "can do" attitude. Recognition of the lives and property at risk by not acting promptly to provide sustainable and resilient infrastructure is a responsible and appropriate concern. The time, however, has come to focus greater resources on long-term efforts associated with critical infrastructure. Deliberate efforts to develop a new generation of professionals working with critical infrastructure now seem equally essential with addressing immediate risks to the safety, health, and welfare of the public.

It is important to recognize that efforts in these areas have begun, but the efforts are independent and do not have consistency in direction. There is a need for national-level leadership, and without such leadership, the direction forward in developing professional workforces is not clear. Concerted efforts by practitioners, academicians, and professional organizations will be required to chart a course for the "long haul."

Joe D. Manous Jr., P.E., Ph.D., D.WRE, is the international activities manager for the Institute for Water Resources, U.S. Army Corps of Engineers and works closely with the Office of he Assistant Secretary of the Army for Civil Works. He is a civil engineer specializing in the areas of water resources and environmental security issues associated with water. Previously, he served as an academy professor at the United States Military Academy at West Point, where he taught courses in environmental engineering, water resources, and environmental security. After more than 28 years of service, he retired as a colonel in the U.S. Army. He is active in the American Society of Civil Engineers, Society of American Military Engineers, The Infrastructure Security Partnership, and the National Institute for Engineering Ethics and has worked on a variety of infrastructure, professional development, and college outreach initiatives.

Preparedness 101 & Beyond

By Catherine L. Feinman, Editorial Remarks

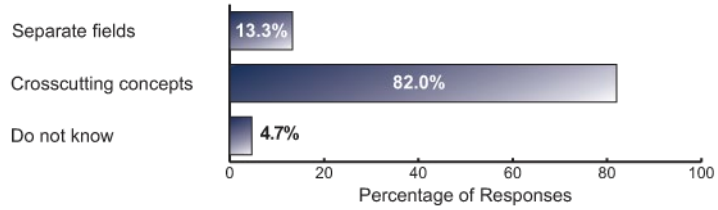
Critical infrastructure, sustainability, and resilience are terms that are commonly used by emergency planners, responders, and receivers in various disciplines and jurisdictions. However, questions surround who needs to understand and implement these concepts, how the terms are defined and used, and how the concepts contribute to resilient communities. In this month's survey, 151 DomPrep readers replied to a flash poll that addressed these topics. This article is a compilation of these responses, including one that provided the following headings.

Preparedness 101: Defining Critical Infrastructure

Most of the respondents (82.0 percent) stated that critical infrastructure, sustainability, and resilience are cross-cutting concepts that are applied to established fields of practice, rather than fields unto themselves (Figure 1). However, all of these concepts require collaborative efforts and effective plans in order to promote overall preparedness.

First, there needs to be a basic understanding of each concept, preferably with common terminology determined in a cooperative effort by government, academia, and trade associations. Lessons learned from other collaborative efforts – for example, the National Response Plan – could serve as a starting point for determining a course of action toward infrastructure protection.

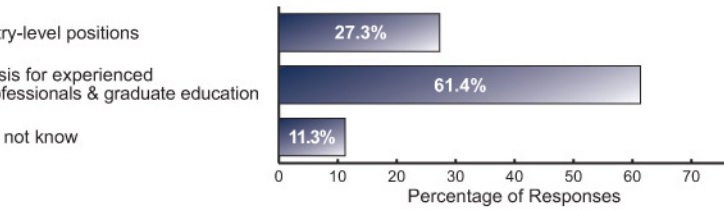
Figure 1:
Are critical infrastructure, sustainability, or resilience fields unto themselves or are they cross-cutting concepts applied to established fields of practice?



Although more than half (61.4 percent) of the respondents stated that critical infrastructure, sustainability, and resilience topics are more suited for experienced individuals and graduate education, arguments were made for these topics to be covered in the entry-level workforce as well (Figure 2). These arguments include:

- Training and education are necessary at the entry level, but the actual "work" should be performed with a combination of new and experienced workforce members.
- The entry level should at least include a simple awareness program, with more detail about how these concepts interact as employees reach higher managerial levels.
- Information shared at a more basic level – including at the high school level – should help with disseminating important concepts to the public.
- As concepts progress, change, and improve, having a solid base would make it easier to build on knowledge, history, and future changes.
- Protecting critical infrastructure, sustainability, and resilience apply to all preparedness fields and are underlying goals, so everyone should understand them.

Figure 2:
Are critical infrastructure, sustainability, or resilience topics for entry-level positions in the workforce or fields for well-experienced individuals and graduate education?



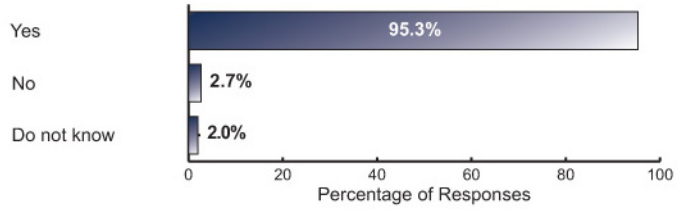
Preparedness 201: Protecting Critical Infrastructure

After laying the foundation, emergency professionals can begin to develop and implement specific plans from a generalized national "warehouse" of ideas and strategies. Most of the respondents (95.3 percent) agree that there is a need for "bodies of knowledge" – shared understanding of key terms, definitions, concepts, principles, tips, techniques, and procedures – within critical infrastructure, sustainability, and resilience topics (Figure 3).

A centralized knowledge base established by a task force of experienced professionals in various fields – civil engineers, architects, developers, emergency managers, business continuity and risk management professionals, insurance professionals, legal and environmental agency representatives, academia, as well as other specialists – would be useful because concepts are ever changing. The knowledge base could house documents and share information on: prescriptive guidance; vulnerability assessments; best practices; prevention and mitigation strategy development; response, continuity, and recovery planning; lessons learned; studies; tools; risk assessments; and other resources.

Preparedness 301: Sustainability of Actions

Figure 3:
Is there a need for "bodies of knowledge" within critical infrastructure, sustainability, or resilience topics or fields?



Analysis and critique of protection efforts help identify problems, encourage evolution, and maximize efficiency of work performed. In order to effectively sustain actions, there must be proper training, education, and experience that is passed from experienced professionals to newer employees. The independent complexities for managing and supporting each area require mature sets of skills. Therefore, in order to effectively communicate across multiple industries, a new curriculum is required to train and certify professionals for sustainment of cross-cutting employment operations.

Such training must be at least at the same level as those who are retiring. Retiring workforce members also should spend time before their departures transferring knowledge to a database and helping train replacements to ensure maximum knowledge transfer. Other ways to transfer knowledge and ensure sustainability include, but are not limited to: continuing education; reviewing lessons learned; sharing current concepts and practices; acquiring experience and life lessons; taking formal and informal training and refresher courses; mentorship programs; peer-to-peer sharing; secondary and postsecondary education programs; and tabletop exercises.

Many free training courses are available through the Federal Emergency Management Agency Independent Study. The following are just some of the courses related to critical infrastructure, sustainability, and resilience:

- IS-1 Emergency Manager: An Orientation to the Position
- IS-200.B Incident Command System for Single Resources and Initial Action Incidents
- IS-546 Continuity of Operations (COOP) Awareness
- IS-547.A Introduction to Continuity of Operations (COOP)
- IS-662 Improving Preparedness and Resilience Through Public-Private Partnerships
- IS-700.A National Incident Management System (NIMS)

- IS-800.A National Response Plan (NRP), an Introduction
- IS-860.B National Infrastructure Protection Plan (NIPP)
- IS-921.A Implementing Critical Infrastructure Security and Resilience

Preparedness 401: A Resilient Community

With the transparency and open communication, the best and most effective actions may be used for the supporting elements of a community outside the critical infrastructures. A standardized plan of action and an inventory of assets will enable quicker transfer of duties and responsibilities to new personnel.

For community resilience, teams, committees, or groups of public and private sector professionals with various talents and experience can collaborate to accomplish specific goals. The information gathered must be secured to prevent potential perpetrators from accessing information about the community's valuable scenarios, recommended actions, and other findings. One respondent suggested using protected forums such as Homeland Security Information Network and Law Enforcement Online as reservoirs of knowledge.

As one respondent wrote, "In the end, the 'mindset of preparedness' needs to be, as uniform as possible, established at all levels of society – throughout all branches of government, industry, and citizenry." It is not enough to say that critical infrastructure needs to be protected, that actions need to be sustainable, and that communities need to be more resilient. There must be clear definitions, specific plans of action, and actionable ways to become more resilient.

Catherine Feinman joined Team DomPrep in January 2010. As the editor, she works with writers and other contributors to build and create new content. With more than 25 years experience in publishing, she previously served as journal production manager for Bellwether Publishing Ltd. She also volunteers as an emergency medical technician, firefighter, secretary of the Citizen Corps Council of Anne Arundel County and City of Annapolis, and a Community Emergency Response Team (CERT) trainer.

Critical Infrastructure Protection: History, Overview & Update

By Kay C. Goss, Emergency Management

On 30 July 2014, the Federal Emergency Management Agency (FEMA) released the National Protection Framework, the last in a series of five frameworks. The National Planning Frameworks describe how the whole community works together to achieve the National Preparedness Goal (released in September 2011), which serves as the cornerstone for implementing Presidential Policy Directive 8 on national preparedness (signed by President Barack Obama on 30 March 2011). The national goal is, "A secure and resilient nation with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk."

The five frameworks, which highlight the roles and responsibilities "from the fire house to the White House," are part of the National Preparedness System, with one framework for each of the following preparedness mission areas:

- National Disaster Recovery Framework (released in September 2011);
- National Mitigation Framework (released in May 2013);
- National Prevention Framework (released in May 2013);
- National Protection Framework (released 30 July 2014); and
- National Response Framework (second edition, released in May 2013).

Placing an Emphasis On Critical Infrastructure

Critical infrastructure protection has long been a priority in the United States. However, most of this vital protection planning remained classified as a function of the federal government. After the Oklahoma City bombing and Omnibus Counterterrorism Act of 1995, many agencies and organizations became aware and engaged in the protection planning process.

In May 1998, President William Jefferson Clinton solidified and defined the new emphasis and challenge, by issuing Presidential Decision Directive 63 (PDD-63), which recognized parts of the national infrastructure as critical to the national and economic security of the United States, and required steps to be taken to protect it. The basic guidelines and general principles the president enunciated in PDD-63 to protect this infrastructure included:

- Consult with, and seek input from, congress on approaches and programs;
- Share responsibilities and partnerships between owners, operators, and the government, and encourage international cooperation;
- Make frequent assessments of critical infrastructures' existing reliability, vulnerability, and environment because, as technology and the nature of threats to critical infrastructures continue to change, protective measures and responses must be able to adapt;
- Use market incentives as the first choice for addressing the problem of critical infrastructure protection; use regulation only if there is a failure to protect the health, safety, or wellbeing of U.S. citizens and, in such cases, identify and assess available alternatives to direct regulation, which include providing economic incentives to encourage the desired behavior or information to help the private sector make decisions;
- Make available the full authorities, capabilities, and resources of the government, including law enforcement, regulation, foreign intelligence, and defense preparedness to ensure critical infrastructure protection;
- Respect privacy rights – consumers and operators must have confidence that information will be handled accurately, confidentially, and reliably;
- Encourage – through research, development, and procurement – the introduction of increasingly capable methods of infrastructure protection;
- Serve as a model to the private sector of how infrastructure assurance is best achieved and distribute results;

- Focus on preventative measures as well as threat and crisis management; encourage private sector owners and operators to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist on a voluntary basis; and
- Take into consideration the essential needs, activities, and responsibilities of state and local governments and first responders.

PDD-63 was updated on 17 December 2003 by President George W. Bush through Homeland Security Presidential Directive 7 for critical infrastructure identification, prioritization, and protection, which described that some critical infrastructure is "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." This critical infrastructure now includes 16 sectors: chemical; communications; dams; emergency services; financial services; government facilities; information technology; transportation; commercial facilities; critical manufacturing; defense industries; energy; food/agriculture; healthcare/public health; nuclear reactors/waste; and water wastewater.

Redefining the Federal Government's Role

On 12 February 2013, the White House released Presidential Policy Directive 21 (PPD-21), which outlined and emphasized the federal role in critical infrastructure protection – especially the leadership of the U.S. Department of Homeland Security – and set three overarching strategic imperatives:

- "Refine and clarify functional relationships across the federal government to advance the national unity of effort to strengthen critical infrastructure security and resilience";
- "Enable efficient information exchange by identifying baseline data and systems requirements for the federal government"; and
- "Implement an integration and analysis function to inform planning and operational decisions regarding critical infrastructure."

To strengthen critical infrastructure, the U.S. Department of Homeland Security operates two national critical infrastructure centers – one for physical infrastructure and another for cyber infrastructure – that function in an integrated manner and serve as focal points for critical infrastructure partners to obtain situational awareness and integrated, actionable information to protect critical infrastructure. Their effectiveness depends on the quality and timeliness of information and intelligence they receive from the federal departments and agencies, critical infrastructure owners and operators, and state, local, tribal, and territorial entities.

In case of a disruption in the primary systems, the goal is "to enable efficient information exchange through the identification of requirements for data and information formats and accessibility, system interoperability, and redundant systems and alternate capabilities." PPD-21 recognized that information sharing within the government and with the private sector needed to increase, while also respecting privacy and civil liberties.

The integration and analysis function resides at the intersection of the two national centers, including the capability to collate, assess, and integrate vulnerability and consequence information with threat streams and hazard information. According to this directive, such integration and analysis would:

- Aid in prioritizing assets and managing risks to critical infrastructure;
- Anticipate interdependencies and cascading impacts;
- Recommend security and resilience measures for critical infrastructure prior to, during, and after an event or incident; and
- Support incident management and restoration efforts related to critical infrastructure.

Emphasizing Capabilities

The new Protection Framework covers a vast array of capabilities necessary to secure the nation against all hazards and disasters, with key distinctions between protection, prevention, and mitigation. For example, protection covers activities related to all kinds of hazards, while prevention applies only to activities

related to imminent terrorist threats. In addition, protection focuses on everyday activities to promote security and threat deterrence, while mitigation focuses on everyday activities to create resilience. The mission activities listed in the Protection Framework are classified into three broad categories:

- *Community and infrastructure protection* – including cyber security, defense against weapons of mass destruction threats, defense of agriculture and food, and health security;
- *Transportation and trans-border security* – including border security, immigration security, maritime security, and transportation security; and
- *Protection of key leadership and events.*

The Protection Framework describes each of its 11 core capabilities and lists critical tasks for each one:

- *Planning* – Implement security, protection, resilience, and continuity plans and programs, train and exercise, and take corrective actions;
- *Public information and warning* – Determine requirements for protection stakeholder information and information sharing;
- *Operational coordination* – Determine jurisdictional priorities, objectives, strategies, and resource allocations;
- *Intelligence and information sharing* – Adhere to appropriate mechanisms for safeguarding sensitive and classified information;
- *Interdiction and disruption* – Prevent movement and operation of terrorists into or within the United States and its territories;
- *Screening, search, and detection* – Develop and engage an observant nation, including individuals, families, communities, and local, state, tribal and territorial government, and private sector partners;
- *Access control and identity verification* – Control and limit access to critical locations and systems to authorized individuals carrying out legitimate activities;
- *Cyber security* – Detect malicious activity and conduct technical countermeasures and mitigation activities;
- *Physical protective measures* – Implement security training for workers, focused on awareness and response;
- *Risk management for protection programs and activities* – Identify, implement, and monitor risk management plans; and
- *Supply chain integrity and security* – Analyze key dependencies and interdependencies related to supply chain operations.

Thus, the new Protection Framework provides individual, community, private sector, nongovernmental organizations, and government decision makers with an understanding of the spectrum of protection activities "to create conditions for a safer, more secure, and more resilient nation by enhancing protection through cooperation and collaboration."

Prevent, Detect & Deter

Special Report on Explosives & IEDs

Earlier this year, DomPrep conducted a by-invitation-only roundtable with 30-35 subject matter experts to discuss issues related to the detection, deterrence, and prevention of explosives and IEDs. A nationwide survey was conducted and a special report will be published next month.

Key takeaways from the roundtable:

- Privacy vs. Security concerns
- Gaps that exist between local and federal authorities
- The definition of "success" as it relates to detecting, deterring, and preventing attacks

FEMA guidance in implementing the National Protection Framework is for the whole community to unite and to build national preparedness. "Partners are encouraged to develop a shared understanding of broad-level strategic implications as they make critical decisions in building future capacity and capability. The whole community should be engaged in examining and implementing the unifying principles and doctrine contained in this framework, considering both current and future requirements in the process."

These planning and preparedness frameworks provide a strong foundation for all levels of government and all aspects of the private and nonprofit sectors to work together in the protection mission. It is the shared responsibility of everybody – not just law enforcement, emergency management, or homeland security – to protect against potential hazards and disasters as reflected in the December 2011 Strategic National Risk Assessment: aircraft as a weapon; animal disease outbreak; armed assault; biological attack (non-food); biological food contamination; chemical attack (non-food); chemical substance spill or release; chemical/biological food contamination attack; cyber attack against data; cyber attack against physical infrastructure; dam failure; earthquake; explosives attack; flood; human pandemic; hurricane; nuclear attack; radiological attack; radiological substance release; space weather; tsunami; volcanic eruption; and wildfire.

Kay C. Goss, CEM®, is executive in residence at the University of Arkansas and the chief executive officer for GC Barnes Group, LLC. Previous positions include: president at World Disaster Management, LLC (2011-2013); senior principal and senior advisor of emergency management and continuity programs at SRA International (2007-2011); senior advisor of emergency management, homeland security, and business security at Electronic Data Systems (2001-2007); associate Federal Emergency Management Agency director in charge of national preparedness, training, and exercises, appointed by President William Jefferson Clinton (1993-2001); senior assistant to the governor for intergovernmental relations, Governor William Jefferson Clinton (1982-1993); chief deputy state auditor at the Arkansas State Capitol (1981-1982); project director at the Association of Arkansas Counties (1979-1981); research director at the Arkansas State Constitutional Convention, Arkansas State Capitol (1979); project director of the Educational Finance Study Commission, Arkansas General Assembly, Arkansas State Capitol (1977-1979).

True Resilience in Practice

By Marko Bourne, CIP-R

There is broad and growing recognition that resilience is important, but there is less consensus about what this concept looks like in practice. The term could mean the ability to rebuild and recover from a disaster, the ability to mitigate risks and hazards, the ability to restore economic development and growth, or all of these factors combined.

True resilience is a combination of recovery, risk mitigation, and economic growth, but achieving it is easier said than done. Translating "resilience" from a laudable but amorphous concept into measurable results requires two key ingredients: (a) breaking out of operational and program silos at all levels of government; and (b) working with nontraditional groups that wield significant social influence.

Breaking Out of Silos

Communities receive funding from various sources – Federal Emergency Management Agency (FEMA), U.S. Department of Housing and Urban Development (HUD), U.S. Department of Health and Human Services (HHS), U.S. Department of Commerce, and others – and programs that often are not affiliated with each other. However, these funding partnerships – for example, FEMA Public Assistance and HUD Community Development Block Grants – sometimes create operational silos that may hinder resilience.

For example, communities typically receive federal grants from the U.S. Department of Homeland Security (DHS) to support state and local preparedness efforts by fire and police departments. These grants are targeted and augment what communities would normally do. Then there is another set of funds that localities receive from the Federal Emergency Management Agency (FEMA) to mitigate hazards (Hazard Mitigation Grant Program) and reduce future risks, such as flooding.

Mitigating risk is the hallmark of both programs, but one has a terrorism-centric focus, while the other is used primarily for flood mitigation or tornado safe-room development. Both programs talk about how to improve the current infrastructure of people, places, and things to make them

more resilient, but they are programmatically split, victims to separate political spheres of influence and rarely coordinated at a national program level or even within states.

Communities could avoid such division by examining how to link disparate programs and funding sources so they address resilience in a holistic, rather than unsystematic, way. For example, when a hurricane damages the public infrastructure of a community such as a bridge that carries an important road network, more than just the bridge is at stake. Commerce may be adversely affected when people lose mobility to travel to their jobs or to the store to get supplies. Local governments also can experience a drop in tax revenue. The economic ripples grow as private sector companies have their supply chain and workforce disrupted.

When considering these impacts, several mechanisms to support the rebuilding exist – FEMA for disaster reconstruction support and highway trust fund money from the U.S. Department of Transportation, just to name two federal resources. As community leaders think about restoring a lifeline bridge, they need to consider not only how to rebuild it better to withstand the next hurricane, but also how it can be built in such a way to enhance community growth, to prepare for the next event, and to promote community development or public safety. In turn, funding that expands the potential use beyond FEMA support could include other federal, state, and local resources, making the project more feasible, while also creating lasting resilience implications for the community.

After Hurricane Katrina in 2005, some states like Mississippi developed wide-ranging programs that focused on long-term major improvements to infrastructure, and used funding from multiple federal and state sources. They coined the phrase "global match," the goal of which was to leverage widespread federal funds that all required a state match to meet the criteria of each program so as to limit a large taxpayer burden for their already storm-ravaged economies. In some cases, this approach created improved and more resilient public safety communications systems that will have long-term resilience effects.

Harnessing the Power of Social Media & Community Groups

Local governments and communities are accustomed to working with familiar organizations such as the Red Cross and Salvation Army to aid in disaster response, but it is important to recognize that other ad-hoc community groups can have an even bigger impact, especially given the power and reach of social media. However, it can be challenging for emergency managers and local officials to learn how to harness the power of nontraditional groups in a fast-moving situation.

Part of resilience lies in understanding where the social capital of a community lies, and in being able to recognize new influencers and centers of gravity as they emerge. This means thinking less about how to control social media and more about how to harness and work with it, learn from it and make use of the power it can have. Some groups that are vital to the fabric of a community can be identified ahead of time, but not all of them. What matters is the ability to register when new community power brokers surface as events unfold, and to understand how to enlist their help and support.

Identifying the barriers to recovery efforts and working together to lift them is crucial. For example, it is the role of the power company to restore power quickly – but the state can lift permit requirements to allow out-of-state line workers to help, with community groups clearing the right of way to let these trucks in.

Breaking out of operational silos and harnessing the social power of local communities are the keys to real resilience. The results are measurable not only by how quickly any given community recovers from a disaster, but also by its success in reinvigorating and growing its economic base. Resilience in practice starts with rebuilding and planning, but does not end there. A community mired in disaster response mode for too long cannot return to healthy economic activity, which in turn would attract more business and more people wanting to live and work in the region. That is the meaning and the measure of true resilience.

Marko Bourne is a principal at Booz Allen Hamilton and a DomPrep40 advisor. He is leader of both the company's FEMA market team and its Emergency Management and Response practice, and has more than 27 years of experience in: emergency services; emergency management; policy, governmental, and legislative affairs; and public affairs. Before joining Booz Allen Hamilton he was FEMA's director of policy and program analysis (2006-2009) – and, earlier, director of business development for homeland security (2004-2006) at Earth Tech Inc./Tyco International. He also served as acting director of the DHS National Incident Management System Integration Center and as deputy director of FEMA's Preparedness Division (2003-2004).

RADIATION DETECTION & IDENTIFICATION

SMALL. SIMPLE. SPECIFIC.

Confident decision-making is critical when lives are at stake. Emergency responders must have fast and accurate threat information where they need it the most - in the field.

FLIR is focused on delivering advanced threat detection and identification tools that are more affordable and easier to use than ever before.

For example, the identiFINDER® R300 is the world's first pager-size radiation instrument that can detect, locate and identify radioactive isotopes.

Worn on a belt similar to a personal radiation detector (PRD), the identiFINDER® R300 provides the operator with all the information necessary to respond with confidence in the most hazardous and stressful environments.

To learn more about the identiFINDER® R300 and our other laboratory-caliber products visit www.flir.com/r300

FLIR®

THE WORLD'S SIXTH SENSE™

/flirhq @FLIRdetection

Building Resilience – School Safety & Security Standards

By Wayne P. Bergeron, Standards

Fire drills occur regularly in schools across the United States – a fire alarm sounds, students form a line and exit the classroom, teacher closes the door, and the class lines up on the playground, all in about 45 seconds. Fire drills do work so, even though there are an estimated 5,500 school fires that occur yearly according to the U.S. Fire Administration/National Fire Data Center, fatalities are exceedingly rare. However, such drills may not adequately prepare students and staff for all types of school emergencies. When an emergency is not a fire, the school may not have a drill for it.

It is not always apparent from the reports in the popular media, particularly in the wake of high-profile incidents such as school shootings, but schools are relatively safe places for children. According to a June 2013 report prepared for the National Center for Education Statistics (NCES), from 1992 to 2011, an annual average of 23 youths (ages 5 to 18) in the United States were the victims of homicides "at school" – defined as "in school buildings, on school grounds, on school buses, and at places that hold school-sponsored events or activities." That number is significantly lower than the 1,396 total homicides (at and away from school) in the same age group between 1 July 2009 and 30 June 2010.

Although every death of a child is tragic and heartbreaking, the average number of deaths from school homicides pales in comparison to the overall number of 45,069 child deaths (ages 0 to 19) in 2010 as reported by the National Center for Health Statistics. This also is significant considering that there are more than 130,000 public and private schools in the United States with more than 50 million students in grades K-12, according to the NCES. However, in light of recent high-profile incidents, perhaps they could be even safer, thus reducing 23 to a lower number, or perhaps even zero. Publilius Syrus, a Latin writer in first century B.C., stated, "He is most free from danger, who, even when safe, is on his guard."

Nature of the Problem

Because of the intense media coverage and high-profile nature of school shootings, it might be assumed that schools throughout the United States would be getting all of the help and assistance that they need to ensure complete and comprehensive school safety programs. However, an October 2013 NBC News article quoted one school safety expert, Kenneth Trump, "The federal government has repeatedly since Columbine cut federal school safety funding." Although there have been renewed efforts and programs since the Newtown, Connecticut, school shootings in 2012, the actual state of school safety in the United States is not completely clear. According to Trump, "There's always been a context of politics around this topic. The parents don't know what they don't know, and no one is rushing to tell them. There's been a history of downplay, deny, deflect and defend ... to protect the image of the schools."

There has been much discussion, information, and guidance concerning school safety and security in light of the many high-profile incidents over the past two decades. However, there has been an emphasis on active shooters, which tend to be low-probability incidents. Many of these programs and resources do not even begin to address the spectrum of school safety issues that are more likely to occur and that can be just as dangerous as, and result in as many or more fatalities than, an active shooter scenario – for example, tornadoes or other natural disasters, school bus traffic accidents, or a manmade catastrophe such as a train derailment of hazardous materials or chemical spill in close proximity to a school.

The reality is that a single research-based set of universally accepted standards regarding school safety and security currently does not exist. Albeit, some states have either developed or are considering their own standards, but they vary widely in scope, scale, and applicability. Even at the federal level, there have been a number of studies on these issues by various federal agencies, but a single set of guidance and standards has yet to emerge that is widely accepted, much less researched and validated. In many cases, this may be due to an overall lack of empirical research into exactly what standards are most effective. There also is the issue of differences and variations between individual schools and districts that make a universal set of standards and guidelines a difficult proposition at best.

A Possible Solution

The overall emergency management community has the Emergency Management Accreditation Program (EMAP) and the National Fire Protection Association's NFPA 1600 standard as benchmarks for overall emergency management programs. Law enforcement has the Commission on Accreditation of Law Enforcement Agencies (CALEA®) and its voluntary program. However, no such equivalent exists for school safety and preparedness. Rather than a stringent set of mandatory regulations dictating "how" a school or district must provide school safety, a more suitable approach for education may be a broad-based set of voluntary school safety and security standards and guidance that allow schools and districts the flexibility to apply solutions within their own specific environment, culture, and resource constraints. Such an approach would establish requirements, but also provide options for how to accomplish them given the nature of the particular environment.

Of course, creating a voluntary program has specific value in terms of effectiveness since most schools and districts have more than enough mandatory requirements that sometimes lead to "check the box" compliance. Additionally, having such a program or project eventually being developed into an actual accreditation like EMAP or CALEA® would offer legitimacy and validity. Having a statewide or national organization – for example, National Emergency Management Association, National Sheriff Association, National Association of Police Chiefs, or the National Association of School Resource Officers – sponsor such a program as a voluntary accreditation program would ensure standardization and proper advocacy. Applicable models already exist in other areas, so perhaps it is time to apply them to something as important as school safety and security.

Wayne P. Bergeron, lieutenant colonel, retired from the United States Army in May 2011 after a 23-year career within the Military Police Corps and Special Operations Forces. He currently serves as an instructor teaching both criminal justice and security and emergency management at the University of North Alabama in Florence, Alabama. His education includes undergraduate degrees in criminal justice and political science, a master's degree in international relations from Troy University, and he is currently in his third year of doctoral study in emergency management at Jacksonville State University.

Solar Storm Near Miss & Threats to Lifeline Infrastructure

By Charles Manto, Cyber & IT

In July 2011, the InfraGard National Board and the Federal Bureau of Investigation approved the formation of the InfraGard National Electromagnetic Pulse Special Interest Group (EMP SIG) for the purpose of sharing information about threats that could affect critical infrastructure nationwide for more than a month and encouraging local communities to become more resilient. The threats specifically include manmade electromagnetic pulse (EMP), cyberattacks, coordinated physical attacks, pandemics, and extreme space weather. Many are not aware that the "100-year solar storm" creates ground-induced currents that travel up ground wires and can damage transformers and other large electronic systems that have long repair or replacement times.

High-impact threats are qualitatively different from many other threats for one main reason. Unlike hurricanes Katrina or Sandy, which affected regions and allowed other areas to rally to the aid of local communities, high-impact events have the capability of affecting much of the country simultaneously and limiting resources that are necessary for relief and recovery efforts. Instead of waiting days for help, affected regions could wait months for any meaningful aid. In a "just-in-time" society, the consequences are barely imaginable, but a historical background may help planners appreciate the need to minimize these effects.

Building National Awareness

In October 2011, the National Defense University and the EMP SIG co-sponsored the first comprehensive nationwide contingency planning workshops and exercise on extreme space weather that could have a nationwide impact. Until that time, even the U.S. Department of Defense had not planned for a collapse of civilian infrastructure nationwide that would last more than a couple weeks (outside of nuclear or world war). In December 2011, the EMP SIG reported its findings in a seminar at the December 2011 Dupont Summit of the Policy Studies Organization in Washington, D.C. Less than 8 months after the summit, on 23 July 2012, the earth experienced a near miss of a potentially cataclysmic solar storm.

Since then, on the first Friday of December each year, the EMP SIG has gathered top technical and policy experts to discuss such high-impact threats at subsequent Dupont Summit gatherings. Proceedings from the 2012 and 2013 summits are available online. By the second anniversary of the solar near miss, an array of scientific articles provoked attention in the international media.

On 9 July 2013, *Space Weather* published a study conducted by university and NASA researchers, entitled "A major solar eruptive event in July 2012: Defining extreme space weather scenarios." A NASA article published on 23 July 2014 quoted one of the *Space Weather* authors, Daniel Baker from the Laboratory for Atmospheric and Space Physics at the University of Colorado Boulder, "I have come away from our recent studies more convinced than ever that Earth and its inhabitants were incredibly fortunate that the 2012 eruption happened when it did. … If the eruption had occurred only one week earlier, Earth would have been in the line of fire."

The NASA article cited the often-quoted 2008 National Academy of Sciences report on a FEMA-funded economic impact assessment, which stated that the total economic impact of such an event "could exceed $2 trillion or 20 times greater than the costs of a Hurricane Katrina. Multi-ton transformers damaged by such a

storm might take years to repair." Baker further said, "In my view, the July 2012 storm was in all respects at least as strong as the 1859 Carrington event. … The only difference is, it missed."

In another July 2014 research article published in *Space Weather*, entitled "Assessing the Impact of Space Weather on the Electric Power Grid Based on Insurance Claims for Industrial Electrical Equipment," the authors showed how even small space weather events have been causing damage to the electric power grids. Claim statistics from an examination of over 11,000 insurance claims from 2000 to 2010 revealed that "geomagnetic variability can cause malfunctions and failures in electrical and electronic devices that, in turn, lead to an estimated 500 claims per year within North America." If small events can have such an effect, it becomes a lot easier to imagine the impact of the storm that just missed Earth in 2012. In addition, this data suggests that, if protection were to be provided for equipment against the larger threat, then money would be saved on a day-to-day basis for even the smaller ones.

Assessments & Studies Raising Awareness

Awareness of this storm peaked when *The Washington Post* editorial board made its recommendation on 9 August 2014, "The world can and should do more to prepare, adapting satellite systems, toughening electric grids and, above all, ensuring that scientists have the tools they need to anticipate space weather…. For a variety of reasons – including the threat of severely inclement space weather – lawmakers must take a wider view."

Manmade EMP poses even greater problems according to studies publicly released by the congressional EMP Commission between 2004 and 2008 and highlighted in the 14 August 2014 op-ed by R. James Woolsey and Peter Vincent Pry, both formerly with the Central Intelligence Agency. Not only is it possible for small mobile electromagnetic interference devices to be used at relatively close range against vulnerable electronic equipment and systems, but a relatively small-yield nuclear weapon could be placed on a scud missile, launched from an offshore freighter, and detonated in the upper atmosphere (80-300 miles high) to impact multiple regions or an entire continent. The electromagnetic fields emanating from EMP weapons include those that are in the billionths of seconds – much faster than lightening strikes. They travel through the air and across any kind of conductor, particularly long power or communication wires that act as giant welcoming antennae.

A 10 September 2007 economic impact assessment by the Sage Policy Group of Baltimore showed that even a regional EMP incident between Richmond, Virginia, and Baltimore, Maryland, could cause $770 billion of economic damage, even without considering loss of equipment or secondary effects such as lack of water in a large fire. The EMP Commission gave high marks for the study methodology and results, as did the economists who did the work quoted by the Academy of Sciences. In addition, the Sage report determined that protecting even 10 percent of the most critical infrastructure could alleviate up to 60 percent of the economic losses in medium-impact scenarios.

This study shows that it can be relatively inexpensive to protect critical infrastructure and that not all infrastructure may need to be protected to the same degree. However, as in the case of extreme space weather, little has been done until now to protect civilian critical infrastructure. Numerous studies have shown that U.S. lifeline infrastructures are highly interdependent and erected much like a "house of cards." Subsequent tests by Iran of freighter-launched missiles, North Korean satellite success, and turbulence in places such as the Middle East have increased concerns about the ability of nonstate actors and the likelihood of a high-altitude nuclear EMP event.

Cyberthreats – Big & Small

Cyberattacks have affected everyone, even if they have merely been an inconvenience. Fortunately, insurance and other companies have shielded communities and absorbed billions of dollars in costs resulting from effective cybercrime. The largest risks to society are likely to be experienced in the arena of industrial controls, which are largely unprotected by traditional cyberprevention techniques. Numerous reports have shown that foreign cyberattackers have already breached many utilities.

What is most telling is the public release of a Federal Energy Regulatory Commission report on 12 March 2014, which some say was for official use only, showing how the successful attack of only nine electric grid facilities could result in a nationwide power outage. The report published in *The Wall Street Journal* resulted in a hastily convened U.S. Senate hearing. There was no challenge to the accuracy of the report about the grave vulnerability the country faces, but rather only a challenge because the report was "mishandled" and leaked to the public.

Although the vast majority of cyberattacks are low-impact, high-frequency events, there is a growing concern about their ability to become high-impact, low-frequency events. Like other high-impact threats, they have the ability to cause similar levels of disaster, especially when combined with other threats. However, the right type of mitigation and preparation can reduce both the impact and the temptation for adversaries to try to use them.

What remains uncertain is the willingness to engage these high-level threats. Psychological and political views complicate the discussion – a way to impose more government regulation versus a scare tactic to raise the nation's defense and homeland security budgets. In reality, there are daily cost savings, economic development, as well as environmental and security benefits when taking a reasonable systems approach to mitigate these threats. This is especially true when local communities are more sustainable and capable of creating and managing a larger percentage of their critical power and food requirements.

Sharing the Right Information With the Right People

Similar to concerns that senators have raised at past cyberthreat hearings, some may think it is a challenge to begin an EMP discussion without causing panic or providing too much information to "the bad guys." One possible solution is to engage the emergency management and contingency planner communities, who are already emotionally and intellectually accustomed to dealing with disaster planning. Another is to make better use of InfraGard. So far, InfraGard is the only federally sponsored program that requires all of its individual members to sign nondisclosure agreements so they can trust each other as they hold confidential conversations and share sensitive law enforcement information. The Federal Bureau of Investigation also provides background checks so an even greater level of trust can be achieved. These trusted and informed conversations can then lead to more-effective engagement with the public – through social media outlets – similar to the EMP SIG conferences.

This year, the EMP SIG will hold its conference on Friday, 5 December 2014. On the day before, it will conduct a by-invitation-only tabletop exercise based on a high-impact incident. For additional information or to attend the conference, visit the event page. The November 2014 issue of the *DomPrep Journal* will bring together subject matter experts to take a more in-depth look at this topic to further the EMP discussion and determine what actions may be considered to better prepare for and mitigate these threats.

Charles "Chuck" Manto is CEO of Instant Access Networks LLC, a consulting and research and development firm that produces independently tested solutions for EMP-protected microgrids and equipment shelters for telecommunications networks and data centers. He received six patents in telecommunications, in computer mass storage and EMP protection and has another one pending for a smart microgrid controller. He assists other entrepreneurs and investors with their intellectual property strategies and has developed valuation methodology accepted by the U.S. Department of Defense, countries, and companies participating in industrial defense conversion. He is a senior member of the IEEE and founded and leads InfraGard National's EMP SIG. He can be reached at cmanto@stop-EMP.com

BioFire Defense has led

the industry for over 15 years

in pathogen identification

technologies.

Now, more than ever

we remain committed

to providing the industry

with superior products,

unsurpassed customer support,

and a solid future of

innovation and design.

Follow us, we'll show you how.

BIOFIRE™

DEFENSE

Follow us at www.BioFireDefense.com

Leadership Consciousness: A Call to Action

By Samuel Johnson Jr., Standards

Tragedies have the potential to claim thousands of lives, injure thousands more, and generally cause disruption. Events such as the 2001 airplane attacks on the World Trade Center in New York, the 2013 backpack bombing at the Boston Marathon, and the major landslide that collapsed an entire street in the city of Baltimore, Maryland, in May 2014 bring these tragic incidents to the national stage. These events also increase awareness about the courage of first responders when faced with pain, as well as loss and destruction to society.

Long before disaster strikes, emergency management and public safety professionals are serving in their communities. The uniforms, badges, police cars, and fire apparatus are reminders that responders often put service before self. The calling to the public safety profession and to the role of leadership within these organizations should not be taken lightly. Professional safety standards that these people vow to uphold are surpassed only by the requirement that personnel exercise high levels of personal responsibility. The hallmark of that responsibility is to model behavior that is beyond reproach and that builds positivity in the neighborhoods they serve.

Laying a Strong Foundation

With this call to action, it becomes the duty of all personnel to be an agent for change in order to influence and design a sustainable culture of leadership consciousness within public safety organizations. "Leadership consciousness" is the awareness that there are consequences for all actions – either positively or negatively – and that public officials have the ability to influence others through the authority of his or her position. Although the authority to act in times of emergency is noble, the authority to influence a positive model within the community and throughout an agency is just as great.

Emergency management has highly trained professionals in the nation's workforce. They receive hundreds of hours of instruction to meet initial certification requirements, and countless hours of continuing education units to maintain these credentials. They are taught to exercise this training during the course of their duties, and revert to such teachings as second nature to enhance survival efforts during stressful situations. But leadership consciousness challenges these professionals to train themselves not only to effectively act in the face of danger, but to weigh the implications of their actions and behaviors. They must consider the weight of their actions and how those outcomes could potentially affect themselves, their organizations, and their communities.

Leadership consciousness requires leaders to examine their thoughts and beliefs. This process includes honesty and recognition of the visibility and impact leaders have because others model their behaviors, in reverence or rebellion, to authority. From the 2000 movie, "Remember the Titans," came the following quote, "Attitude reflects leadership." Public safety leadership is not about personnel titles within an organization, but about the effect officials have on the people they serve. Mark Sanborn, president of Sanborn & Associates Inc., stated in his 2006 book, entitled "You Don't Need a Title to Be a Leader":

> "Leadership is influence.... You don't need a title to be a leader in life. And the simple fact of having a title won't make you a leader. I've found that everyone has the opportunity to lead, every day. It doesn't matter what your position is, or how long you've worked at your job.... Anyone at any level can learn to be a leader and help to shape or influence the world around them."

Instilling Honor & Respect

From the person on the front line providing emergency response services to the department head of an organization, each person has to have the consciousness to know that every move they make and every action they take is being watched, critiqued, and followed by somebody. Officials also need to realize that, by virtue of the positions they hold, the public's perception is reality.

Former police commissioner of Baltimore City, Leonard Hamm, offered in an address to a 2006 graduating class of the police academy this sage advice: "Do what's right in the face of what's wrong."

Actions or behaviors have the potential to defy – or exemplify – departmental policies, local ordinances, or state and federal laws. Therefore, it is important to remember and honor the oath of office, leading officials to examine their moral compasses and act in a professional manner at all times.

In the wake of massive corruption scandals throughout the country and abroad, the "face" of public safety is being smeared by the actions of a few rogue officials. With every report of an incident in which officials decide to act outside of their prescribed training and oath of office, it gives the public safety profession a "black eye" and cuts away at the fabric of society as well as at the organizations their positions were created to uphold.

Sir Robert Peele authored the "Principles of Law Enforcement" in 1829. The foundation of those nine principles still holds true today, but Principle Two resonates throughout all public safety disciplines, "The ability of the police to perform their duties is dependent upon public approval of police existence, actions, behavior and the ability of the police to secure and maintain public respect."

Respect is a vital ingredient in creating an effective public safety organization. When officials choose not to obey the laws themselves, the respect, public approval, and support that these offices are expected to garner, vanish without a trace.

Building Rapport & Awareness

The absence of internal, organizational, and community leadership was demonstrated in the aftermath of Hurricane Katrina. The inability to build rapport and create a positive working influence contributed to complete anarchy during that crisis. In the days following that historic storm, looting, violence, and other criminal activities became serious problems. The actions of people within the community trying to survive as well as those of public safety officials contributed to the disarray.

Reporter Julianne Hing wrote in a 2010 article published by *Colorlines*, "The New Orleans Police Department has long been synonymous with brash corruption and misconduct.… But when the storm arrived on August 29, 2005, and swept away New Orleans' lower 9th ward, it opened up a period of unchecked police aggression that shocked not just the city but the nation."

All agencies and organizations harbor their own baggage. Therefore, this is not an indictment simply on the New Orleans Police Department, but a lesson on how the failure of leadership consciousness can dismantle any agency or organization. Emergency management defines preparedness as a state of readiness to respond to a disaster, crisis, or any other type of emergency. As such, perhaps preparedness is the cognitive recognition of awareness. In addition to ensuring that the right emergency operations plan and the appropriate equipment to respond to potential threats and dangers are in place, agencies must ensure that they have people who exercise the highest level of ethical and moral behavior in the face of crisis.

In a position of such great magnitude, fiduciary responsibility, and visibility, everything matters. People may not give their behaviors or actions a second thought unless they have the potential for adverse implications or consequences. Perhaps scrutinized almost as much as the members of professional sports teams, public safety officials have a duty to represent themselves and their organizations in a professional manner every time they put on their uniforms, or engage in any way with the public.

In the end, leadership consciousness within public safety is the ability to understand that each person represents something bigger than him- or herself, and that each day these professionals carry the reputation and image of fellow colleagues on their shoulders with every action and behavior they exhibit. They should never underestimate the impact that actions and behaviors will have on other people. The message conveyed through the many works of Mahatma Gandhi resonates with the concept of leadership consciousness, "Be the change that you want to see in the world."

Samuel Johnson Jr., is the training coordinator for the Mayor's Office of Emergency Management in Baltimore City. In this role, he is responsible for providing emergency preparedness training for over 5,000 public safety professionals within a city that services over 640,000 residents. He has served within the city of Baltimore for 6 years in various capacities, which include the Baltimore Police Department and the Housing Authority of Baltimore City. He completed his masters degree at the Johns Hopkins University, Police Executive Leadership Program. Contact information: samuel.johnson1220@gmail.com.

Military & Civilian Resources: Doing More With Less

By Aaron Sean Poynton, DOD

Police action in response to civil unrest in Ferguson, Missouri, following a fatal shooting on 9 August 2014 has brought scrutiny to the U.S. Department of Defense's (DOD) Excess Property Program 1033 (DOD 1033). Often referred to as the "surplus-property program" or colloquially as the "hand-me-down program," DOD 1033 is a federal program that facilitates the transfer of excess DOD equipment to state and local law enforcement agencies for reuse at little or no cost to the receiving agency.

Two weeks after the shooting, in response to criticism of the perceived militarization of civilian law enforcement agencies, President Barack Obama ordered a comprehensive review of the program. This review likely will: (a) lead to recommendations and changes to ensure the program does not exacerbate the perceived militarization of civilian police forces; and (b) update standards to ensure proper training and use of certain military-grade equipment. Although the review is generally welcomed by the American people to ensure that law enforcement agencies are not on a slippery slope to becoming paramilitary organizations, DOD 1033 is of great value to the American taxpayer and provides much needed equipment to cash-strapped police departments around the country.

Allocation of Excess Resources

The National Defense Authorization Act for fiscal years 1990 and 1991 authorized the transfer of excess DOD property to law enforcement and corrections agencies for use in counterdrug activities, under then-program 1208. During the reduction of military forces in the mid-1990s, large amounts of excess equipment – much of the equipment used in the Gulf War – were passed down to state and local law enforcement and corrections agencies. In 1996, Congress amended the program by removing most corrections agencies, as well as jailers and wardens, as qualified recipients. Other changes widened the receiving agency mission scope beyond just counterdrug activities. DOD 1033 was opened to all bona fide law enforcement agencies whose compensated law enforcement officers have powers of arrest and apprehension.

The types of equipment transferred under DOD 1033 include everything from armored vehicles and helicopters to office supplies. Although much of the recent media attention has focused on MRAP (mine-resistant ambush protected) vehicles and weapons, the list of most-received items includes first aid kits, flashlights, goggles, and sandbags. In 2013 alone, DOD transferred nearly a half-billion dollars' worth of excess property to some of the over 8,000 civilian law enforcement agencies that participate in the program. The program has been successful in the efficient allocation of resources, from which taxpayers benefit.

However, there is public fear that DOD 1033 will facilitate the militarization – policing by military or even paramilitary police forces – of domestic law enforcement. This conviction is deeply rooted in the fabric and history of the United States. The founding fathers cautioned on the dangers of using standing armies for domestic policing, and this sentiment is evident in several of the Federalist Papers. As Samuel Adams wrote in 1768 in the Boston Gazette, "Even when there is a necessity of the military power, within a land . . . a wise and prudent people will always have a watchful and jealous eye over it." Throughout the republic's history, measures have been in place to protect against this concern.

The Posse Comitatus Act of 1878 laid the foundation and removed the army from conducting local policing operations during the Reconstruction era. The Posse Comitatus Act was later applied to all branches of the military – with the exception of the Coast Guard, which now falls under the U.S. Department of Homeland Security (DHS), and the nonfederalized National Guard, which may be empowered with domestic law enforcement responsibilities when under the command and control of a state's governor and the adjutant general. Only under exigent circumstances would the federal military have domestic law enforcement powers under the command of the president and secretary of defense.

Fortunately, in the United States, almost no law enforcement activities require a military response, and the vast majority of police calls do not require a civilian armored or tactical response. Rather, they require the "soft skills" of policing, such as good judgment, problem solving, quick decision-making, effective communication, empathy, compassion, multitasking, resourcefulness, courage, vigilance, and

integrity. However, the United States can be a violent and dangerous place, where criminals exploit their freedoms to do harm.

Many law enforcement agencies deal with hardened and violent criminals daily, with high-risk apprehensions being commonplace in some jurisdictions. Moreover, there is a great threat of domestic terrorism with homemade bombs, such as those used in the 2013 Boston Marathon bombings, and well-armed, coordinated assaults, such as the "Mumbai-style" attacks. Terrorism aside, police departments in the United States occasionally handle crimes from extremely violent, well-armed criminals.

A Shift in Criminals, Budgets & Police Tactics

The 1997 North Hollywood, California, bank robbery and shootout was a watershed moment in modern policing that compelled law enforcement agencies around the United States to reevaluate their equipment assets – or lack thereof. Assailants wore body armor and carried automatic assault weapons with 3,300 rounds of ammunition, including armor piercing bullets. Outgunned and underresourced, Los Angeles Police Department (LAPD) officers had to commandeer a civilian armored truck to evacuate the wounded. During the intense firefight, officers also commandeered shotguns, rifles, and more-powerful ammunition from a local gun shop. In the days after that violent assault, the LAPD secured rifles from DOD surplus as police departments around the country reevaluated their equipment needs.

Although this robbery was an anomaly in its magnitude of violence, the Federal Bureau of Investigation 2012 statistics revealed that a robbery occurs every 1.5 minutes in the United States. In the same year, 48 police officers died in the line of duty during felonious incidents. When an armored or tactical response is required, local police departments need to have equipment to effectively counter the threat and remain safe. However, such equipment is expensive, so many local and state police departments simply cannot afford it. For example, the BEARCAT® (Ballistic Engineered Armored Response Counter Attack Truck) is a popular armored vehicle used by many civilian law enforcement agencies, but it can cost up to $300,000.

The recent economic downturn has put a strain on local and state budgets, as well as public safety budgets. A 2011 report published by the International Association of Police Chiefs found that some 85 percent of responding law enforcement agencies had to reduce their budgets, with nearly a quarter of them cutting 10 percent or more. Buying new equipment often comes secondary to keeping "feet on the street," yet many departments have experienced layoffs and furloughs. A natural and efficient way to meet the needs of state and local law enforcement is to locate excess equipment at low or no cost.

The U.S. federal government is the single largest buyer in the world. Having the biggest defense budget in the world, the DOD spends billions of dollars each year on the development and acquisition of equipment, some of which has dual or multiuse applications. When this equipment is no longer needed, the DOD can pay to have it destroyed or transfer it to other organizations that need equipment. In the case of DOD 1033, some equipment that qualifies for transfer but is not claimed is destroyed, donated, or sold. Matching needy customers to excess supplies is at the heart of efficient allocation of resources.

Continued Support to Fight Future Threats

Like many high-profile incidents, the civil unrest in Ferguson serves as a flashpoint for many peripheral issues. Despite common misconception, Saint Louis County – where the city of Ferguson is located – did not receive heavy tactical equipment, such as MRAPs, through DOD 1033. Rather, DOD records show Ferguson received items such as radios, generators, and utility trucks. This is the type of functional equipment often requested by local first responders during major disasters, such as Hurricane Katrina in 2005. Saint Louis County also received a small number of pistols and rifles under the program, which is equipment frequently procured by law enforcement agencies using their own budgets without DOD's assistance.

Economic benefits of DOD 1033 should not be overlooked due to the tactical response in Ferguson and an ingrained fear of military rule. The saying, "Do more with less," has become conventional in the new era of reduced government spending and DOD 1033 does just that.

Aaron Sean Poynton is a guest writer for the DomPrep Journal and has served in various leadership positions with companies in the defense and homeland security markets over the past 10 years. Before his civilian career, Aaron served in the U.S. Army for seven years, including time as a civil-affairs specialist. He is a graduate of the Johns Hopkins University Army ROTC program and holds a bachelor's degree in economics from the University of Maryland UMBC, a master's degree from the George Washington University School of Business, and a doctorate in public administration from the University of Baltimore.

Applying the Kipling Method to Infrastructure Protection

By Joseph Cahill, EMS

I keep six honest serving-men:
(They taught me all I knew)
Their names are What and Where and When
And How and Why and Who.
– Rudyard Kipling (April 1900)

As in Kipling's poem, protecting the infrastructure requires asking many questions. To begin, "What critical infrastructure needs to be addressed?" Planners must identify critical infrastructure components, beginning with the required work functions. In most cases, agency officials could summarize what their agencies do in just a few bullet points. For an emergency medical services (EMS) agency, these points might include:

- Respond to the scene of emergencies;
- Provide lifesaving and supportive care; and
- Transport patients to the hospital.

Added to this list should be any functions that are required by statute – for example, in the state of New York, this would include:

- Provide a quality assurance officer to perform quality review;
- Supply and equip ambulances to the standard laid out in Part 800 of the statute; and
- Have one licensed physician as medical director per 100 paramedics.

Each of these six responsibilities are integrated within the critical infrastructure: responding and transporting require a functional vehicle; providing care as well as supplying and equipping ambulances assume that vehicle is fully stocked to the standard; and all six assume minimum staffing of paramedics and/or emergency medical technicians. In addition, the call for help has to be received and the unit must be dispatched, which requires more staffing, a fixed facility, and a radio system.

Working Groups & Budgets

After creating a list of critical functions, there needs to be a review of each infrastructure's needs. A working group assigned to review a specific asset would be able to better build a team that includes the expertise needed to do more than a surface evaluation. For example, review of a dispatch system may require more than simply a radio communications person. The team also may need facility expertise, knowledge about information technology, and EMS experience to form a complete picture of the asset and its requirements. This team then would perform a multistep process: (a) assess; (b) identify both current and projected future shortfalls; then (c) create an action plan that includes time frames for completing the work.

Planners and managers often hear the questions, "Why does this money need to be spent? And why now?" A critical infrastructure project typically can be justified by one of the following four statements:

- The infrastructure is at risk of failure and needs to be maintained or repaired;
- The infrastructure needs to be updated in order to comply with a standard/statute;
- The infrastructure is at risk from an outside threat; and
- Improvement of the infrastructure will save or make money in the long term.

"All the elements for success are articulated when the work is linked to a set time frame, specific funding, and detailed responsibilities."

However, the tough question that is ever present is, "Who pays?" A useful strategy is to determine the work needed as if funding were not an issue. This develops the ideal plan, after which planners can develop a number of lesser proposals at different price points. The planner then should assess the current budget, grant opportunities, and possible community partners who might be able to provide funding before the planner must request additional government funding. In this way, planners limit their number of requests for additional funding and are more confident that their funding requests are actually necessary.

Elements for Success

A model that could be adapted for any action plan could include the following questions:

- What asset requires attention?
- Why does it need to be protected?
- How will the infrastructure be maintained, improved, and protected?
- Who will be responsible for performing each task?
- When are the deadline(s) for each task?
- Where will the work be completed?

All the elements for success are articulated when the work is linked to a set time frame, specific funding, and detailed responsibilities. There are no guarantees of success – each time an infrastructure asset is examined, there is the potential for discovering unforeseen needs – but having a clear plan would help limit any problems that arise.

Joseph Cahill is the director of medicolegal investigations for the Massachusetts Office of the Chief Medical Examiner. He previously served as exercise and training coordinator for the Massachusetts Department of Public Health and as emergency planner in the Westchester County (N.Y.) Office of Emergency Management. He also served for five years as citywide advanced life support (ALS) coordinator for the FDNY – Bureau of EMS. Before that, he was the department's Division 6 ALS coordinator, covering the South Bronx and Harlem. He also served on the faculty of the Westchester County Community College's paramedic program and has been a frequent guest lecturer for the U.S. Secret Service, the FDNY EMS Academy, and Montefiore Hospital.

Staying Safe Amid a Violent World

By Richard Schoeberl, Law Enforcement

Every year on September 11, U.S. citizens remember the people lost and the dangers the nation faced during and following the terrorist attacks against the United States in 2001. The domestic unrest – coupled with the mounting insurgency of the Islamic State of Iraq and the Levant (ISIL), the ongoing drug cartel violence in Mexico, the continuing confrontation in the Ukraine, and the crisis in Gaza – may create the perception that the whole world is unsafe. Despite the current turmoil and looming safety concerns associated with this year's devastating earthquakes, tsunamis, tornadoes, and other severe weather, U.S. citizens still travel abroad routinely for work and pleasure. These natural and unnatural disasters not only escalate public safety awareness, they reaffirm the need for individual emergency preparedness.

Recognizing Threats

Recent headlines have been saturated with the ISIL beheadings of two U.S. journalists. Even more alarming is the fact that ISIL is calling on all Muslims to kidnap U.S., British, and Israeli citizens to be used as "bargaining chips." Situational awareness and extra vigilance should not be limited to those traveling in the Middle East, but also should include vacationers, contractors, and military personnel, both domestically and abroad.

The callous ISIL now is vowing to broaden its operation to include killing Americans wherever and whenever they can. The U.S. government knows that some Americans have joined ISIL and are prepared to conduct suicide bombings. This concerns the intelligence community, specifically as it will pose risks upon their return. UK officials believe that hundreds of its citizens have now joined the ISIL militants and, from what has been observed, committed some of its most brutal killings. The Agence France Presse reported on 23 September 2014 that about 3,000 Europeans have joined ISIL.

However, ISIL alone has not triggered the spiral downward in global safety. The continuous conflict in Syria, the worsening situation in Ukraine, and civil war in South Sudan all contribute to the downward trend. The world has become less peaceful each year since 2008 according to the 2014 Global Peace Index (GPI). The Institute for Economics and Peace, which prepares the GPI, calculates how safe, secure, and peaceful a country is by looking at several different indicators. The indicators are weighed according to importance, such as the level of perceived criminality in society, political terror scale, number of deaths from organized conflict, number of external and internal conflicts fought, number of homicides, number of internal security officers and police, and the ease of access to small arms and light weapons.

On 10 April 2014, the U.S. Department of State website issued a worldwide caution to "update information on the continuing threat of terrorist actions and violence against U.S. citizens and interests throughout the world." The website reminds U.S. citizens to maintain a high level of awareness and to take appropriate steps to increase their security attentiveness.

Taking Precautions

In today's volatile world, where terrorists target people simply because of their citizenship, U.S. citizens residing or traveling abroad should take certain safety precautions. To avoid being easy targets – especially for theft and assault – it is important to use good judgment and caution when navigating new and foreign surroundings. According to the U.S. Department of State's website, here are a few recommendations:

- Register in the Department of State's Smart Traveler Enrollment Program (STEP) to receive safety and security announcements pertinent to the countries of travel and, in the event of an emergency, the U.S. embassy in that country can contact travelers more easily;
- Pay attention to travel alerts and warnings available through the Department of State, the Internet, and news outlets, and consider postponing travel to countries experiencing civil unrest, dangerous conditions, terrorist activity or, in some cases, no U.S. diplomatic relations; when traveling, stay in hotels with dependable Internet access and monitor local English-language news websites each morning and evening;
- Do not advertise U.S. citizenship in countries where there could be anti-Western sentiment – including clothing or markings that identify the United States, religious jewelry, and visible guidebooks and street maps that are common among tourists;

- Protect U.S. passports and other recognized travel documents when traveling to or from the United States;

- Make photocopies of all travel documents, information, and pictures of children in case of emergency, loss, or abduction; leave a copy with a family member in the United States; and only carry a passport when necessary – a color photocopy of the passport (the cover and first two pages) can serve as identification while the original is secured in a hotel-room safe; and

- Contact the U.S. embassy if unaware of foreign laws and legal systems, which can be vastly different from those in the United States – more than one-third of Americans imprisoned abroad are held on drug charges, which include possession and/or trafficking of drugs, possession of prescription drugs purchased legally somewhere else, and purchase of prescription drugs that local authorities alleged were for commercial use.

Age is not a discriminatory factor for becoming a target abroad, especially considering that more than 280,000 U.S. college students studied overseas in 2013, according to the Institute of International Education. Sometimes it is not about being the victim of a crime, but rather being involved in a crime. In April 2014, the Federal Bureau of Investigation (FBI) introduced a video to discourage U.S. college students, who have been targeted by foreign governments to serve as spies, from getting involved in espionage. The FBI warns that foreign intelligence officers initially develop a relationship under apparently harmless pretexts, such as an internship, writing assignments, or cultural immersion program. The effort by the FBI is in reaction a U.S. college student from Michigan, Glenn Shriver, who studied in China. After being seduced by Chinese intelligence officers, Shriver agreed to provide national defense information. He received $70,000 over a five-year period for his efforts and ultimately was sentenced to federal prison for four years for attempting to provide sensitive information to China.

Crime and violence are serious problems and can occur anywhere. However, places where pockets of anti-U.S./anti-Western feelings are present raise the threat level for travelers. A Google Consumer Survey conducted between 22 April and 24 August 2014 revealed that only 13 percent of U.S. residents decided to travel abroad for holidays – based on kidnappings, terrorist threats, and general concern for safety – over the previous year. In general, people are concerned for their safety outside the United States, but careful planning can help reduce the risk by researching travel warnings and restrictions, preparing a checklist, double-checking documentation, and most importantly having an emergency plan of action.

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

62nd IAEM-USA Annual Conference & EMEX

November 14–19, 2014

EMERGENCY MANAGEMENT

Navigating the New Normal

Meet colleagues, hear experts and see the latest technology in Emergency Management at IAEM 2014 in San Antonio!

Grand Hyatt San Antonio Hotel | San Antonio, TX

Conference: November 14–19, 2014

EMEX: November 17–19, 2014

www.iaem.com/conference

IAEM International Association of Emergency Managers
www.iaem.com

EMEX Emergency Management & Homeland Security Expo www.emex.org
www.emex.org

Be a part of the organization that represents Emergency Managers in local communities, and around the globe.

Emergency concerns cross borders—whether you are down the street or across the world. Today, being connected is more important than ever. IAEM brings together emergency managers and disaster response professionals from all levels of government, as well as the military, the private sector, and volunteer organizations around the world.